



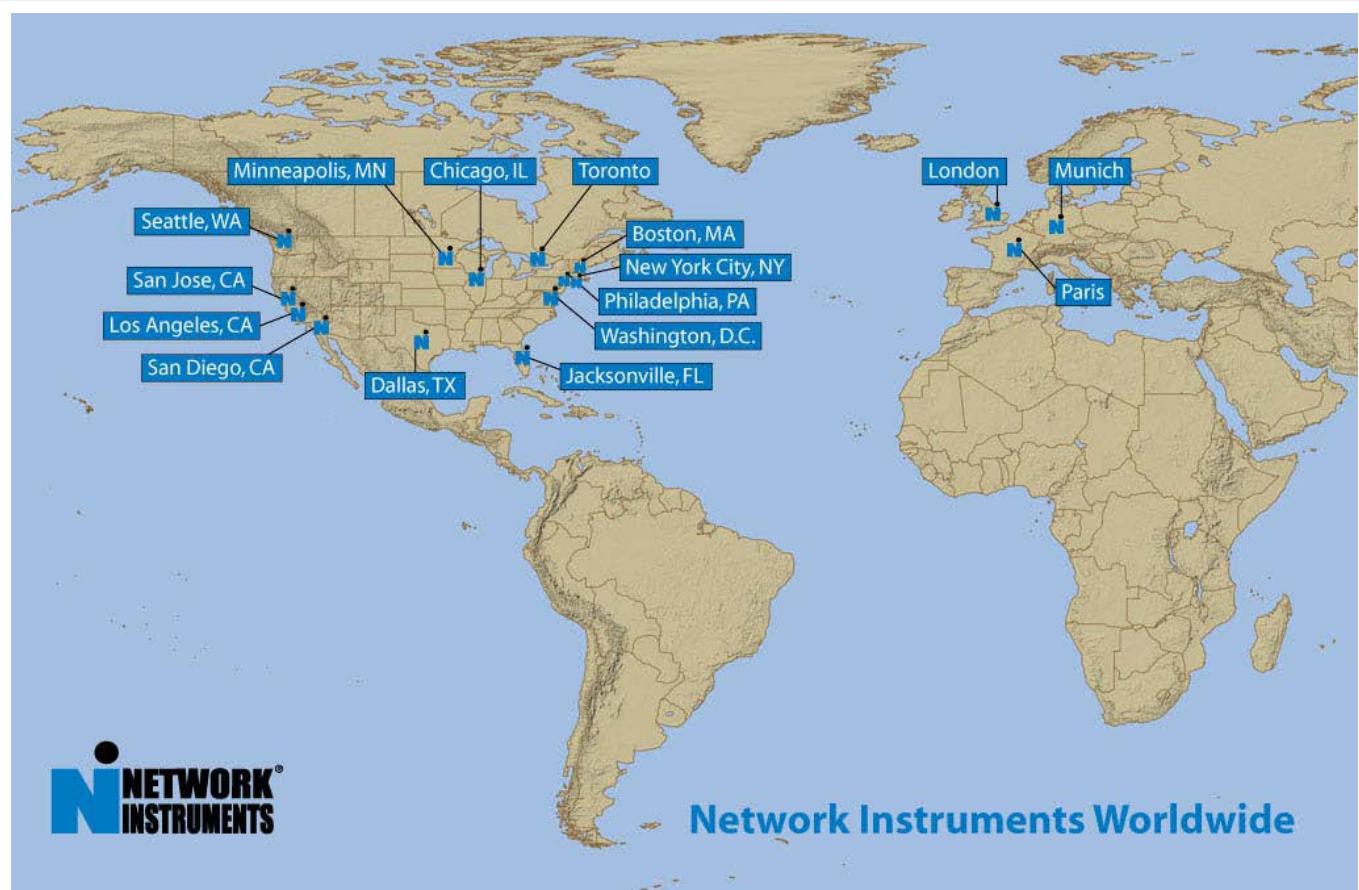
Network Instruments Solutions d'Analyse Réseau

ELEXO

20 Rue de Billancourt
92100 Boulogne-Billancourt
Téléphone : 33 (0) 1 41 22 10 00
Télécopie : 33 (0) 1 41 22 10 01
Courriel : info@elexo.fr
TVA : FR00722063534

Qui sommes-nous?

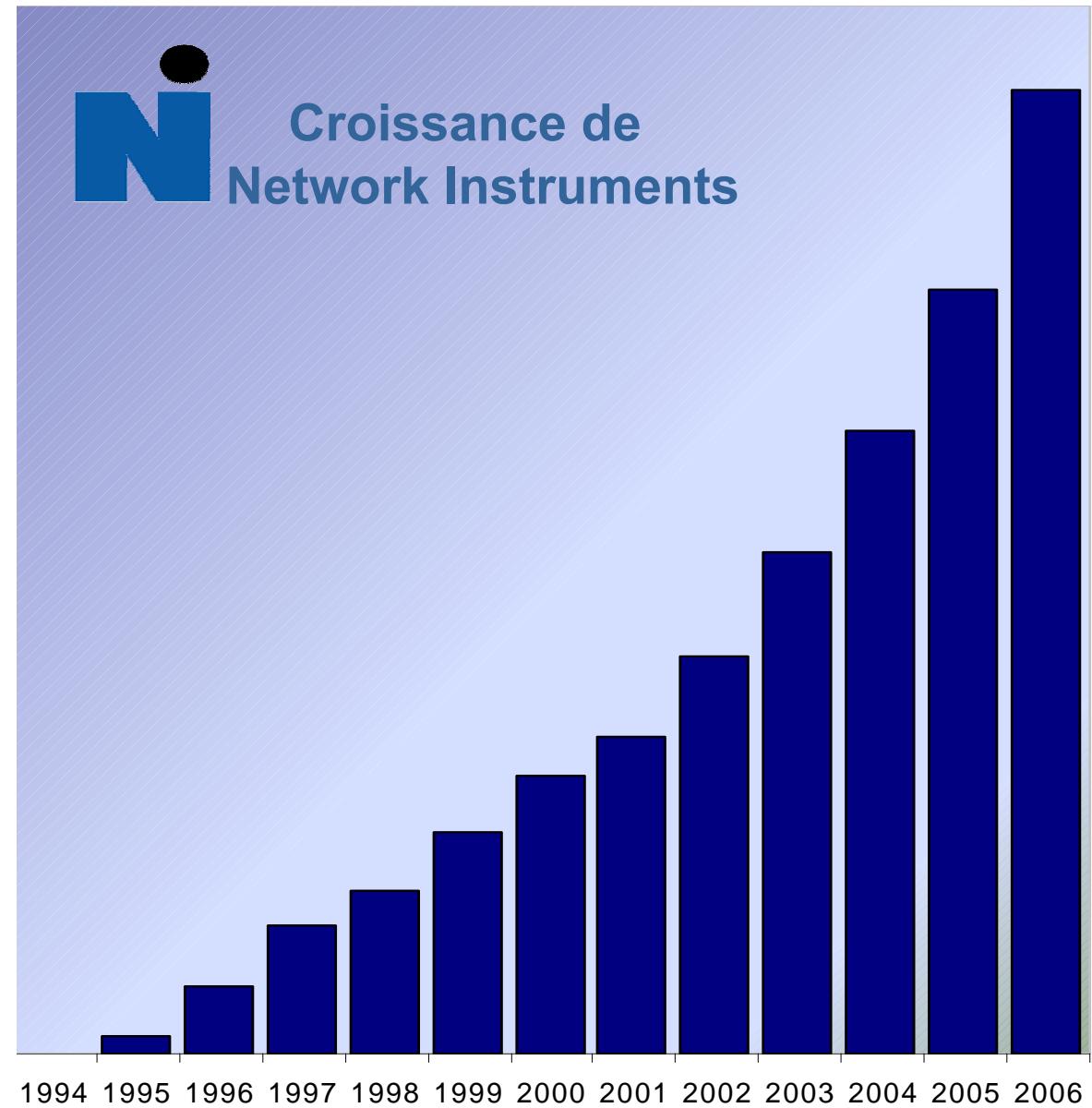
- Société fondée en 1994
- Siège Minneapolis USA
- Fonds privés, 100% détenus par fondateurs
- près de 50 000 licences installées
- 16 bureaux dans le monde
- 3 nouveaux bureaux en 2006
- 130 partenaires dans 50 pays
- Plus d'une nouvelle société par jour cliente en France



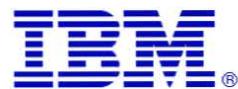
“Network Instruments croît de manière constante contrairement à d’autres vendeurs qui chutent ou abandonnent le marché .” - Steve Steinke, Groupe 451

Un coup d'oeil sur notre croissance

- Seule société sur le marché de l'analyse réseau avec un historique constant de croissance et de développement
- Depuis 5 ans = 25% de croissance annuelle
- Croissance 2006 = 26%
- Croissance France +300% entre 2003 et 2006
- Les facteurs de la croissance
 - Ventes de GigaStor™
 - Fidélité et développement de la clientèle existante
 - Remplacement d'installations concurrentes



Quelques références clients





Pourquoi Network Instruments?

Comment résoudre les problèmes efficacement?

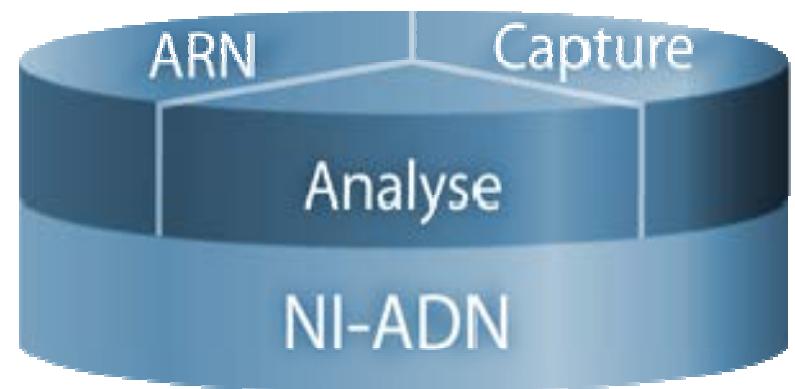


1^{ère} étape: Démarrez avec... l'Analyse Distribuée du Network (NI-ADN™)

2^{ème} étape: Assurez vous d'avoir une... Analyse puissante et précise

3^{ème} étape: Déterminez si le vendeur vous... Garantie une Capture fiable

4^{ème} étape: Expertisez les problèmes complexes grâce à... l'Analyse Rétrospective du Network (ARN™)



Démarrez avec l'Analyse Distribuée du Network (NI-ADN™)



Trois avantages uniques

Code uniifié

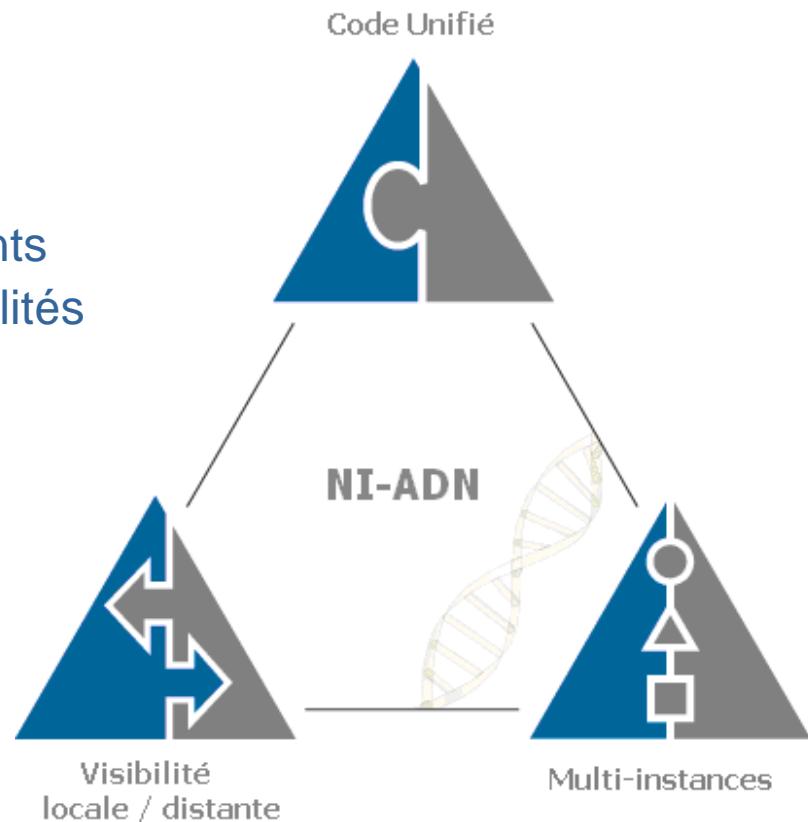
- Le cœur de l'application se connecte à tous les produits
- Les Améliorations sont ajoutées à toutes les plateformes
Ex. IPv6, NetFlow, VoIP, MPLS

Visibilité locale et distante

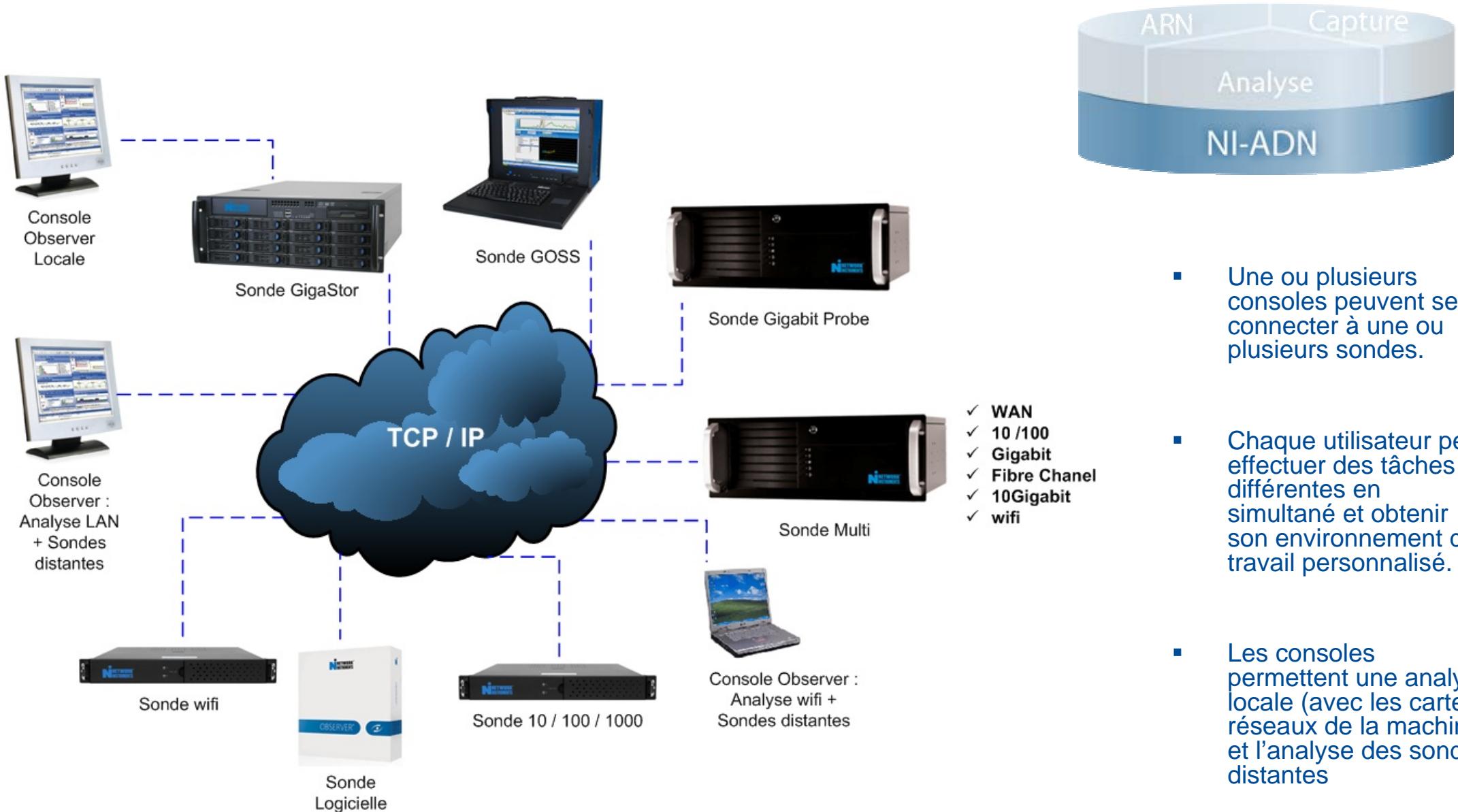
- Fonctionnalités identiques à travers tous les segments
- Une seule interface (GUI) pour toutes les fonctionnalités

Multi-Instances

- Topologies multiples
- Utilisateurs multiples
...le tout simultanément



Démarrez avec l'Analyse Distribuée du Network (NI-ADN™)

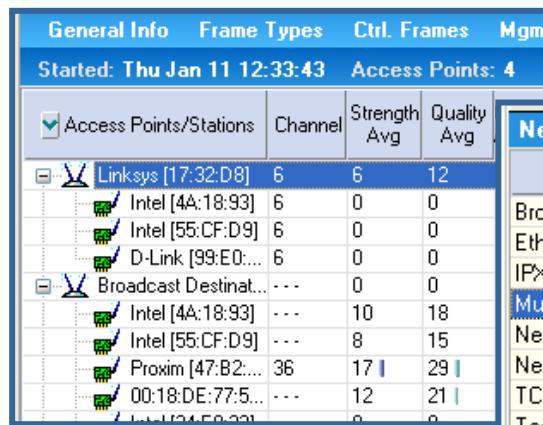


Du LAN jusqu'au WiFi. En Local & A Distance. Données & Applications.

Assurez vous d'avoir une Analyse puissante et précise



- Analyse Experte en temps réel
- Analyse Applicative
- VoIP
- Collecteurs NetFlow / sFlow
- Analyse des temps de réponse
- Analyse Forensics (sécurité)
- Rapports à travers toute l'entreprise

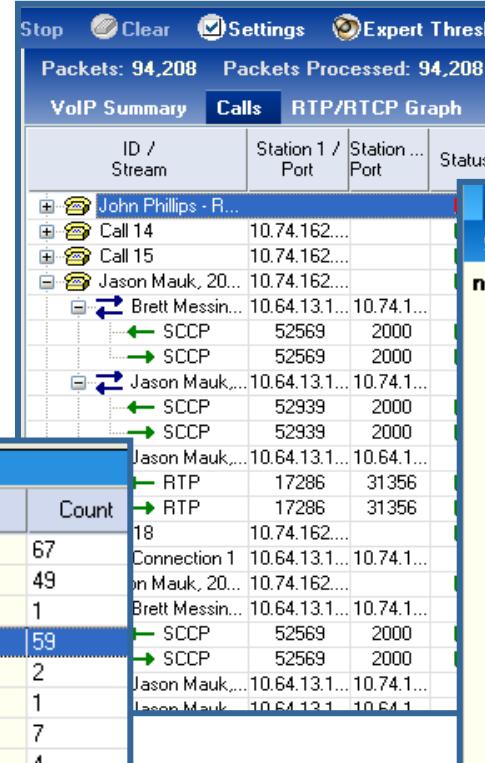


Site Survey WiFi

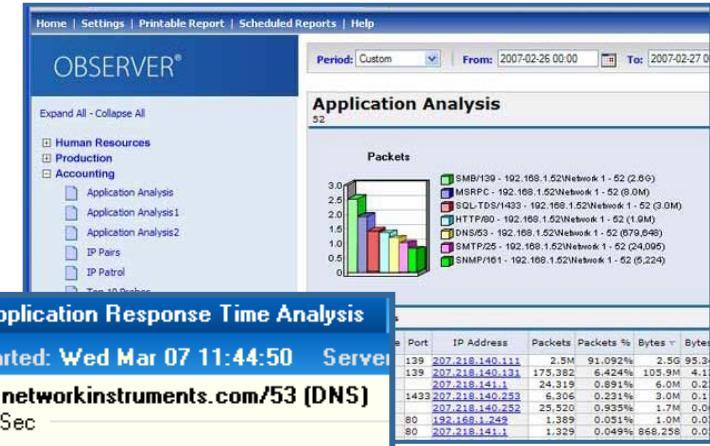


Analyse Experte

Détail des appels VoIP



Temps de réponse



rapport



Déterminez si le vendeur vous Garantie une Capture fiable

Carte de Capture Gen2™

Carte conçue en interne créée spécifiquement pour des analyses hautes performances



Performance

- **Traitements rapides** en temps réel
- **Capture pleine bande** Full-duplex en GB & 10GbE
- Transfère directement vers la mémoire physique
- Horodatage à la nanoseconde



Flexibilité

- Haute densité de ports – **jusqu'à 8 ports Gb**
- Basée sur des **SFP**: passez du cuivre à l'optique facilement

Exclusivement dans les Appliances Network Instruments

Adaptabilité

- Traitement et analyse au niveau de la carte
- Upgrade du driver par Flash

Gen2 Délivre

- ✓ Performance
- ✓ Flexibilité
- ✓ Adaptabilité

Compatible Gigabit, Fibre Channel, & 10 GbE

Expertisez les problèmes complexes grâce à l'Analyse Rétrospective du Network (ARN™)

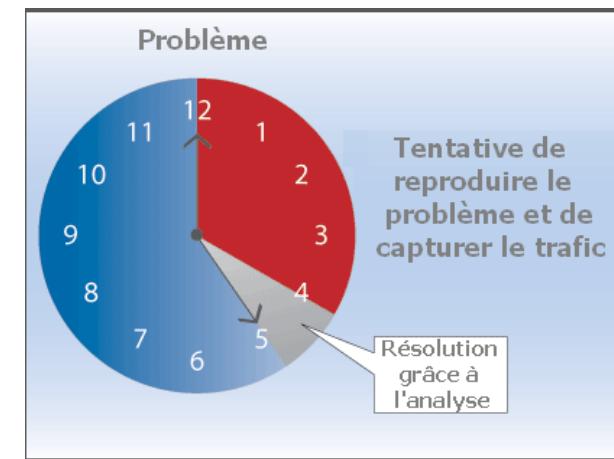


Analyse Rétrospective du Network

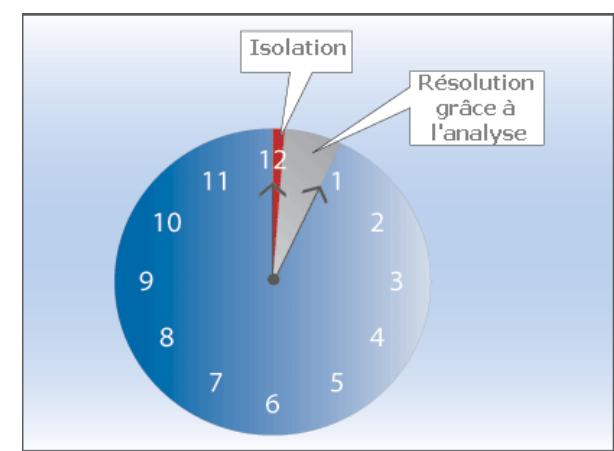


- Équipement de haute capacité de stockage
 - Capturez de grosses quantités de données afin d'étendre la période de temps d'analyse
- Idéal pour
 - Forensics
 - Conformité
 - Forage des données
 - Identification de Problèmes
- Capacités
 - Reconstruction de données
 - Diagnostic des attaques de sécurité
 - Navigation dans le Temps

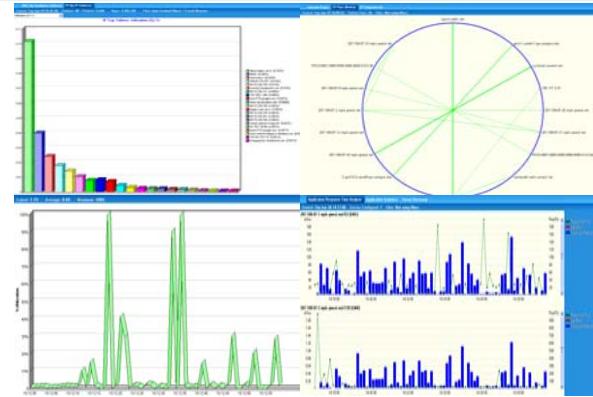
Avant
l'ARN



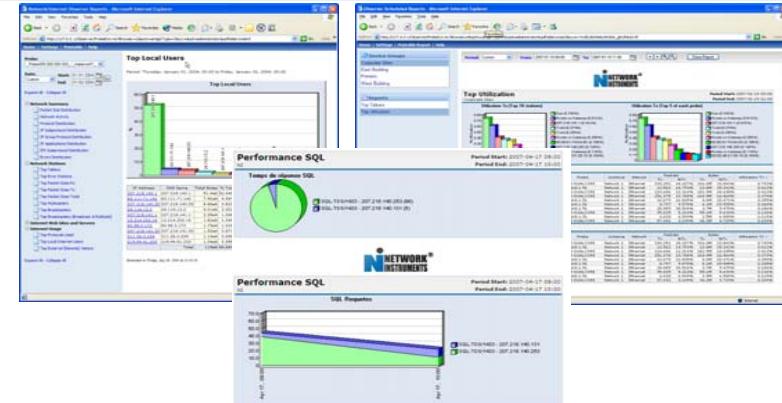
Après
l'ARN



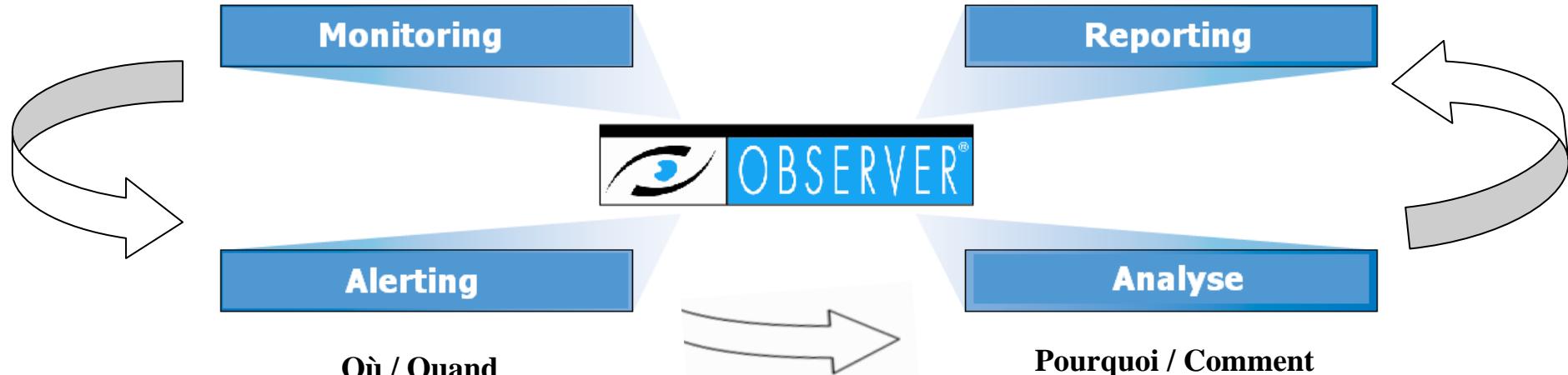
Positionnement Produit Observer



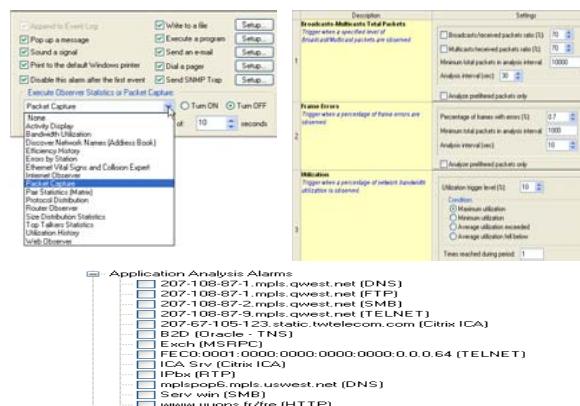
Qui / Quoi



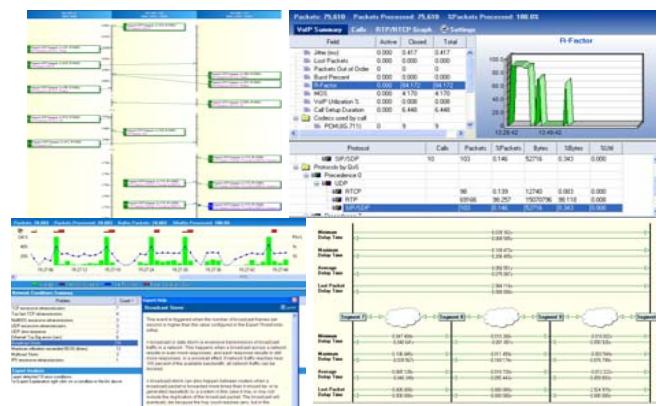
Quelles tendances



Où / Quand



Pourquoi / Comment





Quelques exemples...



Exemple 1...

Le réseau ne fonctionne plus...

Courriel d'un utilisateur vers le support technique

Que se passe-t-il sur le réseau??? - Message

Fichier Edition Affichage Insertion Format Outils Tableau Fenêtre ? Tapez une question

Joindre au format Adobe PDF

Times New Roman 12 G I S

Envoyer Comptes Options... HTML

À... support;
Cc...
Objet : Que se passe-t-il sur le réseau???

Salut Steve,

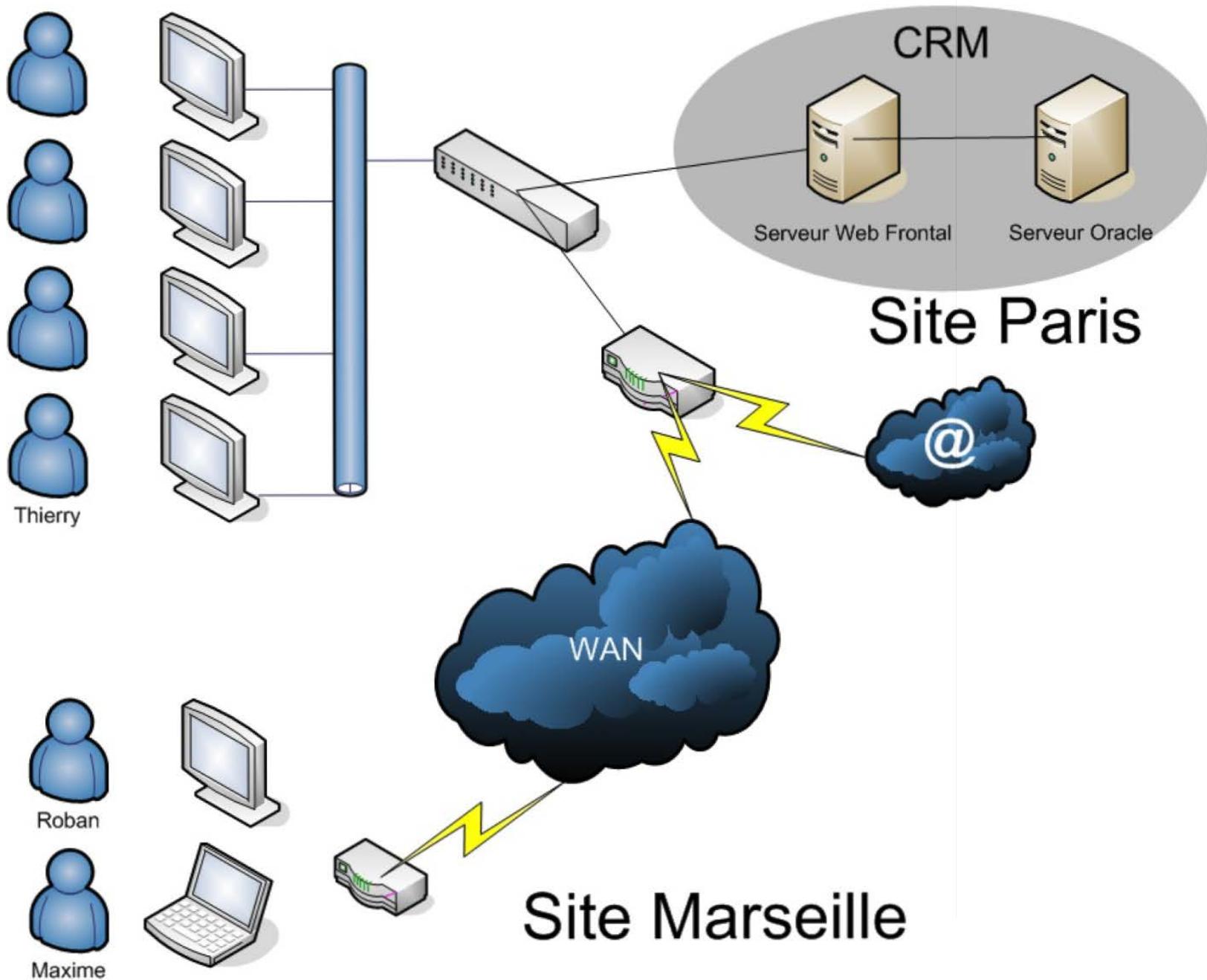
Est-ce que le réseau est tombé ?
Je n'arrive pas à accéder à notre CRM...

Merci de revenir vers moi au plus vite j'ai une proposition à envoyer pour cet après midi....

Thierry

Dessiner Formes automatiques

Schéma de l'architecture



Méthode classique de résolution de l'incident



- a) Ignorer le problème en espérant que le système revienne à la normale rapidement...
- b) Visualiser quelques graphiques de bande passante et une carte de disponibilité des équipements : Pas d'alertes en rouge, Bande passante à 30 %: le problème doit être résolu...
- c) Se déplacer avec un analyseur sur le réseau, tenter de se positionner à l'endroit où le problème s'est produit et espérer que le problème apparaisse à nouveau dans l'heure qui suit...

Nouvelle méthode : Analyse Rétrospective du Network (ARN)

Possibilité de revenir dans le temps afin d'investiguer les problèmes sans la nécessité de les reproduire...



- Problème reporté par un utilisateur ou par la direction
- Investigation avec les outils de management
- Déploiement d'une solution d'analyse pour capturer le trafic
- Recréer ou attendre que le problème apparaisse à nouveau
- Capturer les événements
- Analyser l'information
- Prendre les actions appropriées

Temps

- Problème remonté par le système d'**Alerting**
- Demander au système de "**voir ce qu'il s'est passé**"
- **Analyse** des informations remontées
- Prendre les actions appropriées
- **Communiquer** vers les autres services et la direction grâce au **rapports**

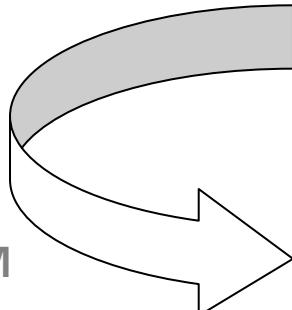
Temps Réduit = Réduction des coûts
Plus de temps pour d'autres tâches

Alerte le serveur de base de données

Alarm List Triggers Actions

Check one or more items to enable Alarms:

- Application Analysis Alarms
 - 131.107.80.229 (HTTP)
 - 172.19.141.35 (HTTP)
 - 207.218.140.7 (HTTP)
 - 207.46.130.150 (HTTP)
 - 207.67.105.123 (HTTP)
 - 207.68.183.32 (HTTP)
 - 207-67-105-123.static.twtelecom.com (Citrix ICA)
 - 64.233.161.147 (HTTP)
 - 64.233.167.104 (HTTP)
 - 80.253.126.120 (HTTP)
 - EXCHANGE (MSRPC)
 - Oracle CRM (Oracle - TNS)
 - www-sjl.salesforce.com (HTTP)

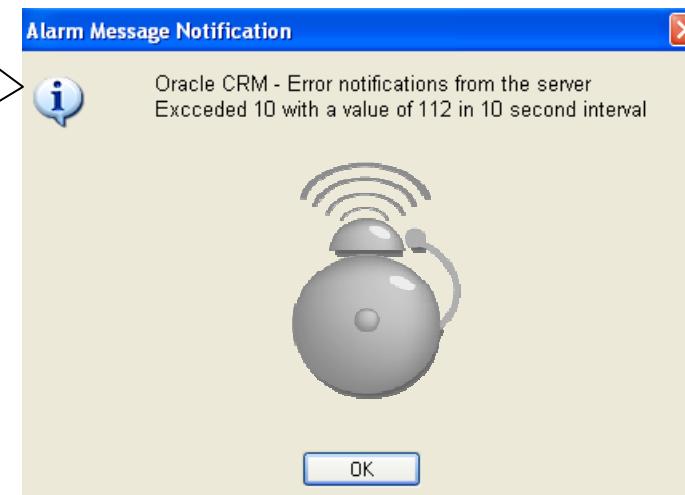


Probe Alarms Settings

Alarm List Triggers Actions

Description	Settings																
Application Analysis: Oracle CRM (Oracle - TNS) <i>Trigger an alarm for each of the checked criteria when the value exceeds the configured threshold within the specified interval.</i>	Alarm Thresholds <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Total Errors</td> <td></td> </tr> <tr> <td>Total Requests</td> <td></td> </tr> <tr> <td>Response Time (msec)</td> <td></td> </tr> <tr> <td>Logins</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Error notifications from the server</td> <td>10</td> </tr> <tr> <td>SQL commands</td> <td></td> </tr> </tbody> </table> Analysis interval (sec): 10	Parameter	Value	Total Errors		Total Requests		Response Time (msec)		Logins		<input checked="" type="checkbox"/> Error notifications from the server	10	SQL commands			
Parameter	Value																
Total Errors																	
Total Requests																	
Response Time (msec)																	
Logins																	
<input checked="" type="checkbox"/> Error notifications from the server	10																
SQL commands																	
Application Analysis: www-sjl.salesforce.com (HTTP) <i>Trigger an alarm for each of the checked criteria when the value exceeds the configured threshold within the specified interval.</i>	Alarm Thresholds <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Total Errors</td> <td></td> </tr> <tr> <td>Total Requests</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Response Time (msec)</td> <td>50</td> </tr> <tr> <td>Successful transactions</td> <td></td> </tr> <tr> <td>Redirected transactions</td> <td></td> </tr> <tr> <td>Page not found</td> <td></td> </tr> <tr> <td>Invalid client requests</td> <td></td> </tr> </tbody> </table>	Parameter	Value	Total Errors		Total Requests		<input checked="" type="checkbox"/> Response Time (msec)	50	Successful transactions		Redirected transactions		Page not found		Invalid client requests	
Parameter	Value																
Total Errors																	
Total Requests																	
<input checked="" type="checkbox"/> Response Time (msec)	50																
Successful transactions																	
Redirected transactions																	
Page not found																	
Invalid client requests																	

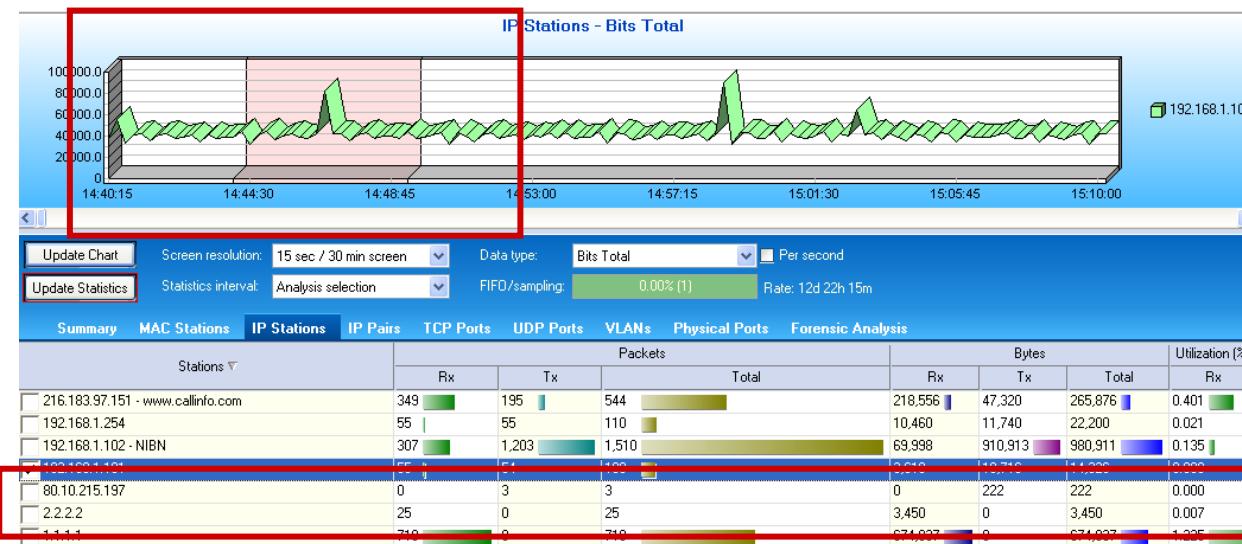
OK Annuler Aide



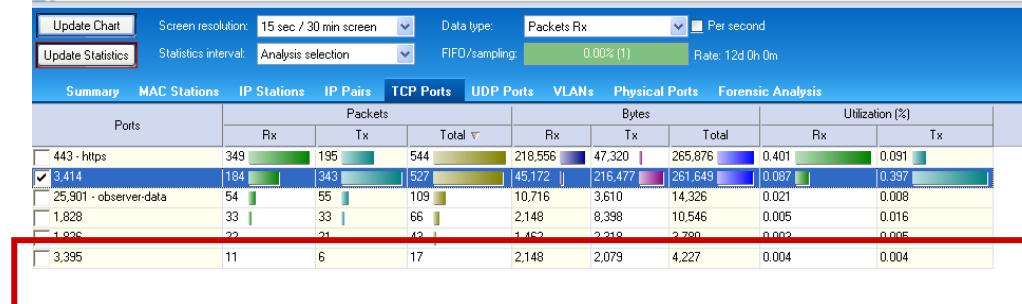
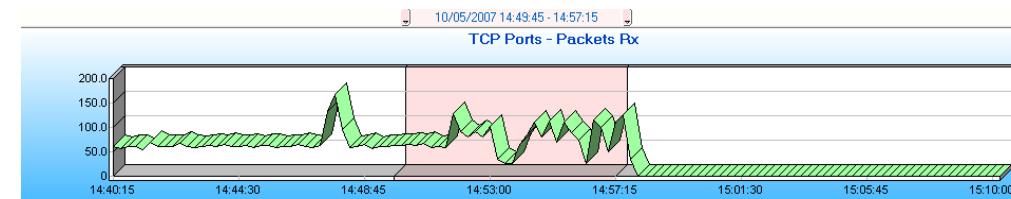
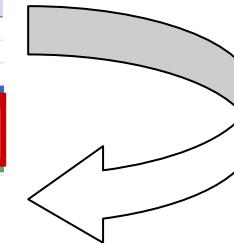
Surveillance des serveurs
constituant l'application CRM

Recherche Temps / Utilisateur / Application

N

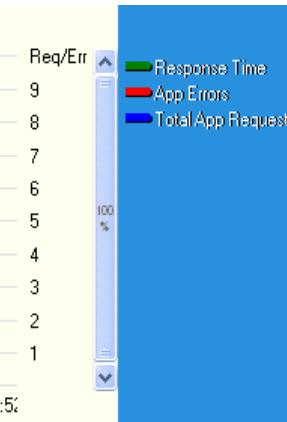
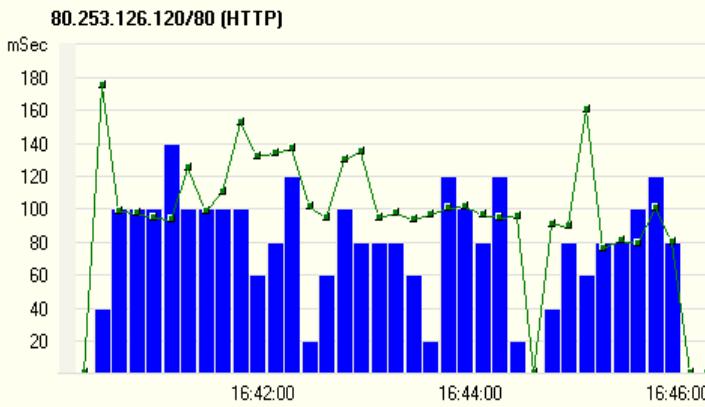


Recherche de la période de temps
+
Sélection de la station concernée



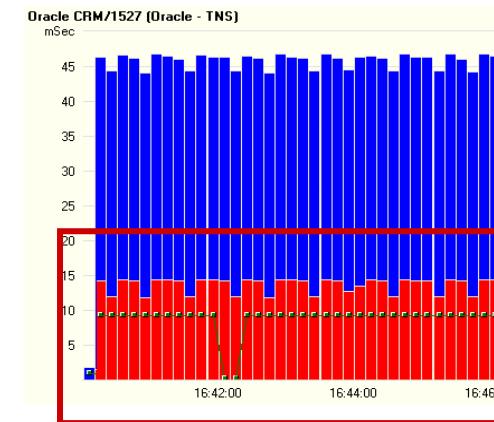
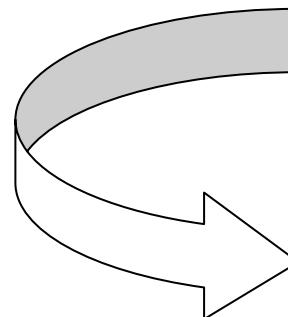
Sélection de l'application
CRM

Analyse Applicative sur le Serveur CRM



- Temps de réponse acceptable sur le serveur frontal HTTP.
- Aucune Erreur Applicative

Beaucoup d'Erreurs de notifications du serveur Oracle



Request Time ▼	Response Time	Request Packet	Response Packet
29/09/2006 10h:31m:19.008s	29/09/2006 10h:31m:19.009s	261	262
29/09/2006 10h:31m:21.998s	29/09/2006 10h:31m:21.999s	873	874
29/09/2006 10h:31m:22.011s	29/09/2006 10h:31m:22.011s	885	886
29/09/2006 10h:31m:25.441s	29/09/2006 10h:31m:25.462s	1948	1951
29/09/2006 10h:31m:25.674s	29/09/2006 10h:31m:25.695s	2039	2040
29/09/2006 10h:31m:25.854s	29/09/2006 10h:31m:25.854s	2102	2103
29/09/2006 10h:31m:26.028s	29/09/2006 10h:31m:26.029s	2166	2167
29/09/2006 10h:31m:26.197s	29/09/2006 10h:31m:26.198s	2228	2229
29/09/2006 10h:31m:26.380s	29/09/2006 10h:31m:26.381s	2293	2294
29/09/2006 10h:31m:26.551s	29/09/2006 10h:31m:26.552s	2356	2357
29/09/2006 10h:31m:26.720s	29/09/2006 10h:31m:26.720s	2419	2420
29/09/2006 10h:31m:26.886s	29/09/2006 10h:31m:26.886s	2482	2483
29/09/2006 10h:31m:27.061s	29/09/2006 10h:31m:27.062s	2545	2546
29/09/2006 10h:31m:27.224s	29/09/2006 10h:31m:27.225s	2608	2609

Oracle CRM/1527 (Oracle - TNS)	60,624
Packets	5,489,113
Routes	0
Logins	986
Error notifications from the server	30,140
SQL commands	

```
.....FOLDER_TYPE..Empty folder....  
..FOLDER_TYPE..Folder for files.....{.....+  
.....ORA-01403: no data found
```

Le Reconstruction du flux nous montre que la base de données a été modifiée : un Dossier n'est plus présent



Exemple 2...

Lenteur sur un site distant

Courriel de Maxime de Marseille vers le support

Internet est très lent... - Message

Fichier Edition Affichage Insertion Format Outils Tableau Fenêtre ? Tapez une question

Joindre au format Adobe PDF

Times New Roman 12 G I S

Envoyer Comptes Options... HTML

À... support;

Cc...

Objet : Internet est très lent...

Bonjour Steve,

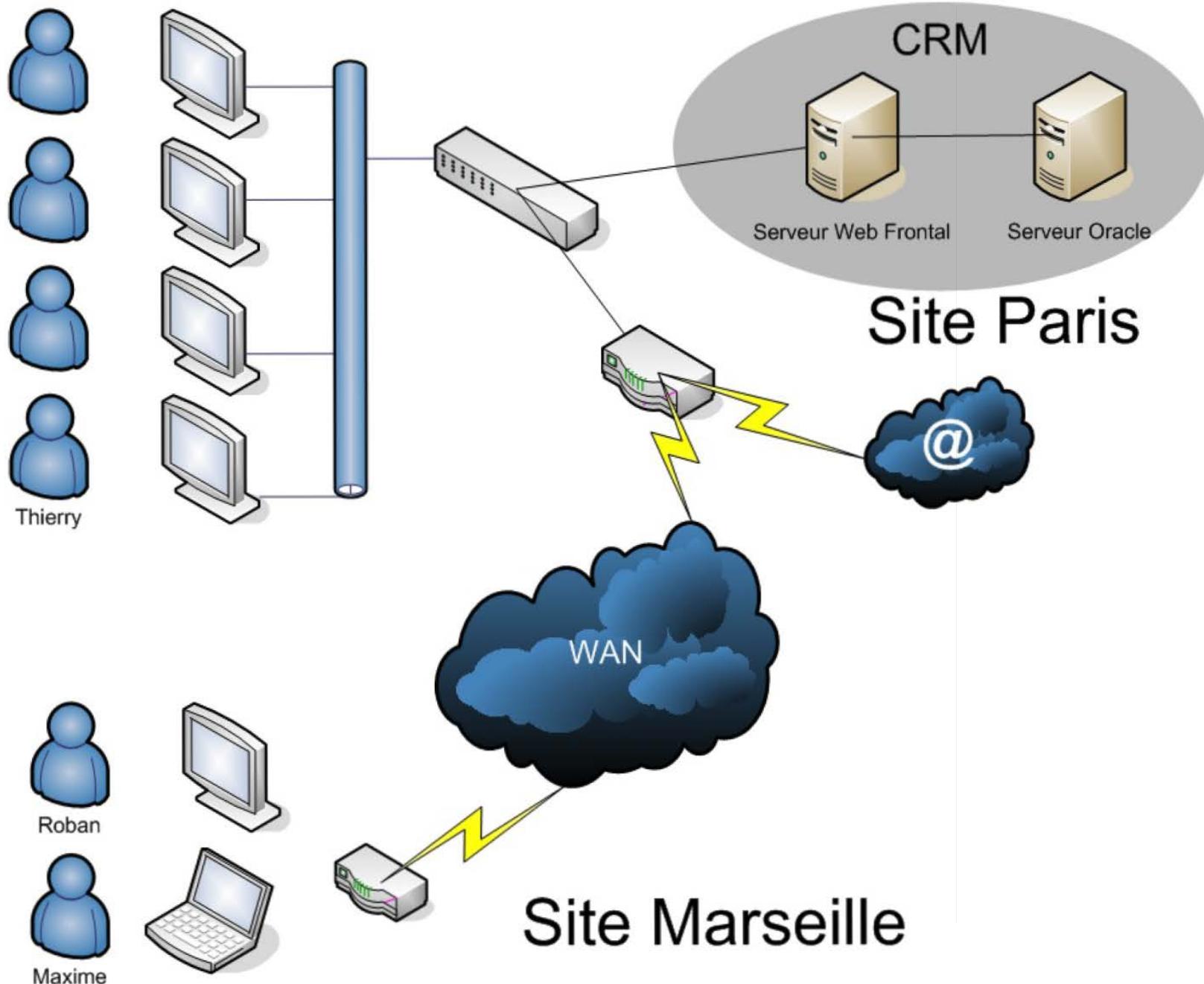
J'essaye d'accéder à Internet et à nos applications de Paris c'est très lent ; que se passe-t-il ?

J'ai une réunion à préparer merci de résoudre le problème rapidement

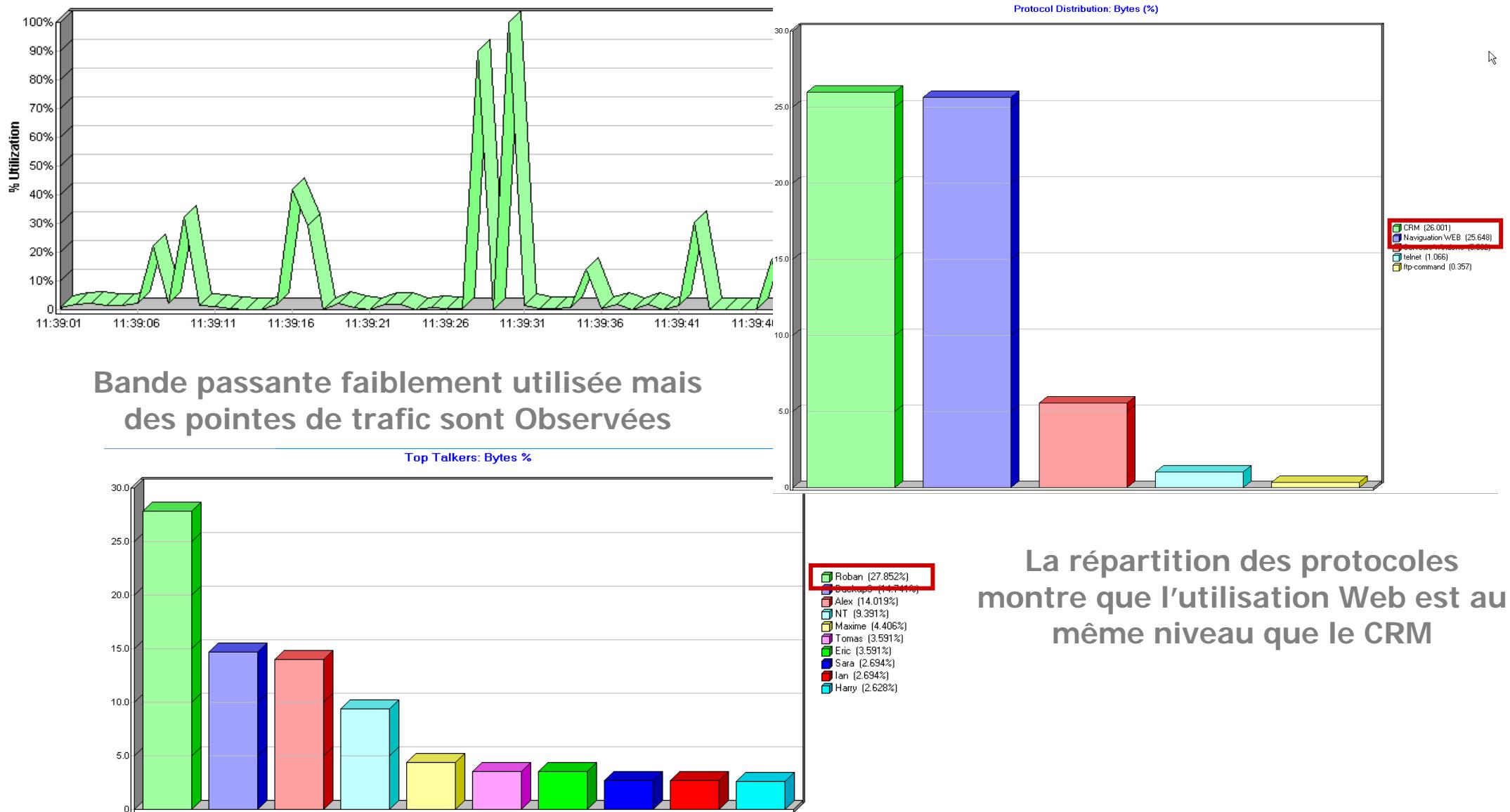
Maxime

Dessiner Formes automatiques

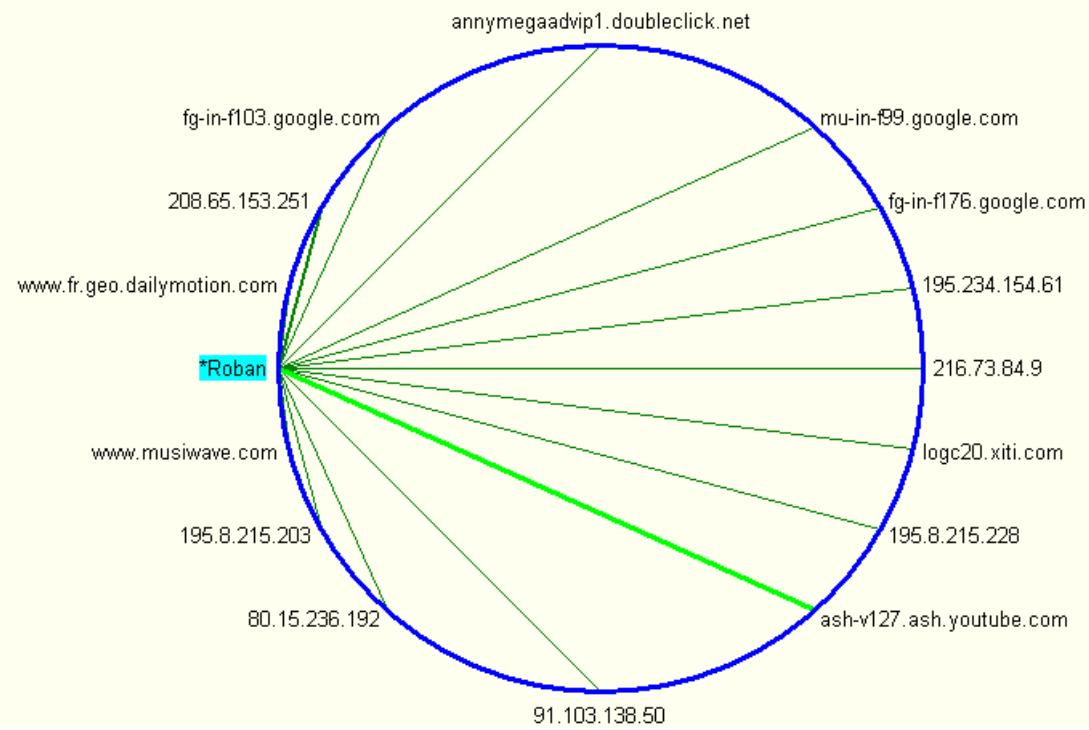
Schéma de l'architecture



Santé du réseau : Monitoring



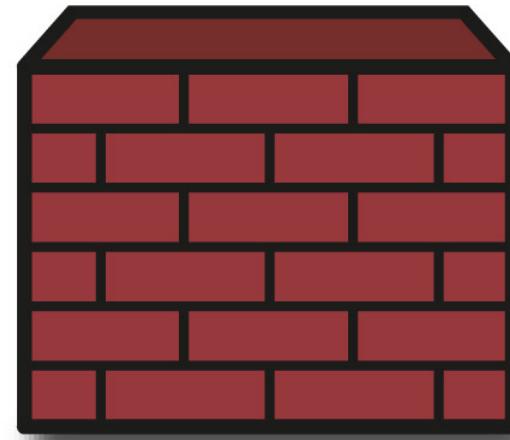
Zoom sur Roban



Roban utilise une grande partie de la bande passante en téléchargeant de la musique et en regardant des Vidéos en Streaming

Modification des règles sur le Firewall pour bloquer les Vidéos et musiques.

Le problème persiste....



Analyse Experte et Diagnostic automatique



Decode and Analysis - Local Observer / LAN

Start Stop Clear Settings Expert Thresholds Tools

Pkts: 3457 Pkts Processed: 3457 % Pkts Processed: 100%

Util %

80%
60%
40%
20%
0%

07:00 09:07:12 09:07:24 09:07:36 09:07:48 09:08:00 09:08:12

Average Utilization Maximum Utilization Total Pkts/Sec Expert Conditions Count

Summary TCP Events UDP Events ICMP Events IPX Events NetBIOS Events Wireless Events Connection Dynamics

Expert Data

Network Conditions Summary

Problem	Count
Ethernet Too Big errors (sec)	6
TCP excessive retransmissions	1994
TCP slow response	6
Too fast TCP retransmissions	4
UDP excessive retransmissions	1
UDP slow response	1

Expert Help

TCP Excessive Retransmissions

This occurs when a sequence number is either identical to a previous sequence number, or is less than a previous sequence number. This indicates that the packet is a duplicate of one previously sent. TCP retransmissions occur for a number of reasons, including the sending station did not receive an acknowledgment, the packet was lost, dropped or otherwise missing. The event is displayed when the percentage of retransmitted packets (by application and address pair) is above the critical value set in the Expert Thresholds. This value is the sum of all identified events in the TCP Events display.

Possible reasons for the event:

- The receiving station was too busy to respond to the sending station.
- Network traffic load was so high the original packet was lost, or the ACK was never received due to the high utilization.
- A router dropped the packet, or was unable to forward the packet. This could be because the router is too busy, or is malfunctioning.
- Bad cabling or a failing switch/hub is causing an intermittent network failure.

Expert Analysis

Expert detected 6 error conditions.
For Expert Explanation right click on a condition in the list above.

Decode Summary Protocols Top Talkers Pairs (M) Site Survey WAN

Événements TCP

Démarrer Arrêter Effacer Paramètres globaux Expert Seuil Expert (Modèle OSI) Vue Outils Refresh

Packets: 41,482 Packets Processed: 41,482 %Packets Processed: 100.0% Connections: 9

Station1/Port -->	<- Station2/Port	Protocol	Status	packets -->	<- Packets	Response Time (ms) -->	<- Response Time (ms)	Network Delay (ms) -->	<- Network Delay (ms)	Retrans -->	<- Retrans
192.168.1.102	72.14.221.99/80	HTTP	■	1452	924	20.335	77.442	0.029	53.779	0	101
192.168.1.102	80.15.236.167/80	HTTP	■	64	66	122.162	54.235	0.034	46.003	0	18
192.168.1.102	80.15.236.241/80	HTTP	■	64	66	144.026	60.058	0.033	44.579	0	17
192.168.1.102	216.183.97.151/443	HTTP TLS/SSL	■	8233	4968	87.900	215.959	0.032	166.203	3	6
192.168.1.102/3863	72.14.221.99/80	HTTP	■	6	4	0.184	60.951	0.037	...	0	1
192.168.1.102/3864	72.14.221.99/80	HTTP	■	2	1	0.000	172.234	0	0
192.168.1.102/3702	72.14.221.99/80	HTTP	■	3	1	0.000	56.470	0	0
192.168.1.101	192.168.1.102/25901	Observer-data	■	1324	1314	1343.596	1311.800	1.163	14.851	0	0
192.168.1.102	192.168.1.101/139	NetBIOS session	■	28	26	0.466	5.304	0.056	0.929	0	0

Expert Data

TCP Events

UDP Events

ICMP Events

IPX Events

NetBIOS Events

VoIP Events

Visualisation de la session entre Maxime et notre CRM:

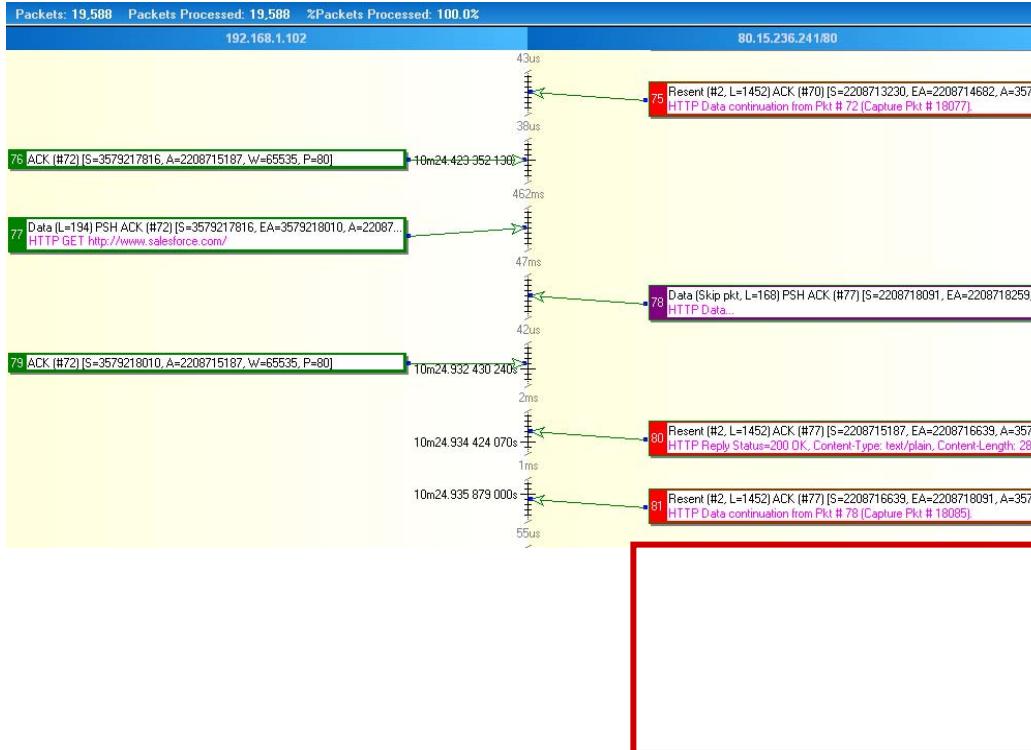
Le mode Expert nous indique un nombre important de retransmissions du Serveur vers Maxime...

Expert Analysis

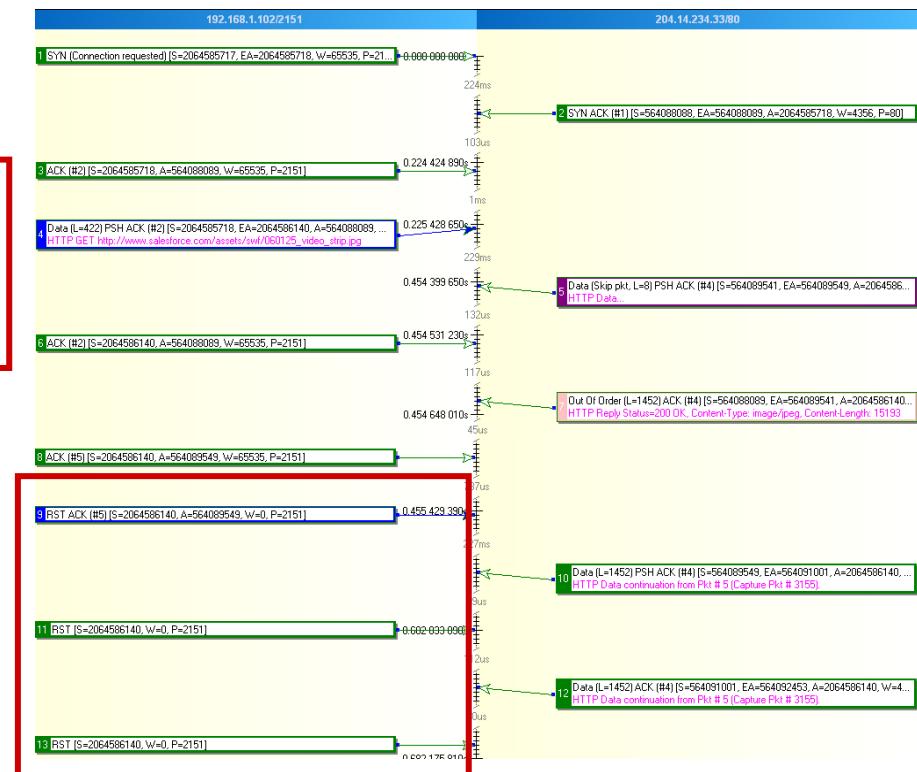
Client: 192.168.1.102 Server: 72.14.221.99/80 [HTTP]
 Client analysis: Client responds sufficiently fast.
 Server analysis: Server responds sufficiently fast. Error conditions on the network: Excessive retransmissions.

Right click on a column for a Expert Explanation about that item.

Connexions Dynamiques

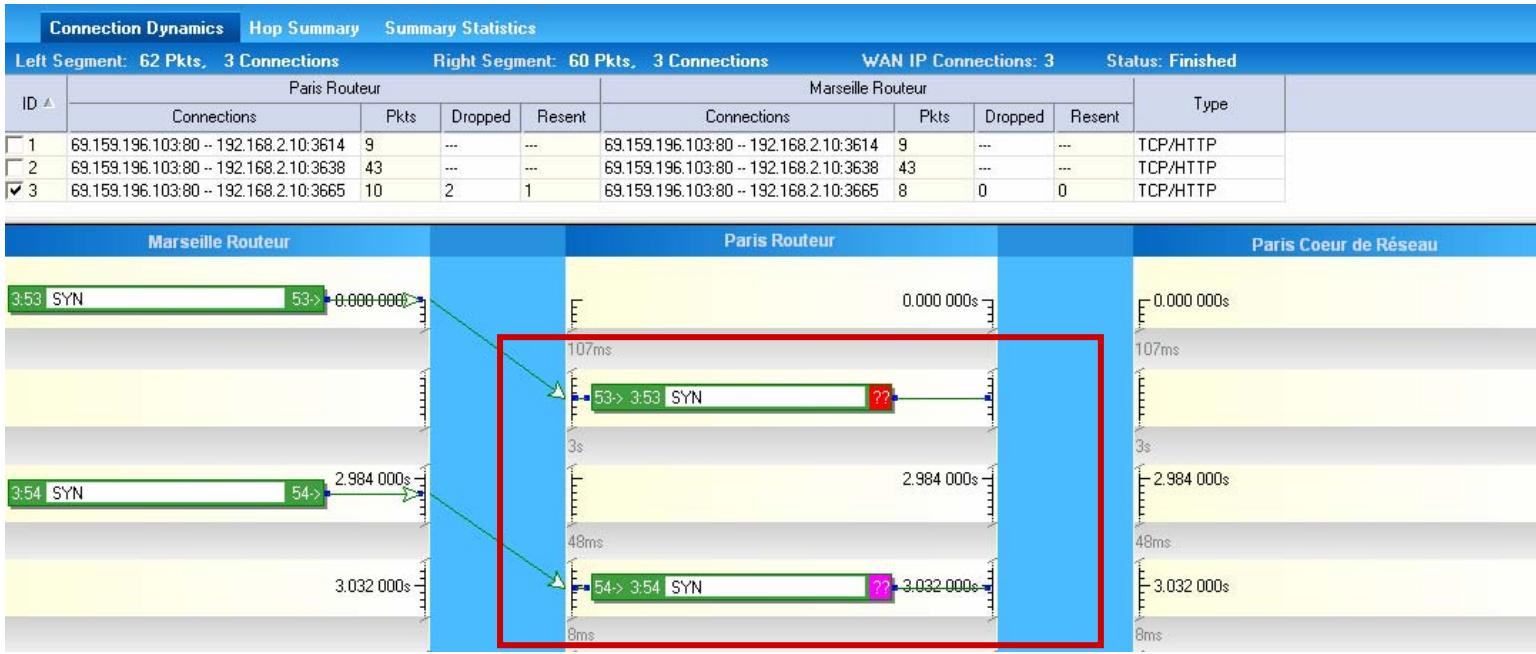


Paquets retransmis...



Le serveurs envoie aussi un grand nombre de Reset de connexion TCP sans raison...

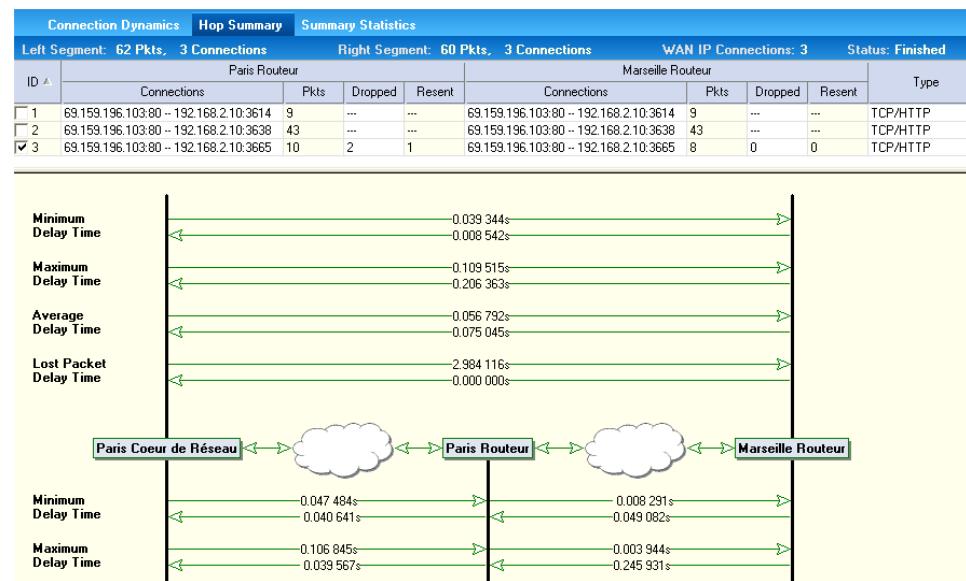
Analyse Multipoints



Grâce à l'analyse Multipoints Observer montre qu'un grand nombre de trames sont perdues du côté du Routeur de Paris

Un ticket d'erreur est ouvert au support du provider

Une vérification sur le serveur montre qu'il est mal configuré et « Reset » la connexion lorsque les temps de réponse sont trop lents.





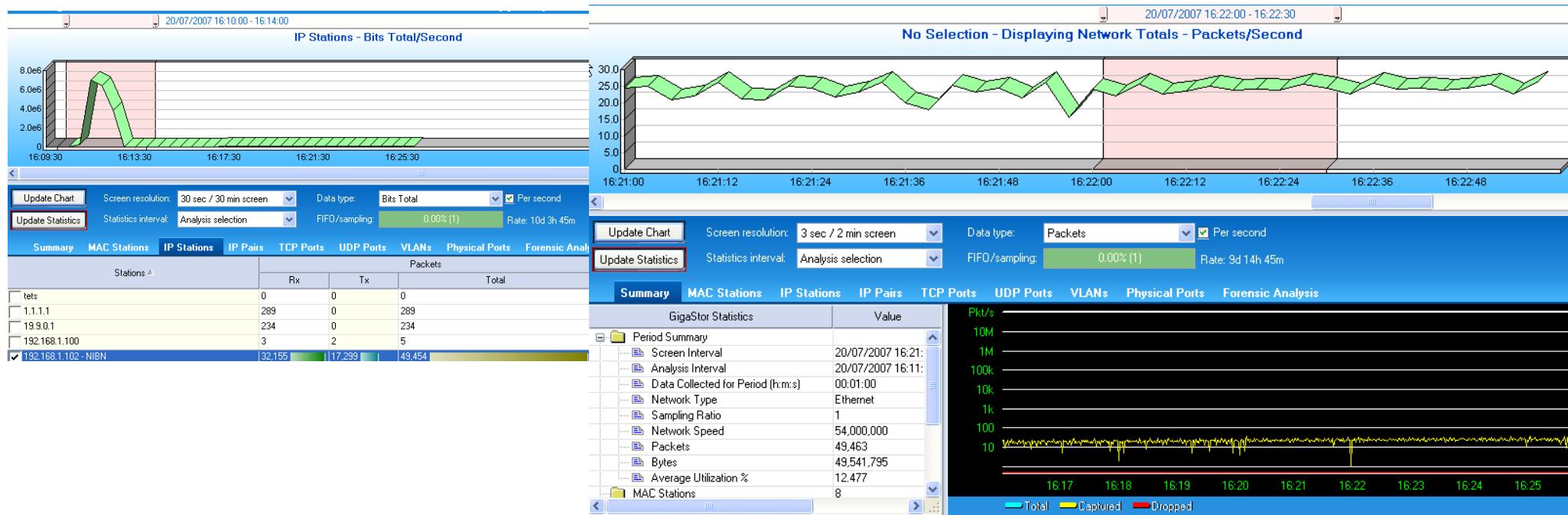
Exemple 3...

Qualité de la VoIP médiocre

Qualité de la communication médiocre....

- Le service réseau est averti que la qualité de la VoIP d'un utilisateur est très mauvaise...
- Le problème est sporadique et les autres téléphones dans le même étage ne subissent pas de problème.
- Les statistiques agrégées du logiciel de gestion de la téléphonie montre une bonne qualité globale...
- Un état des lieux rapide montre que certains liens sont fortement utilisés, l'état général du réseau est bon.

Sélection du temps et de la station



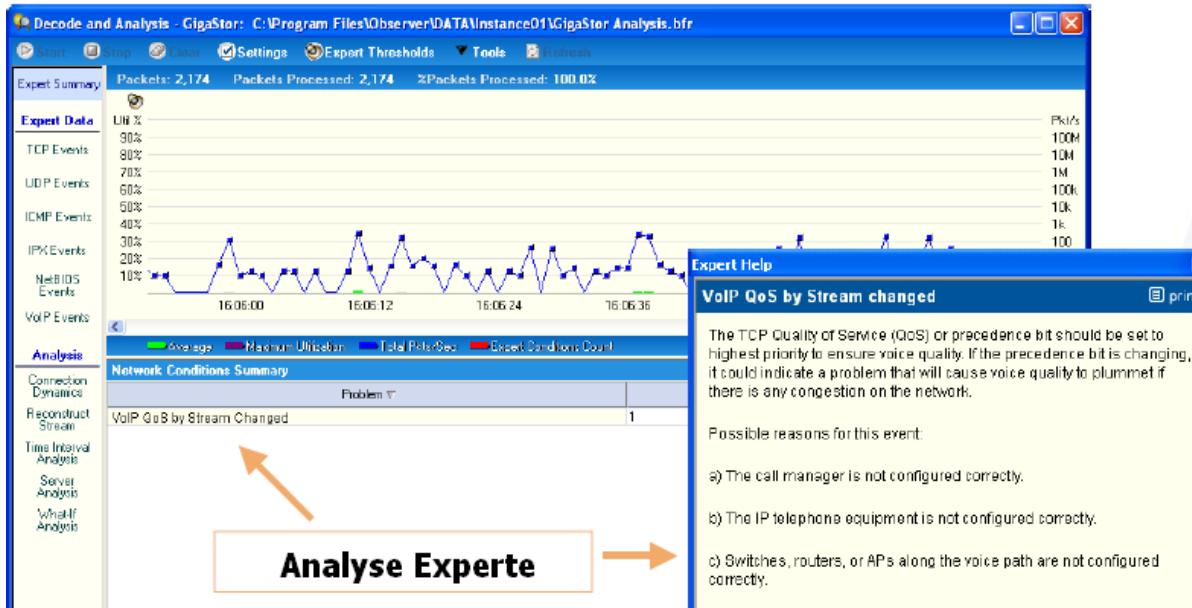
Sélection de la période de temps et de la station



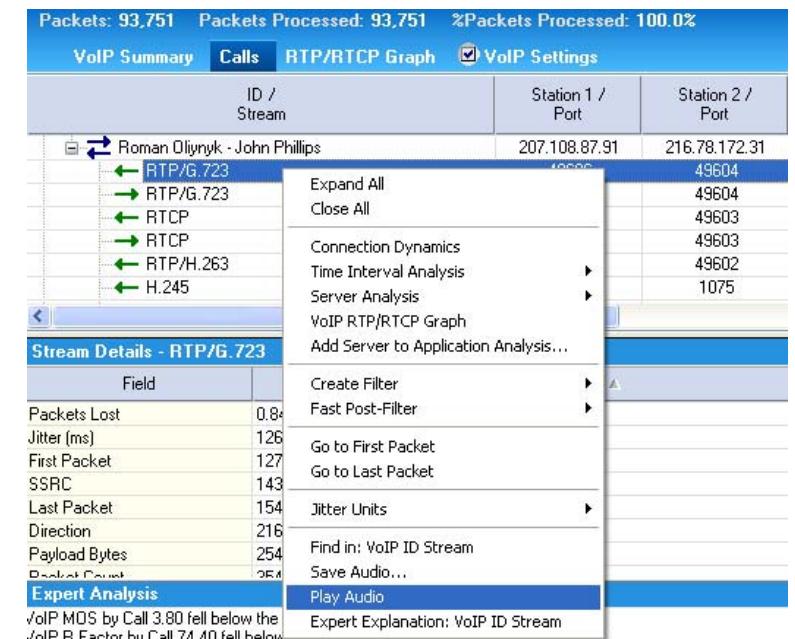
L'utilisation de la bande passante est faible avec des pics de temps à autres

Le jitter est assez élevé

Laissons l'Expert travailler



Analyse Experte



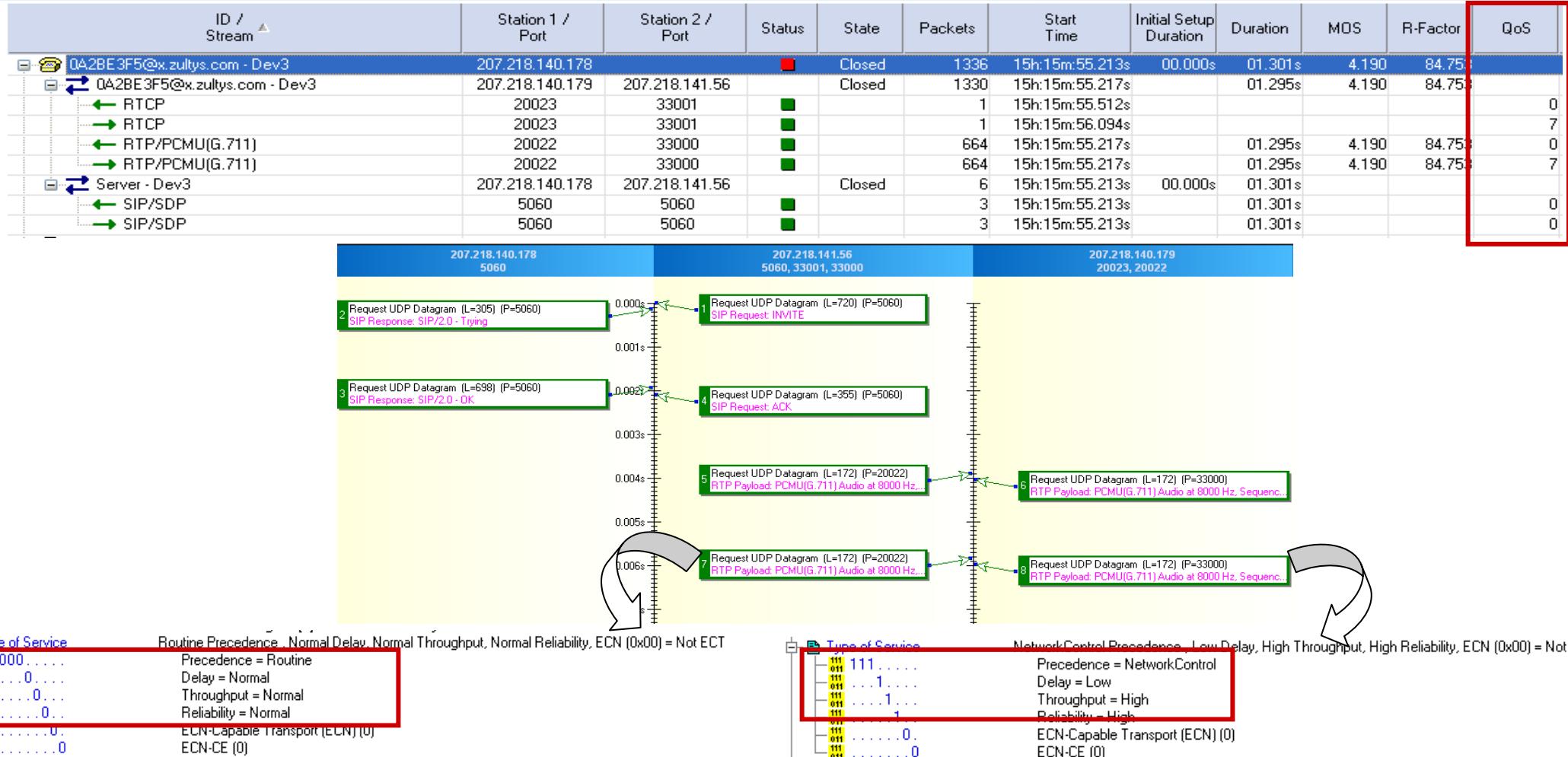
Le mode Expert nous indique que le niveau de QOS a changé durant la conversation... Nous pouvons le vérifier en rejouant la conversation pour en juger la qualité...



Le jitter qui en résulte est instable



Investigation de l'équipement en cause



Le niveau de qualité de service entre le téléphone 1 et le serveur SIP et vers le téléphone 2 est « temps réel »,

Le niveau de qualité de service entre le téléphone 2 et le serveur SIP est « temps réel » mais vers le téléphone 1 en « best effort »

Conclusion : Changement des paramètres de QOS sur le téléphone



Exemple 4...

Migration vers un réseau MPLS...

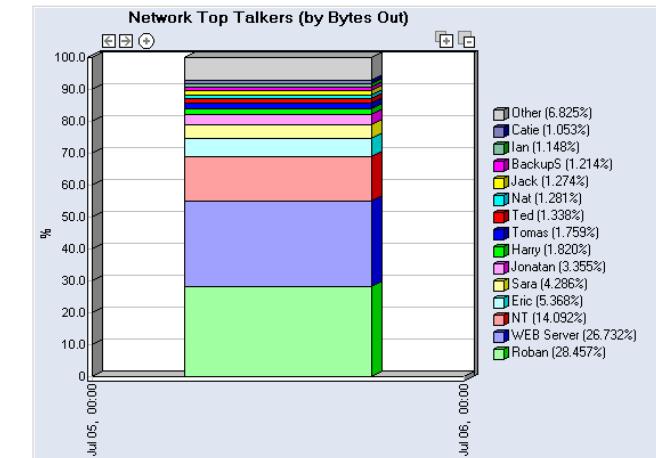
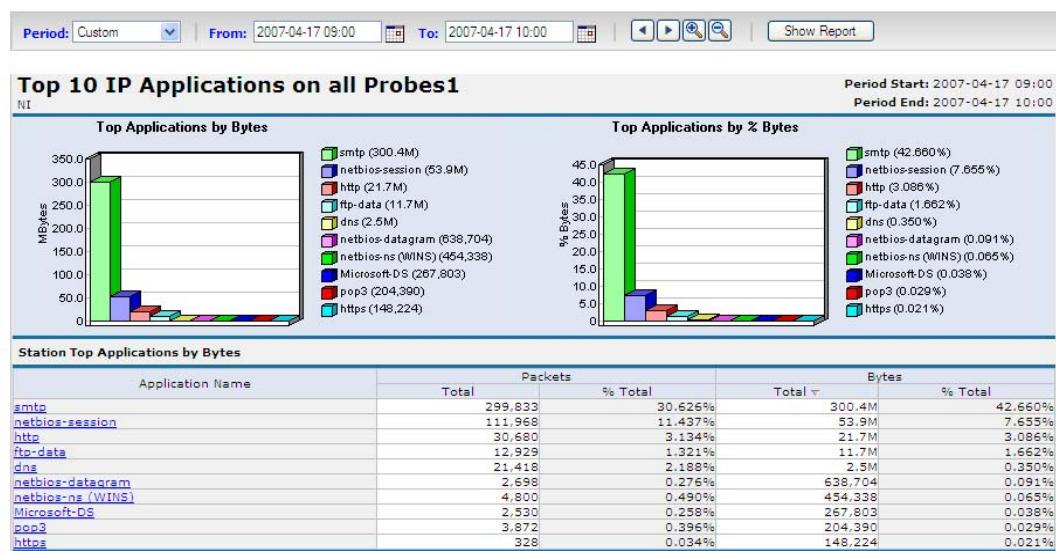
Rapports : Données fondamentales du réseau

N

OBSERVER®

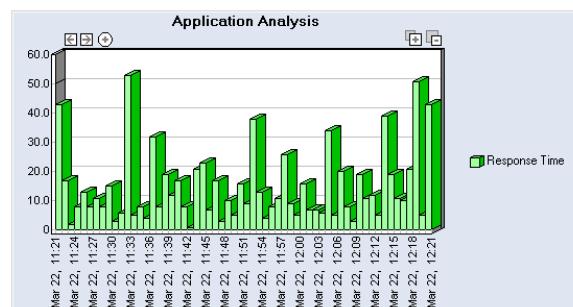
Expand All - Collapse All

- Call Manager
- Database Servers
- Email Servers
- Marseille
- NI
 - Performance SQL
 - Top 10 IP Applications on all Probes
 - Top 10 IP Applications on all Probes1
 - Top 10 IP Pair Stations on all Probes
 - Top 10 Probes by Utilization
 - Top 10 Server Applications on all Probes
 - Top 10 Stations Protocol Distribution on all Probes
 - Top 10 Web Servers on all Probes
- Paris
- Printers
- Production
- Routers
- Serveurs Base de Données
- Serveurs Métier CRM

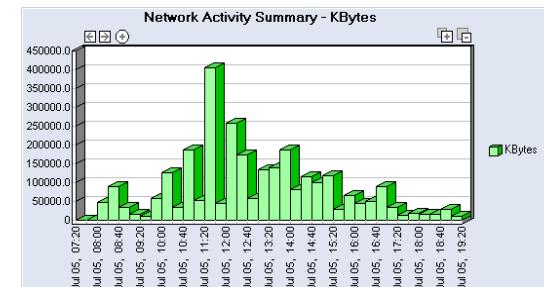


Stations les plus bavardes

Vue Agrégée de la répartition des protocoles sur la globalité des sites distants

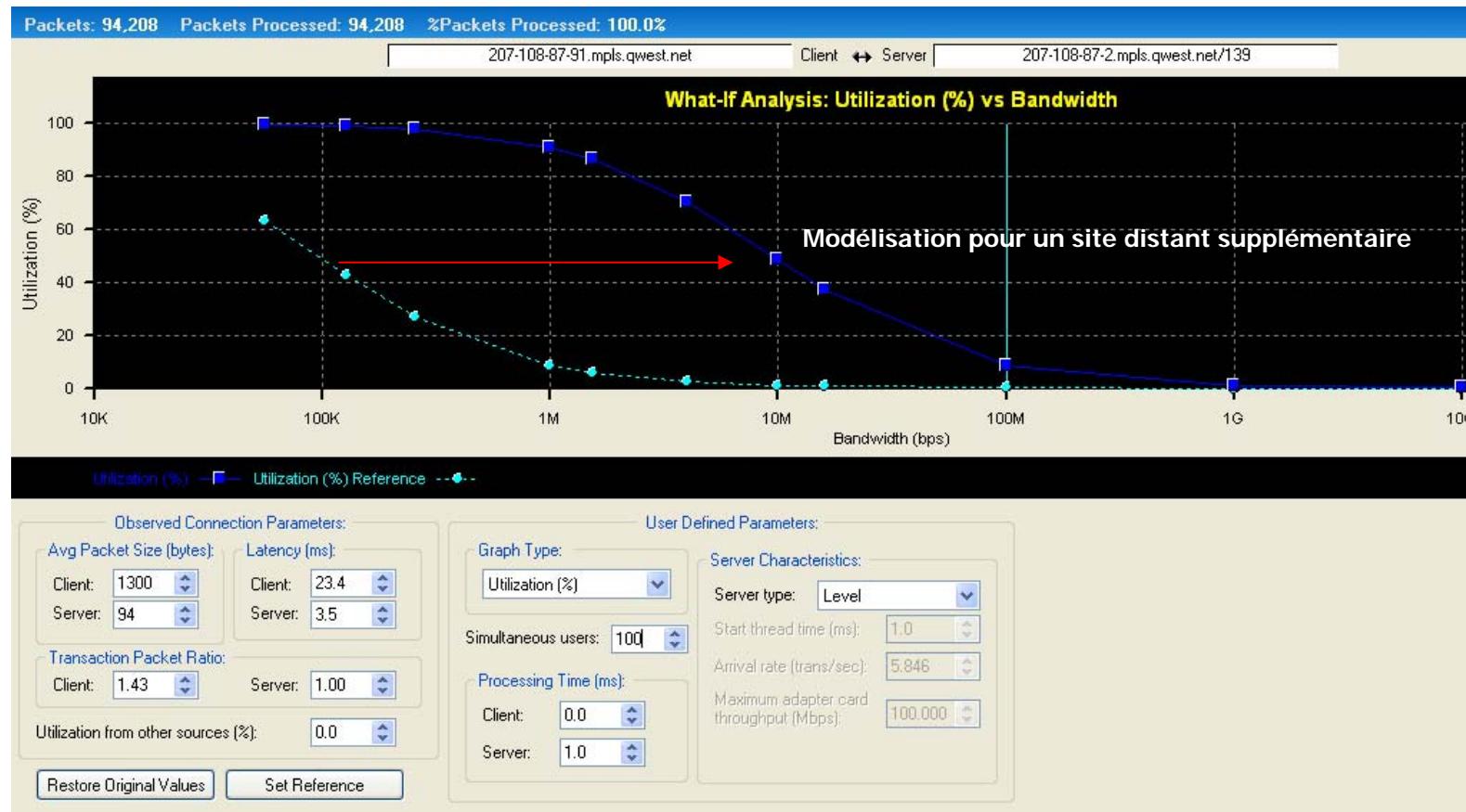


Temps de réponse Serveurs Métiers



Utilisation de la bande passante

Modélisation du trafic



Ajout d'un site et conséquence sur la bande passante et sur les temps de réponse des serveurs métiers

Vérification des niveaux de Cos / Labels

Suivi de la bande passante par Label.

- Quel est le site distant qui consomme le plus de ressources?
- Quelle est la quantité d'information qui circule par site distant?

MPLS Label	IP (by IP address)					
	Started: Thu Mar 01 16:06:37 MPLS Label: 109 Packets: 3749 Bytes: 705318 Filter: Not using filter				Packets	
MPLS Label	Rx	Tx	Total	%	/sec	Rx
2686	751	751	1502	20.032	25.46	58842
2882	602	602	1204	16.058	20.41	85361
2688	318	318	636	8.482	10.78	20701
55	122	122	244	3.254	4.14	27764
3773	99	99	198	2.641	3.36	6765
1447	84	84	168	2.241	2.85	5580
68	82	82	164	2.187	2.78	17324
2596	71	71	142	1.894	2.41	4980
482	67	67	134	1.787	2.27	6182
3370	56	56	112	1.494	1.90	27420
1150	51	51	102	1.360	1.73	41924
316	48	48	96	1.280	1.63	7235
835	48	48	96	1.280	1.63	11552
3597	47	47	94	1.254	1.59	27378
62	47	47	94	1.254	1.59	11670
1127	47	47	94	1.254	1.59	53077

Started: Thu Jun 28 13:58:47 Packets: 210 Bytes: 18,452 Protocol Entries: 15 Filter: Not using filters						
Protocol	Packets	%Packets	Bytes	%Bytes	%Util	
Protocols by CoS						
+ CoS 0	70	33.333	8,820	47.800	0.004	
+ CoS 5	140	66.667	9,632	52.200	0.004	

Suivi des applications et de leurs Cos respectives
Vérification de la SLA fournit par l'opérateur

Alerte lors d'un changement de Cos / Label



MPLS CoS
Trigger an alarm when the number of MPLS packets, matching the specified Class of Service (CoS), exceeds the defined limit within the specified interval.

MPLS CoS: 0 to 7
Operation: Between
 Minimum total matches:
 Matches/total packets (%):
Minimum total packets in analysis interval:
Analysis interval (sec): 10
 Analyze prefiltered packets only

MPLS Label
Trigger an alarm when the number of MPLS packets, matching the specified MPLS Label, exceeds the defined limit within the specified interval.

MPLS Label: 1 to 0
Operation: Greater than or equal to
 Minimum total matches: 1
 Matches/total packets (%): 80
Minimum total packets in analysis interval: 100
Analysis interval (sec): 60
 Analyze prefiltered packets only



MPLS Label List

Alias	MPLS Label
Site Russie	0
Site Angleterre	78
Site USA	83
Site Allemagne	89
Site Belgique	893

Select MPLS Label from Address List:

Alias	MPLS Label

Defined MPLS Labels:

Create New... Modify... OK Cancel

MPLS Unknown Label
Trigger when an unknown MPLS Label is observed that is not found in the defined list.
Defined MPLS Labels: 3
 Analyze prefiltered packets only

Alertes paramétrables lors d'un changement de Cos ou lorsque la SLA n'est pas respectée par l'opérateur

Alertes sur les Labels inconnus



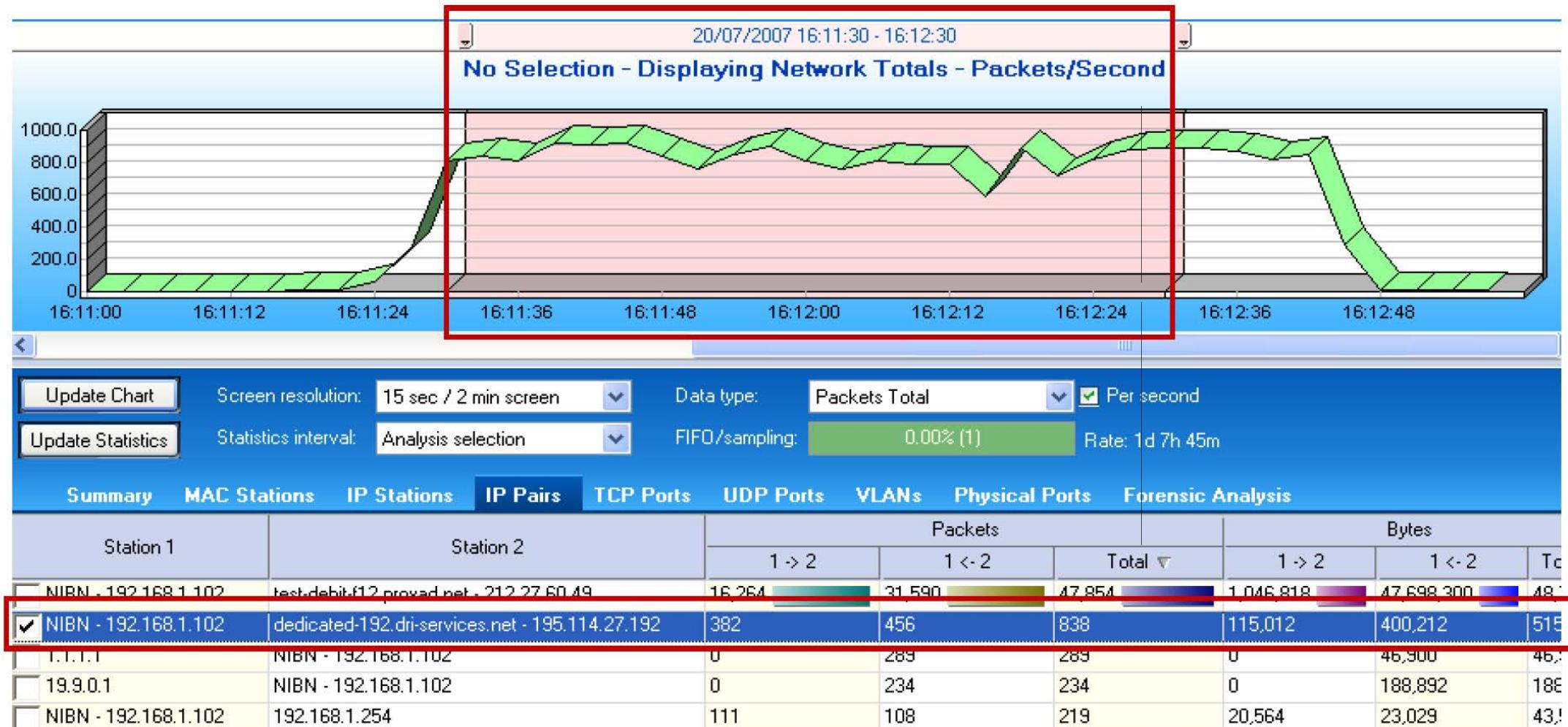
Exemple 5...

Traffic suspect d'un utilisateur...

- John est accusé de visiter des sites Web inappropriés pendant les heures de travail...
- Les méthodes traditionnelles permettent de suivre seulement les URL visitées.
- Les ressources humaines ont besoin d'un outils fournissant les preuves factuelles et les données échangées.

La solution : L'analyse Rétrospective et la possibilité de reconstruire le flux

Recherche de la période de temps et de la station



Observer Reconstruit le trafic

Click on a file link or the  icon below to view the reconstructed file:

```
Packet 132: 192.168.1.102:1079 --> 195.114.27.192:80
GET / HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-
fish, application/vnd.ms-
UA-CFU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR
0.50727; .NET CLR
Host: www.poker.fr
Connection: Keep-Alive
```

Packet 134: 195.114.27.192:80 --> 192.168.1.102:1079
HTTP/1.1 200 OK
Date: Fri, 20 Jul 2007 14:09:41 GMT
Server: Apache
Set-Cookie: PHPSESSID=wsheqp5h7hmetilico56q54bm3; path=/
Expires: Thu, 19 Nov 1981 05:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
Content-Language: fr

Packet 135: 195.114.27.192:80 --> 192.168.1.102:1079, more file data (TempFile.htm)...
 TempFile.htm (27837 bytes)
Preview file content:

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
```

Reconstruction de la page Web visitée

1 SYN (Connection requested) [S=1906302563, EA=1906302564, W=6553...]
2 SYN ACK (#1) [S=849497405, EA=849497406, A=1906302564, W=5840...]
3 ACK (#2) [S=1906302564, A=849497406, W=65535, P=1079]
4 Data (L=536) PSH ACK (#2) [S=1906302564, EA=1906303099, A=84949...]
HTTP GET http://www.poker.fr/
5 ACK (#4) [S=849497406, A=1906303099, W=6432, P=80]
6 Data (L=1452) ACK (#4) [S=849497406, EA=849498858, A=1906303099,...]
HTTP Reply Status=200 OK, Content-Type: text/html
7 Data (L=1452) ACK (#4) [S=849498858, EA=849500310, A=1906303099,...]
HTTP Data continuation from Pkt # 6 (Capture Pkt # 134)

Tout savoir sur le poker, venez découvrir ce jeu, ou partager votre passion : Règles, Photos, J - Windows Internet Explorer

POKER.FR

TOUTE L'ACTUALITÉ DU POKER

FPT LES PHOTOS EN LIGNE 20 Juillet 2007

Le France Poker Tour... Allez on en reparle ! Les photos de la finale sont enfin en ligne. C'est vraiment un bug de l'organisation. La prochaine fois, toute la France exigera en temps réel, des photos et des vidéos de cette finale qui vaut largement la finale de l'EPT...

Non bien mieux que l'EPT puisqu'il n'y avait que des français. Sur les photos on s'aperçoit Maxime qui a remporté cette finale, Rodolphe, un manceau est arrivé 8ème et Fabrice qui a signé des autographes, mais pas en temps que réalisateur de un gars une fille, non, non, en temps que joueur de poker reconnu et apprécié. Cela devrait donner à encore plus de joueurs l'envie de participer l'année prochaine. Ha oui j'oubiais, MERCI UNIBET...

Ce sont les joueurs qui paient

Les sièges EPT pour Barcelone ne sont pas payés par les pokerrooms pour les qualifiés. L'argent est directement versé

En savoir +

DE LA LUMIÈRE À LA CAGOULE

DISCOURS EST UN GUERRIER DU POKER QUI SE RAconte TRÈS BIEN. IL A UN POKER FACE QUASI PARFAITE SAUF lorsqu'un sourire pointé de qui signifie la fin du sérieux pour de longues min...

LE NOUVEAU CHAMPION DU



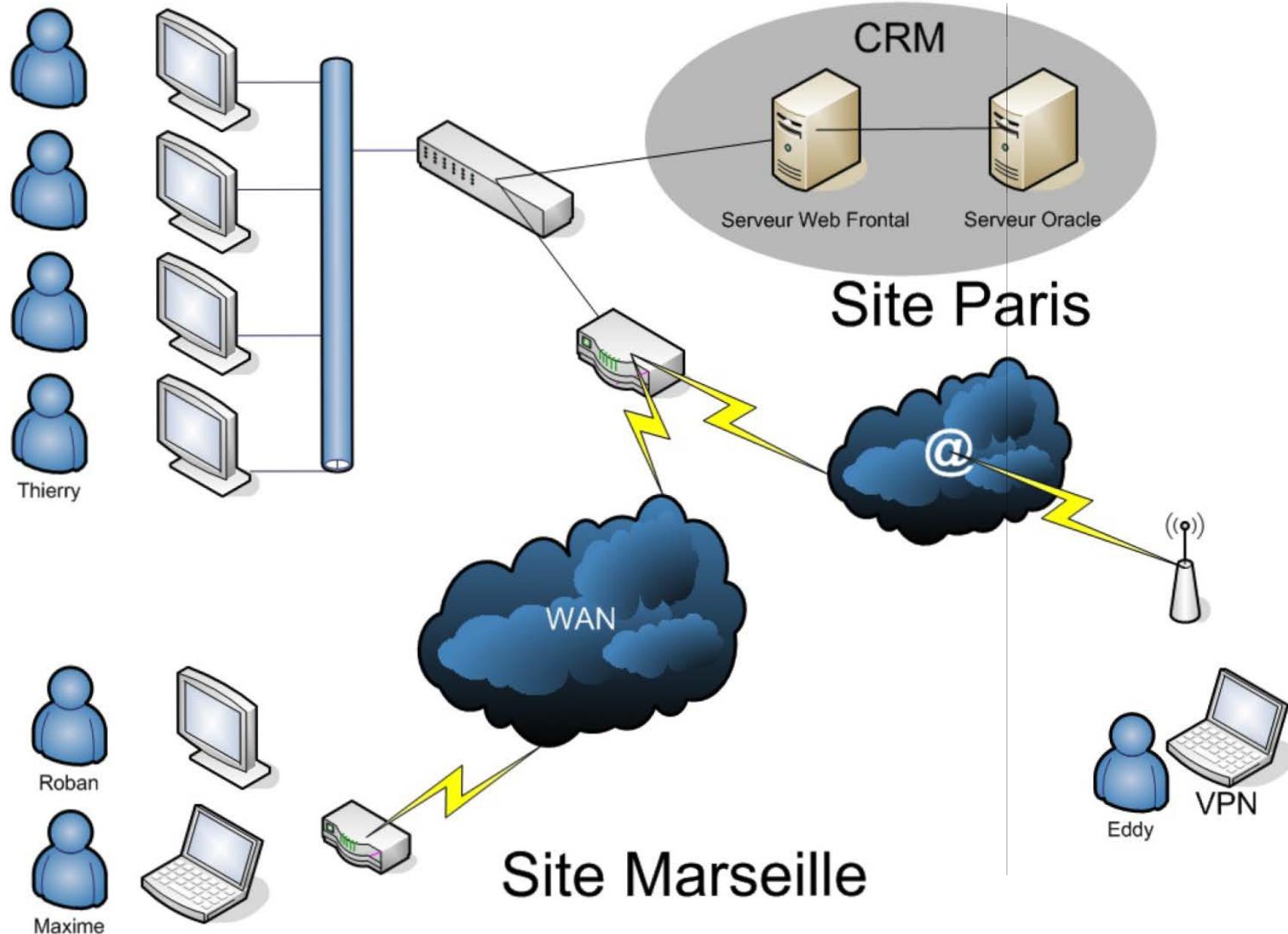
Exemple 6...

Attaque du réseau...

Pourquoi l'analyse Forensic?

- Le périmètre de défense peut être pénétré
- Les attaques internes sont très souvent négligées des systèmes de protection contre les menaces extérieures
- Un grand nombre des système de défense fonctionnent avec les vulnérabilités connues ou existantes, en oubliant les nouvelles attaques...

Utilisateur distant connecté via le VPN

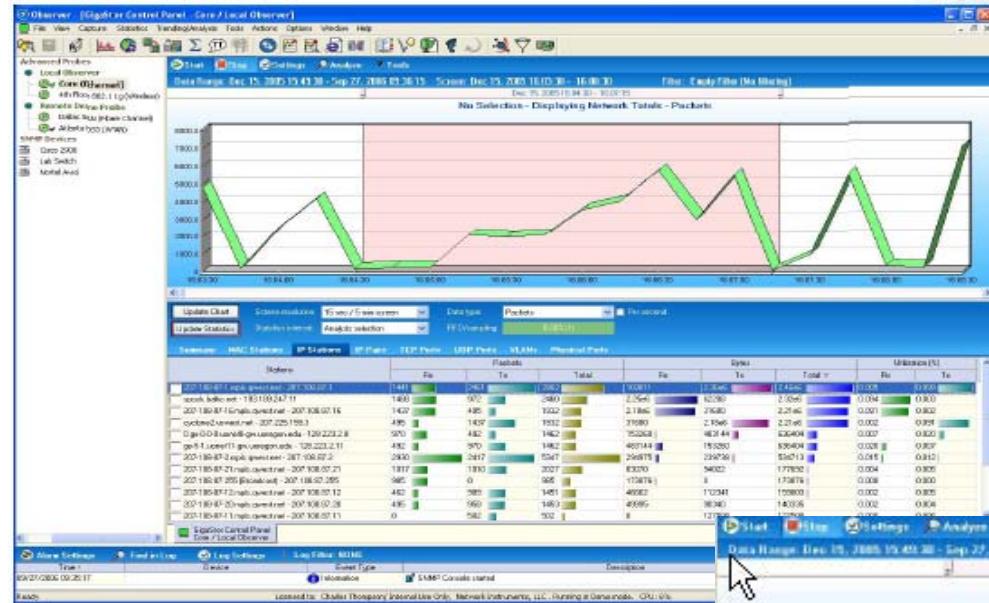


Eddy connecté en VPN via son accès WiFi à son domicile

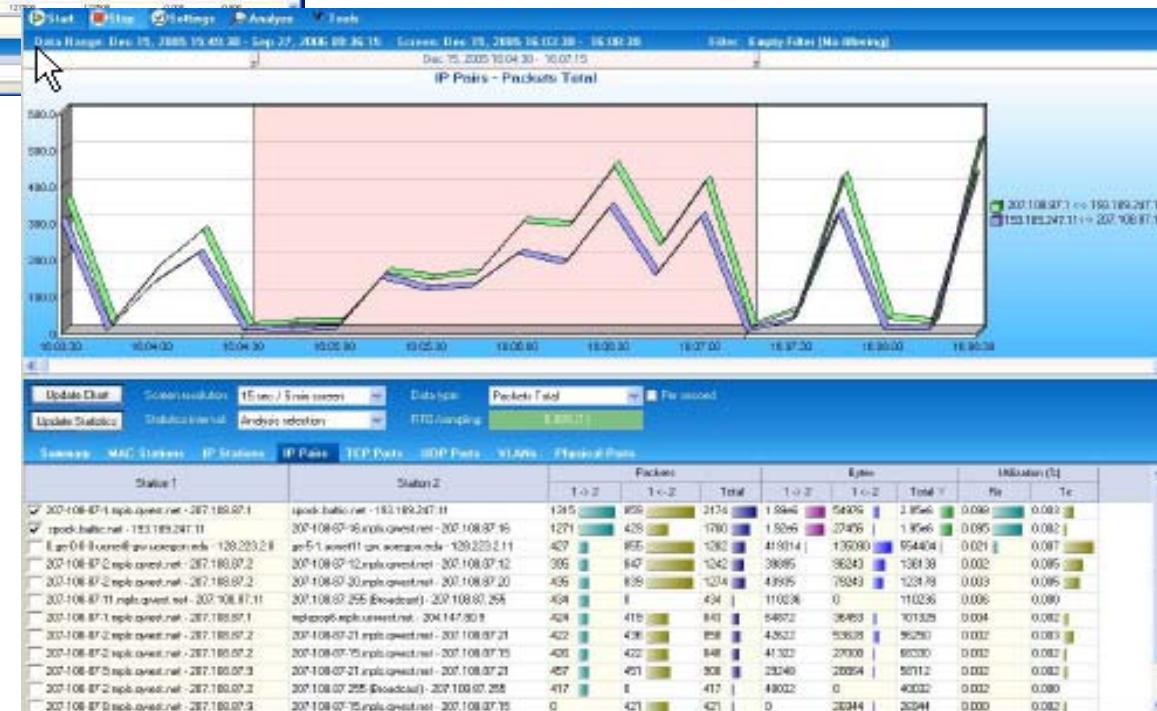
Scénario

- Eddy se connecte depuis son domicile pour voir ses courriels grâce au VPN de l'entreprise
- Il utilise un accès en WiFi avec une clé de chiffrement WEP de 128 bits...Quelques heures suffisent pour qu'une personne hack son réseau et récupère le mot de passe du VPN
- Le pirate obtient alors l'accès à toutes les ressources de l'entreprise.
- Les systèmes de protection existant ne détectent pas cette intrusion

Avec le Gigastor

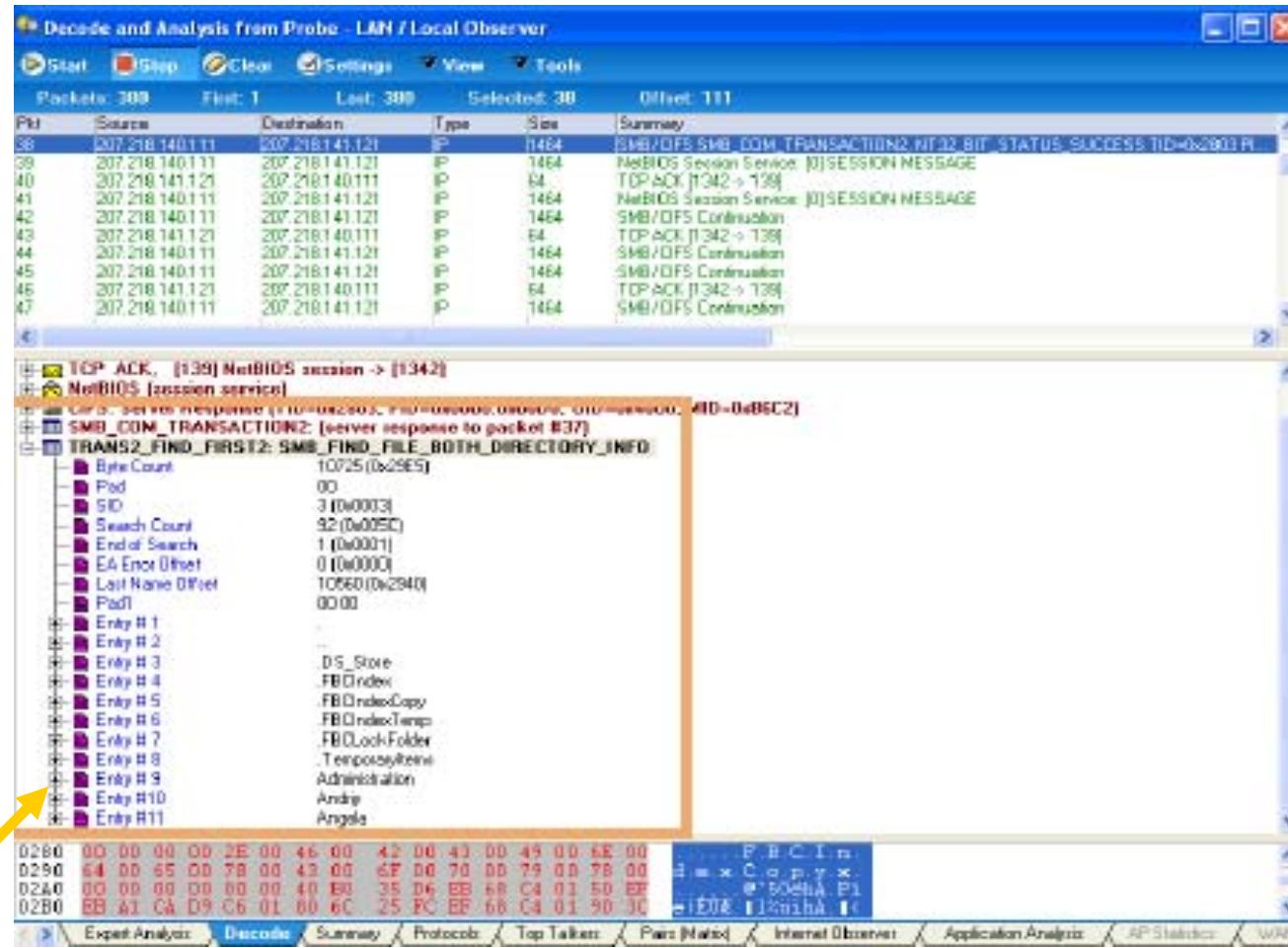


Identification du trafic anormal grâce au Baseline établi par le rapport



Le Graphique montre la déviation d'une utilisation normale vers un comportement suspect

Données lues et copiées par le pirate



Le pirate a accédé à la structure des répertoires d'un serveur Windows

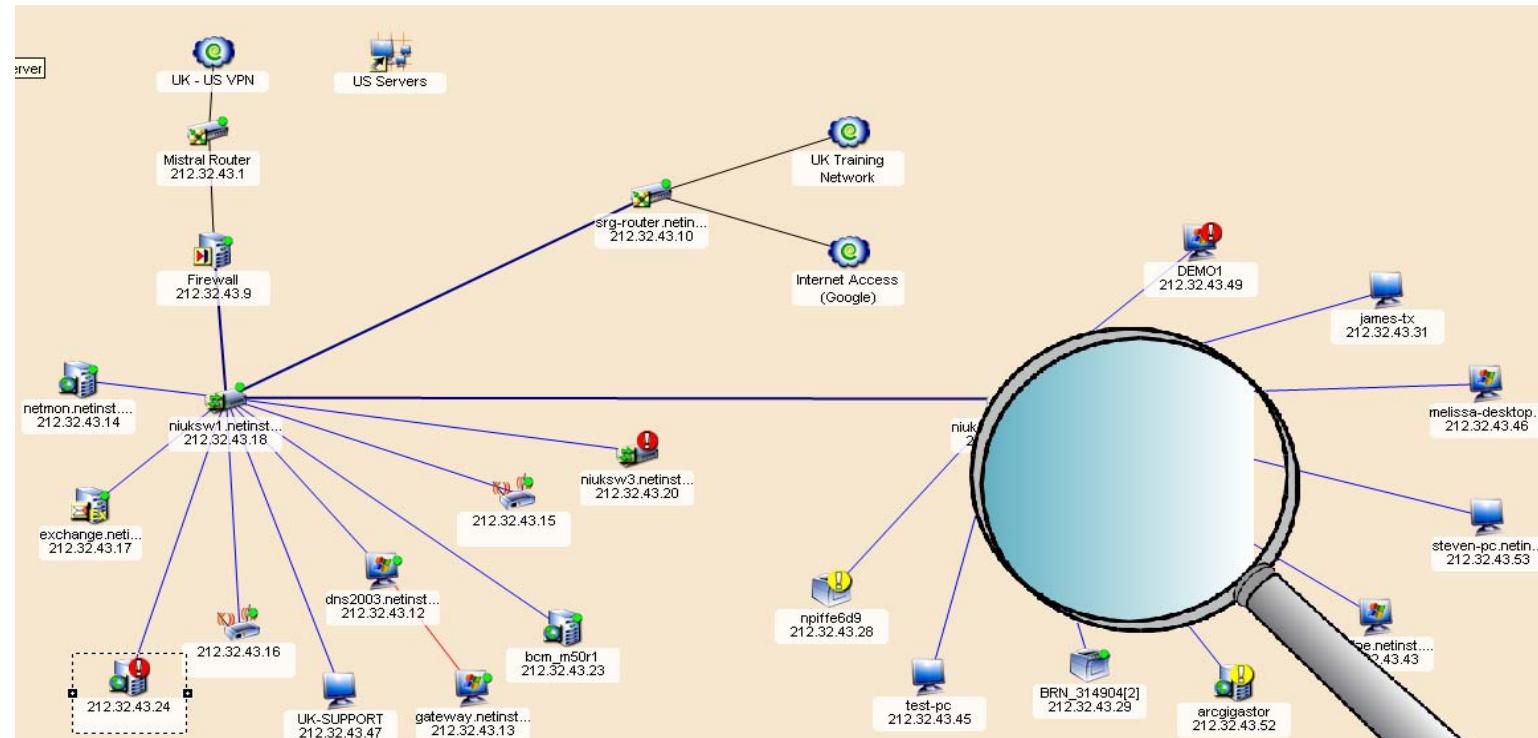
Identification de chaque fichier et commande effectuée par le pirate



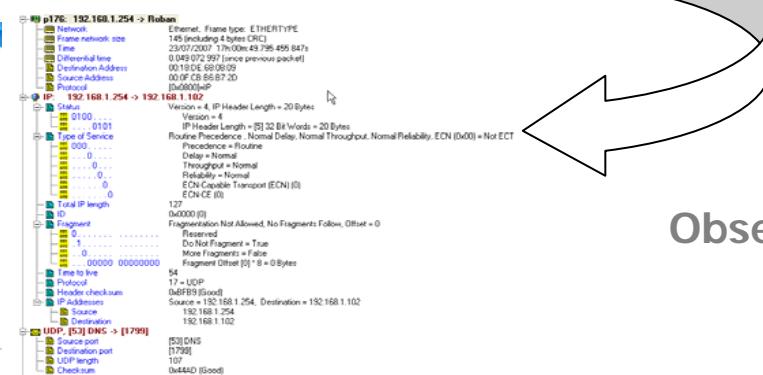
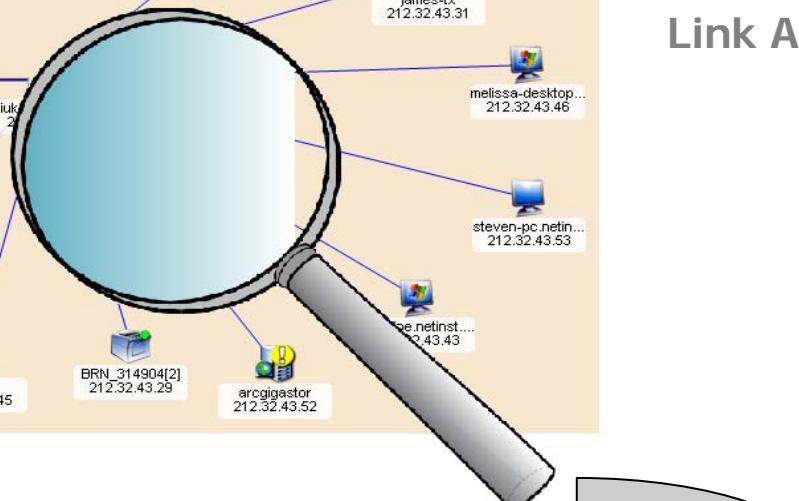
Exemple 6...

Approche Globale...

Méthode Contenant / Contenu



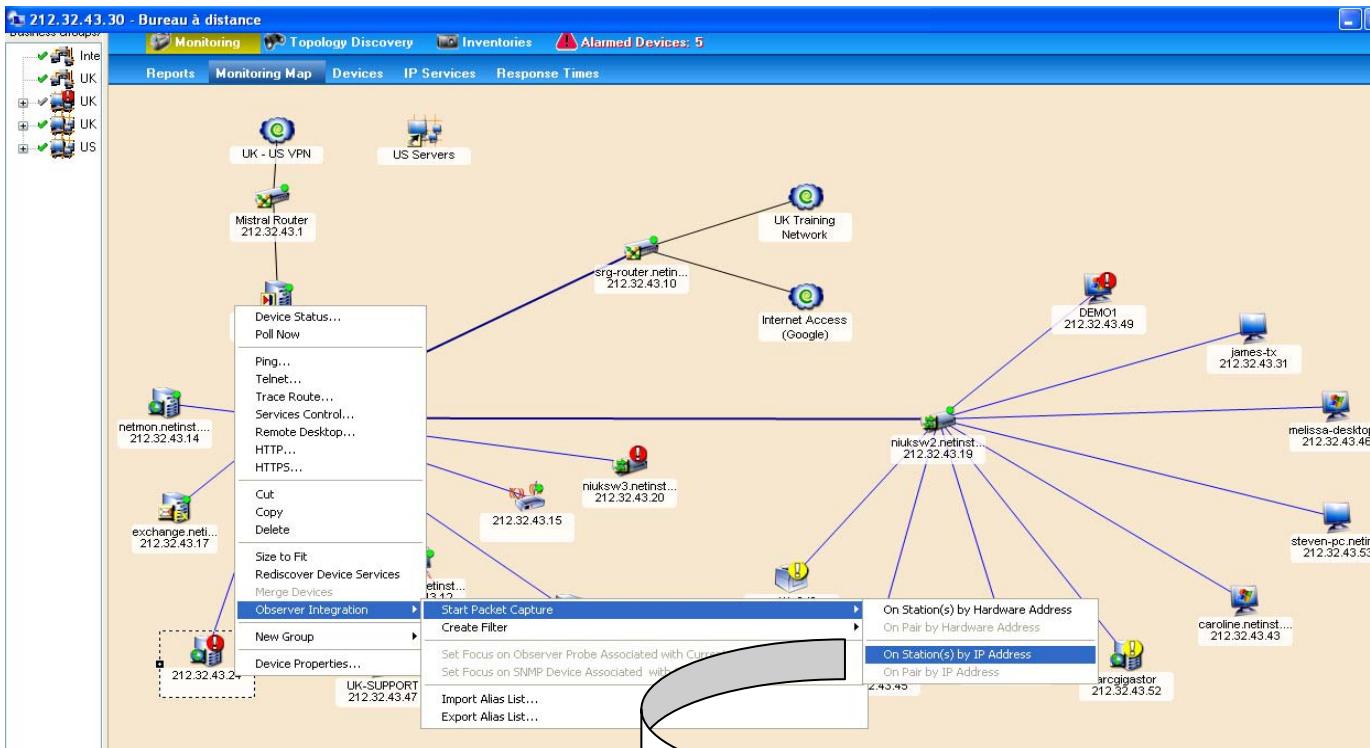
Link Analyst : Contenant



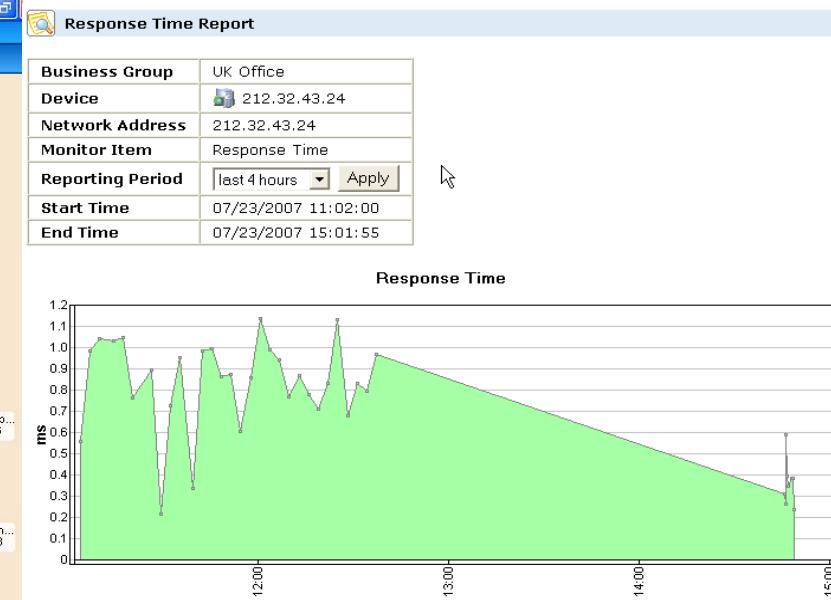
Observer : Contenu



Link Analyst : Cartographie / Supervision



Cartographie complète



Temps de réponse

Edit Filter <AND> <BRANCH> <OR> Toggle Include/Exclude

Filter name: Filtre automatique

Description:

Address - IP/Any
212.32.43.24 Any Address

OK Cancel Help

Intégration automatique avec Observer

Alarms Report

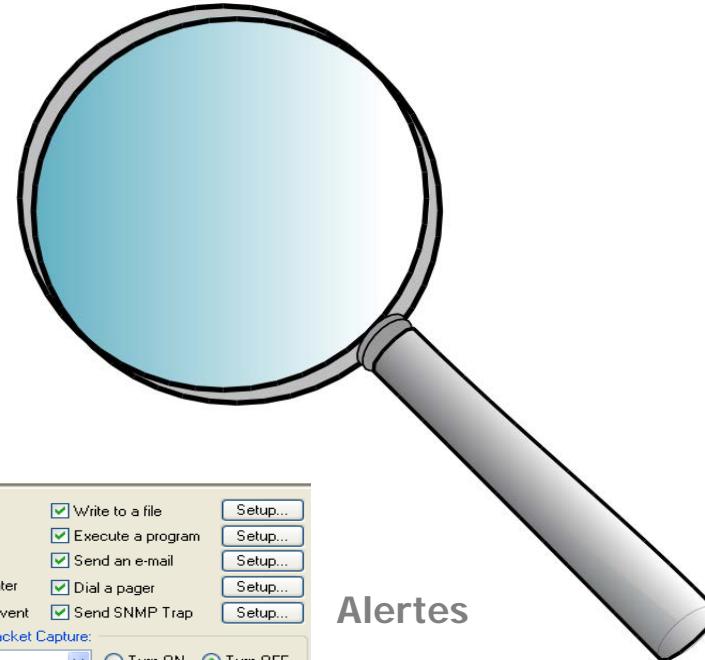
Business Group	UK Office
Report generated	07/23/2007 15:01:04
Last poll time	07/23/2007 14:48:06

Device ▲ (IP) Type Alarms

212.32.43.24	Web Server	IP Services down: HTTP
arcigastor (212.32.43.52)	Web Server	Device is down
DEMO1 (212.32.43.49)	Windows Workstation	IP Services down: HTTP
dns2003.netinst.co.uk (212.32.43.12)	Windows Workstation	Monitor alarms: System Processor Queue Length (21.000)
gateway.netinst.co.uk (212.32.43.13)	Windows Workstation	Monitor alarms: System Processor Queue Length (33.000)
niuksw3.netinst.co.uk (212.32.43.20)	Switch	Device is down IP Services down: HTTP, SNMP, TELNET ResponseTime: No response

Rapport d'alarmes

Observer : Monitoring / Alertes/ Analyse / rapportss



Alertes

Append to Event Log Write to a file

Pop up a message Execute a program

Sound a signal Send an e-mail

Print to the default Windows printer Dial a pager

Disable this alarm after the first event Send SNMP Trap

Execute Observer Statistics or Packet Capture:

Packet Capture Turn ON Turn OFF
of: 10 seconds

- None
- Activity Display
- Bandwidth Utilization
- Discover Network Names (Address Book)
- Efficiency History
- Errors by Station
- Ethernet Vital Signs and Collision Expert
- Internet Observer
- Packet Capture**
- Pair Statistics (Matrix)
- Protocol Distribution
- Router Observer
- Size Distribution Status
- Top Talkers Statistics
- Utilization History
- Web Observer

General Info Frame Types Ctrl. Frames Mgmt. F

Started: Thu Jan 11 12:33:43 Access Points: 4 Stations: 10

Access Points/Stations	Channel	Strength Avg	Quality Avg	Overall Avg
Linksys [17:32:D8]	6	6	12	1.0
Intel [4A:18:93]	6	0	0	0.0
Intel [55:CF:D9]	6	0	0	0.0
D-Link [99:E0:...]	6	0	0	0.0
Broadcast Destination [...]	---	0	0	0.0
Intel [4A:18:93]	---	10	18	1.0
Intel [55:CF:D9]	---	8	15	1.0
Proxim [47:B2:...]	36	17	29	6.0
00:18:DE:77:5...	---	12	21	1.0
Lu-U34-E9:201	---	0	0	0.0

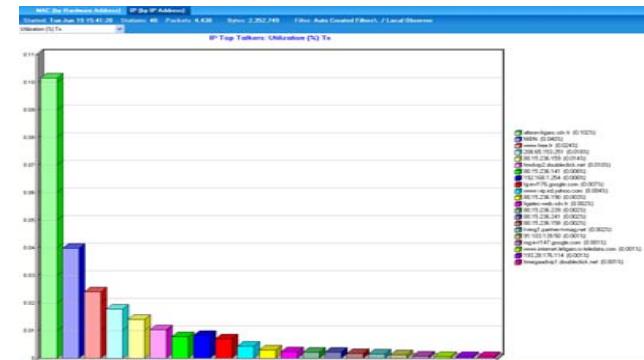
Site Survey WiFi

Network Conditions Summary

Problem	Count
Broadcast Storm	67
Ethernet Too Big errors (sec)	49
IPX excessive retransmissions	1
Multicast Storm	59
NetBIOS excessive retransmissions	2
NetBIOS slow response	1
TCP excessive retransmissions	7
Too fast TCP retransmissions	4
UDP excessive retransmissions	3
UDP slow response	2

Analyse Experte

Santé du réseau



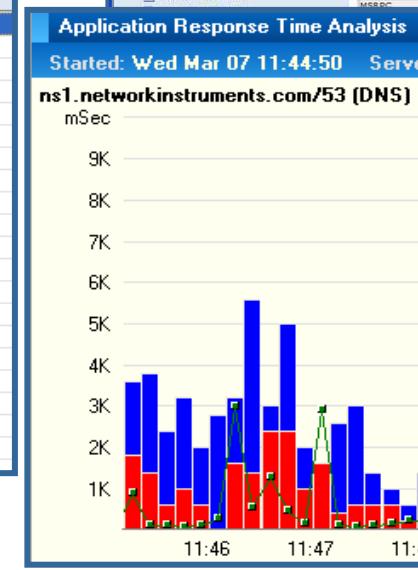
Détail des appels VoIP

Stop Clear Settings Expert Thresh

Packets: 94,208 Packets Processed: 94,208

VoIP Summary Calls RTP/RTCP Graph

ID / Stream	Station 1 / Port	Station ... / Port	Status
John Phillips - R...	10.74.162...
Call 14	10.74.162...
Call 15	10.74.162...
Jason Mauk, 20...	10.74.162...
Brett Messin...	10.64.13.1...	10.74.1...	...
SCCP	52569	2000	...
SCCP	52569	2000	...
SCCP	52939	2000	...
SCCP	52939	2000	...
Jason Mauk, 20...	10.64.13.1...	10.64.1...	...
RTP	17286	31356	...
RTP	17286	31356	...



rapport

Temps de réponse



Famille de Produits

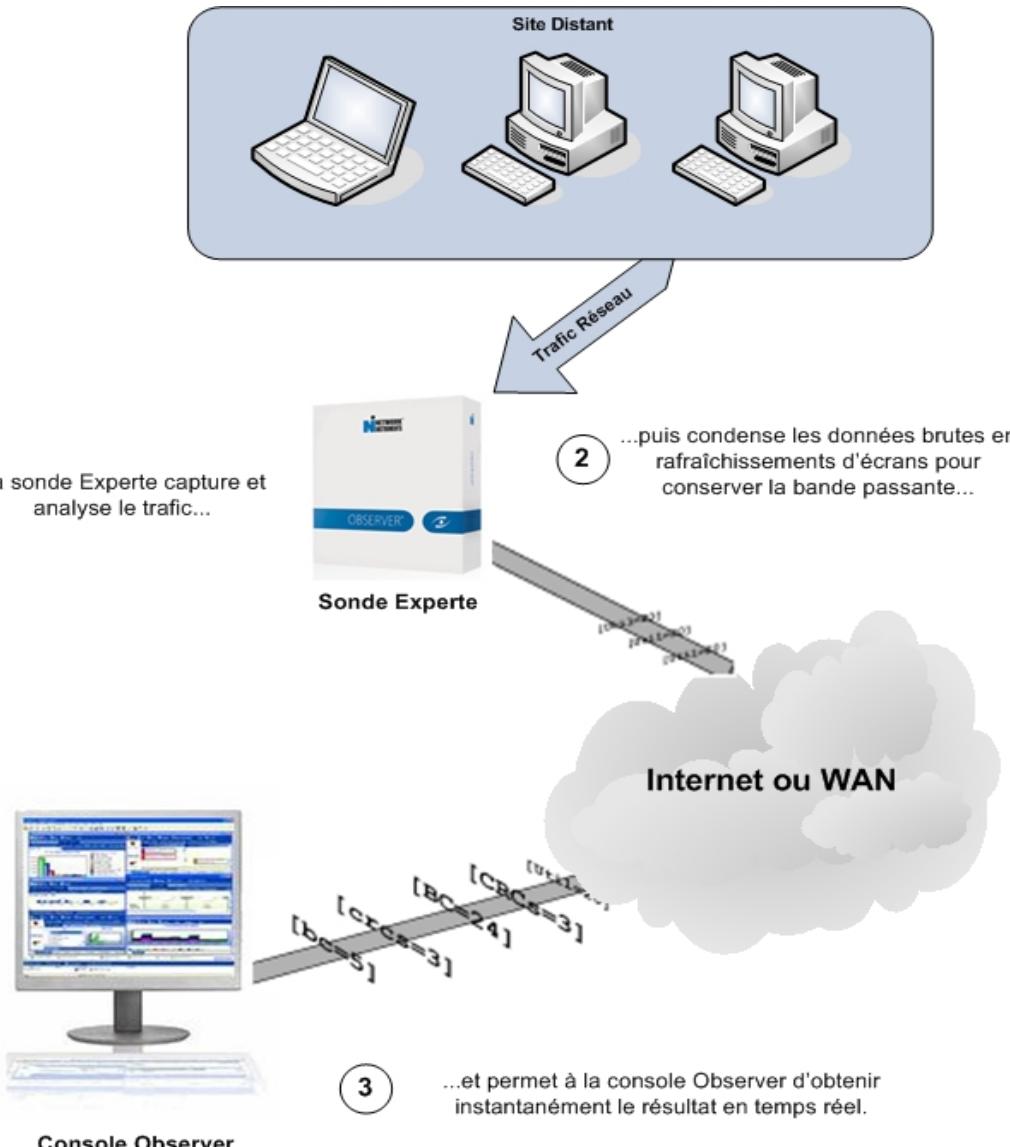
Console Observer



- SNMP, RMON, sFlow, NetFlow
- Analyse MPLS
- Statistiques Temps Réel
- Déclenchement d'Alarmes
- Capture / Décodage de Paquets
- +570 Évènements Experts
- Analyse Applicative
- Connexions Dynamiques
- Modélisation « What If »
- Analyse VoIP
- Rapports Web

enhanced VoIP support
OBSERVER®

Sonde logicielle Experte



- Analyse Experte en temps réel à distance
- Décodage à distance des trames
- Console locale pour analyse et administration
- Supporte toutes les topologies
- Standard avec les sondes Gigabit Full duplex et WAN

Les avantages de la sonde Gigabit

- Exécute l'analyse en local éliminant la nécessité de transférer les données vers la console
- Analyse du trafic en temps réel à distance sans arrêter la capture
- Carte de capture Gen2, choix entre 2, 4 ou 8 ports + Carte de management 10 /100 /1000
- *nTAPS cuivre ou optique inclus pour une visibilité en full-duplex*
- Technologie Experte embarquée
- Double processeur, 2GB de RAM, DD 250 Go, Graveur DVD
- Unité 64bit OS / Matériel
- Multi utilisateurs / multi sessions
- Plusieurs configurations possibles avec un Buffer de capture jusqu'à 124 Go

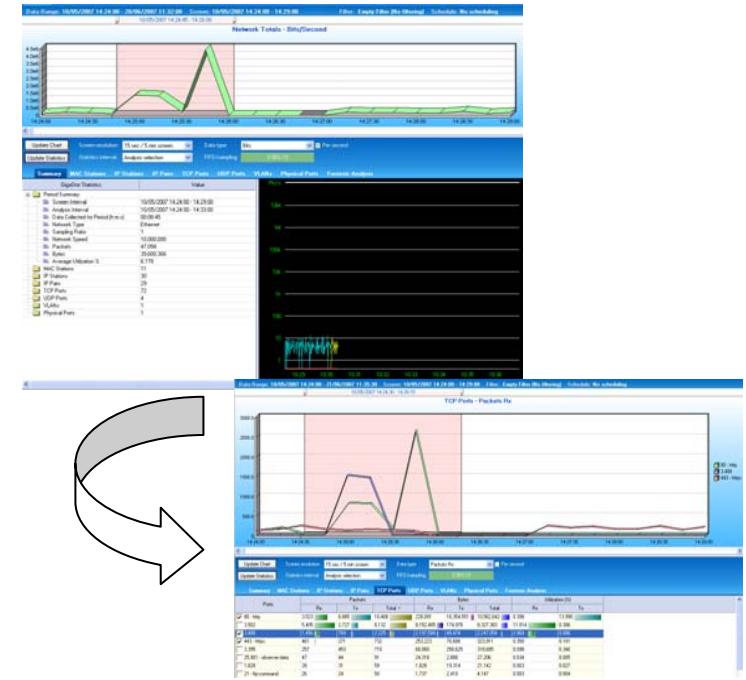


Sonde WAN, Gigabit, FC, 10 GbE



Les avantages de la sonde Gigastor

- Possibilité de remonter dans le temps
- Interface de navigation temporelle
- Exécute l'analyse **en local** éliminant la nécessité de transférer les données vers la console
- Reconstruit le flux de données collecté
- Enregistrement du trafic 24/7 avec des options de stockage entre 4 et 48 TéraOctets.
- Possibilité d'écriture sur SAN 1,2 ou 4 Gbits: capacité de stockage illimité
- Écriture sur disque à des vitesses à plus de 3,7 Gbits.
- Carte de capture Gen2, choix entre 2, 4 ou 8 ports + Carte de management 10 /100 /1000
- nTAPS cuivre ou optique inclus pour une visibilité en full-duplex
- Multi utilisateurs / multi sessions
- Technologie Experte embarquée
- Double processeur, 2GB de RAM, DD 250 Go, Graveur DVD
- Unité 64bit OS / Matériel



GigaStor pour Gigabit,
10 GbE, FC, et WAN

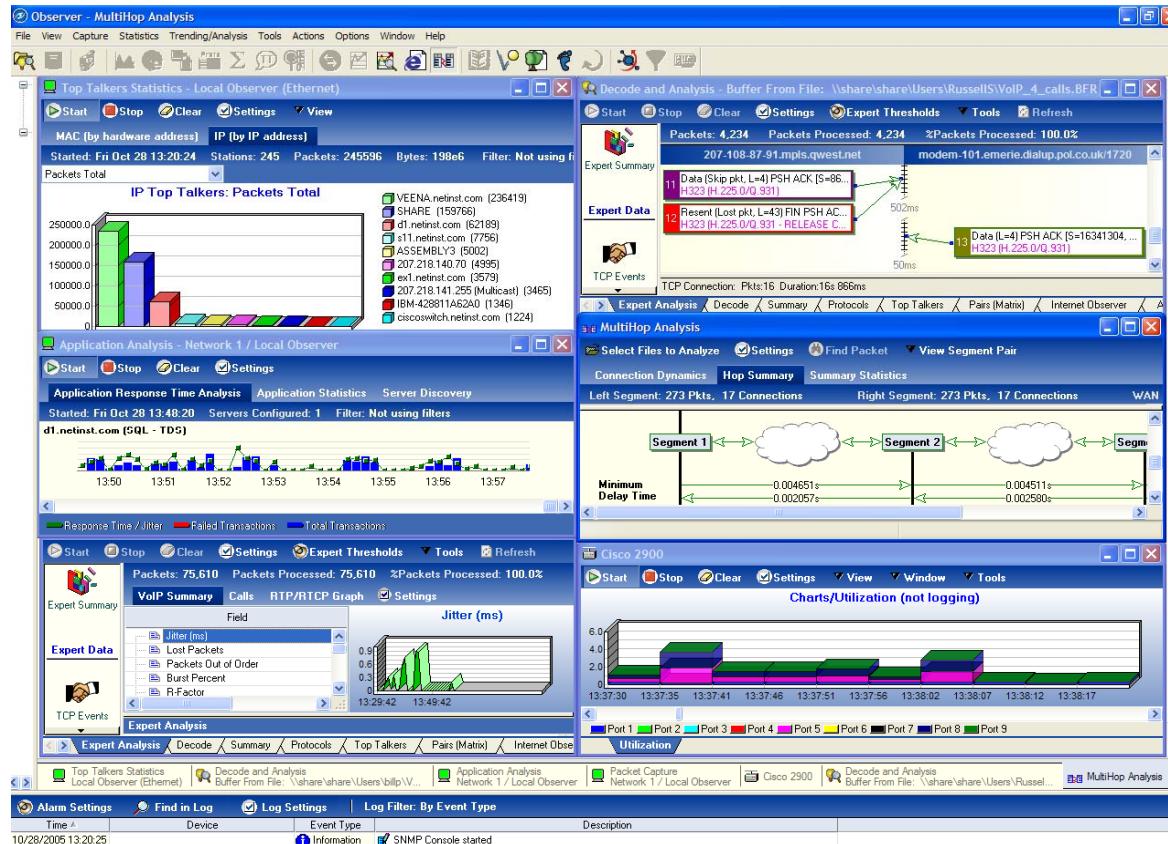
Gen2™
Powered By



Solution d'Analyse Réseau complète



Console Observer



Sonde
Logicielle



Sonde 10/100/1000



Sonde WAN, Gigabit, FC, 10 GbE



GigaStor pour Gigabit,
10 GbE, FC, et WAN



Système Portable
Gigabit, WAN, FC et 10 GbE



Gamme de nTAPS



nTAP 10/100/1000



nTAP SX / LX

nTAP 10/100/1000
convertisseur

Full-duplex

Aggrégateurs

nTAP Aggrégateur
256 / 512 Mo

Serveur
Routeur ...

A

◀1Gb ▶1Gb

1Gb

1Gb

1Gb

1Gb

Analyseur Full-duplex (2 ports)



B

Switch
Firewall ...

Serveur
Routeur ...

A

◀1Gb ▶1Gb

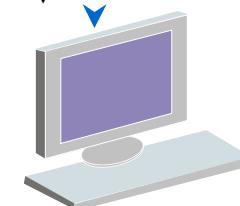
1Gb

1Gb

1Gb

1Gb

Analyseur Half-duplex (1 port)



B

Switch
Firewall ...

nTAPs élimine la possibilité de perte de paquets et erreurs couches basses

Gamme de produits

Observer Console

- Observer Expert
- Observer Suite

Sondes logicielles

- Multi
- Expert

Sondes Appliances

- 10/100/1000
- Wide Area Network (WAN)
- Full-duplex Gigabit
- Fibre Channel
- 10 Gigabit (GbE)
- GigaStor Gigabit, WAN, Fibre Channel, 10 GbE et Portable

Solutions Portables

- GOSS
- FOSS
- WOSS
- 10 GbE GOSS

Management des sondes

- Network Instruments Management Server (NIMS)

Supervision

- Link Analyst

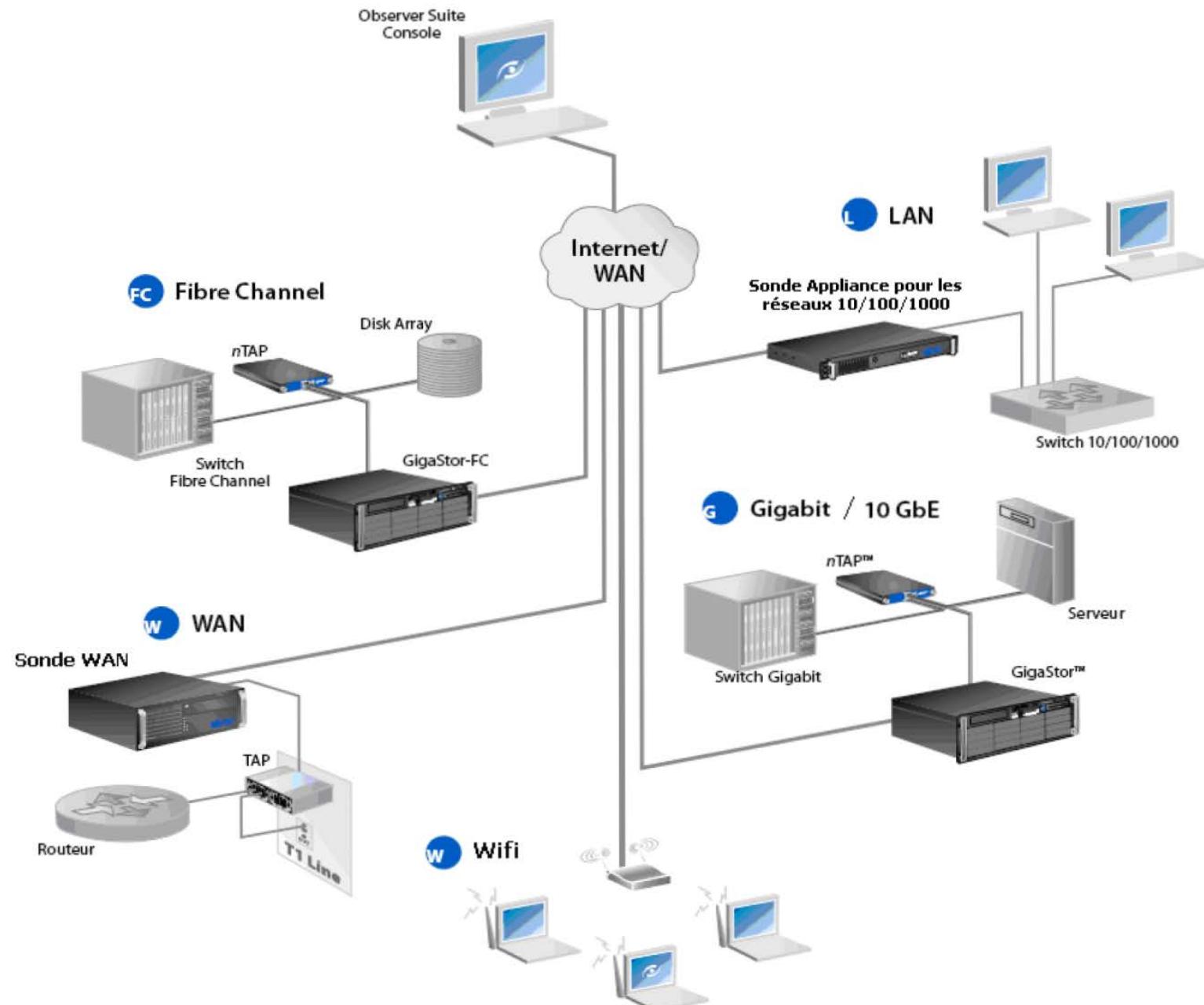
Serveur de rapports

- Observer Reporting Server

nTAPs

- Cuivre
- Optique
- Convertisseur
- Aggrégateur

Placement des sondes



Nos Formations

Introduction à Observer (1 Jour)

Grâce à ce cours, chaque participant apprend les compétences élémentaires de la gestion réseau avec le logiciel d'analyse réseau Observer. Optimiser votre investissement dans la solution Observer en apprenant à résoudre les problèmes liés au trafic et à surveiller et améliorer les performances du réseau.

Suite à cette session, les participants auront appris à :

- Découvrir les problèmes réseaux courants et la méthode pour les résoudre
- Comprendre les spécifications d'un réseau, les principes et les composants du réseau physique
- Comprendre comment utiliser un analyseur de protocoles en environnement commuté, Fast Ethernet et Gigabit Ethernet
- Installer et configurer la console Observer et les sondes avancées
- Diagnostiquer un réseau par l'analyse au niveau du décodage de trames et en utilisant les fonctions SNMP

Formation Observer Avancée ** (2 Jours)

Passez à la vitesse supérieure avec la formation avancée. Découvrez en détail les fonctionnalités d'Observer et notamment le module SNMP, l'analyse experte, les filtres et bien d'autres.

Suite à cette session, les participants auront appris à :

- Utiliser les techniques de filtrage du trafic pour résoudre plus rapidement les problèmes réseau
- Mettre en évidence les problèmes les plus complexes grâce à l'analyse experte en temps réel ou post-capture
- Reconnaître les différences entre les problèmes liés au réseau et ceux liés aux couches supérieures (jusqu'au niveau applicatif)
- Déterminer une approche sûre pour la résolution de problèmes réseaux grâce à une bonne compréhension des concepts définissant l'environnement
- Surveiller les équipements SNMP quelle que soit leur position sur le réseau
- Surveiller et mettre en place des alertes basées sur des « traps » SNMP
- Partager vos analyses avec des graphiques, tableaux et rapports d'activités sur mesure
- Comprendre les techniques de switch scripting

** pré requis: Introduction à Observer.

