Programme
Opérations de registre avancées

NetFlow

Sommaire

- Netflow
  - qu'est-ce que Netflow ? Comment fonctionne-t-il ?
  - utilisations et applications
- Configurations et mises en oeuvre fournisseur
  - Cisco
- Outils NetFlow tools
  - problèmes d'architecture
  - logiciels, outils, etc.

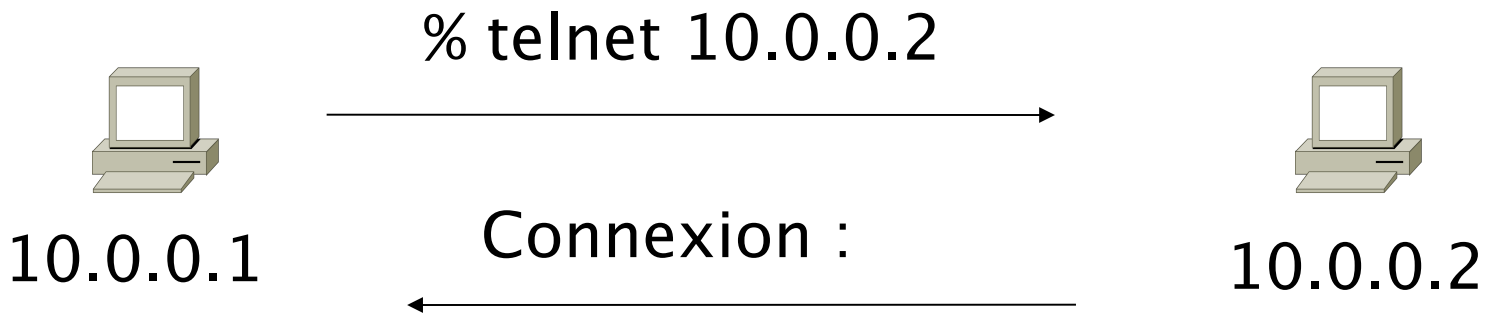
Qu'entend-on par flux de réseau ?

- Des paquets ou des trames présentant un attribut commun.
- Une politique de création et d'expiration –conditions de démarrage et d'arrêt d'un flux.
- Des compteurs – paquets, octets, temps.
- Des informations d'acheminement – AS, masque de réseau, interfaces.

Flux de réseau...

- Unidirectionnels ou bidirectionnels.
- Les flux bidirectionnels peuvent contenir d'autres informations telles que le temps "aller-retour" des paquets (RTT, *Round Trip Time*), le comportement TCP.
- Les flux d'application regardent au-delà des en-têtes afin de classifier les paquets en fonction de leur contenu.
- Flux agrégés – flux de flux.

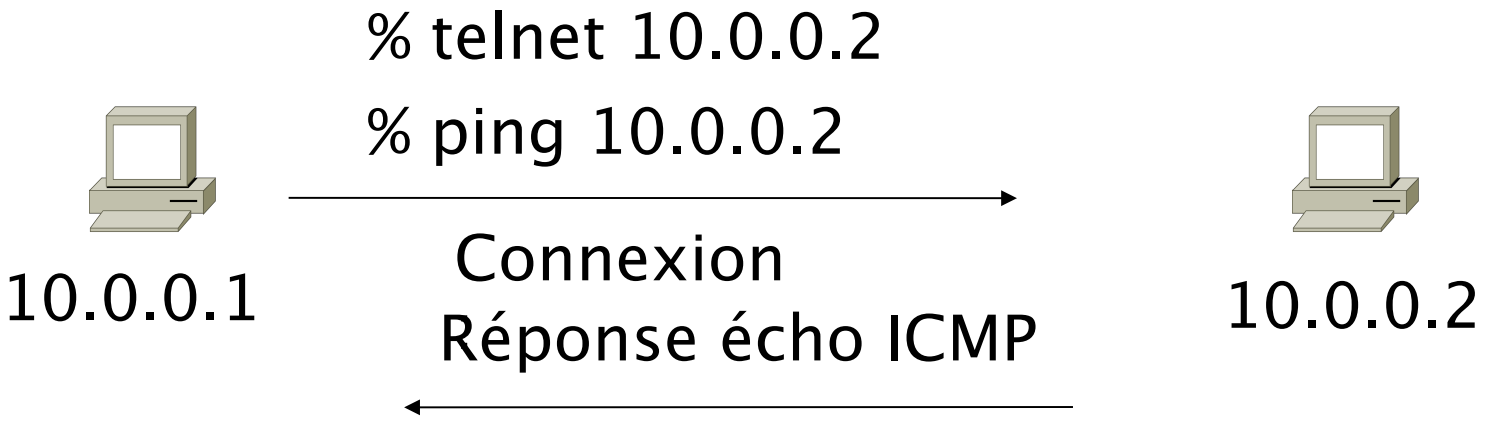
Flux unidirectionnel avec clé IP source/destination



Flux actifs

Flux	IP source	IP destination
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

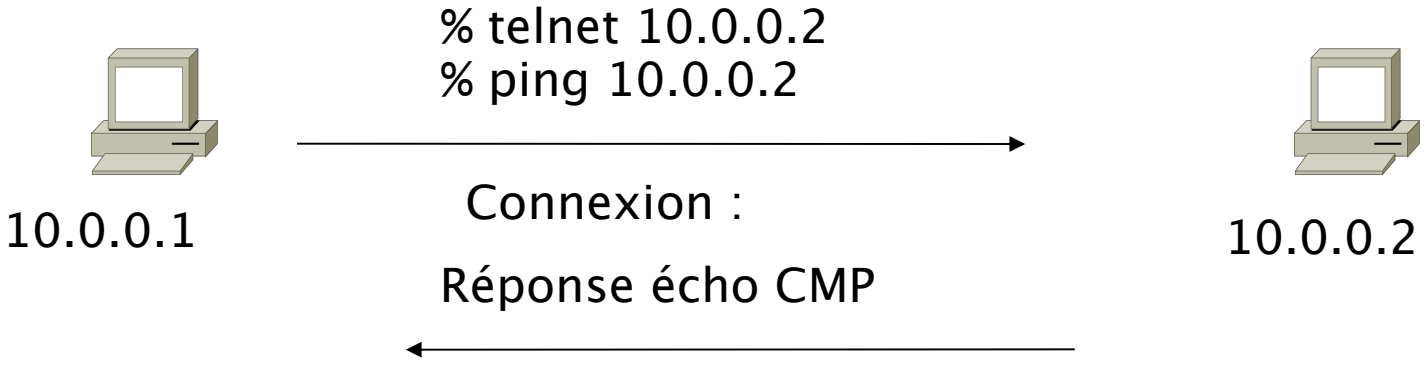
Flux unidirectionnel avec clé IP source/destination



Flux actifs

Flux	IP source	IP destination
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

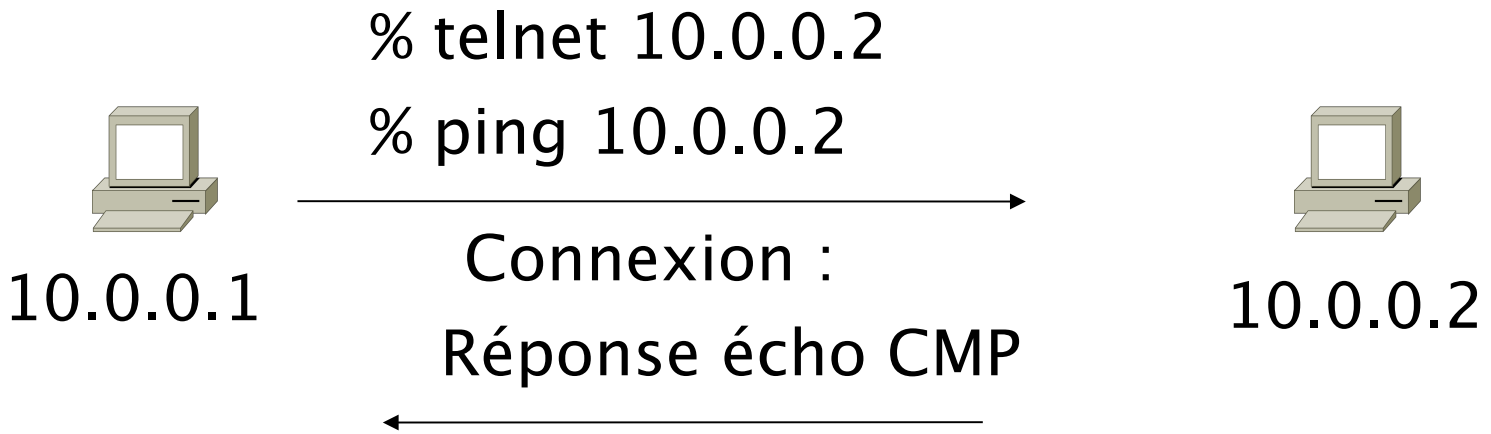
Flux unidirectionnel avec clé IP, port, protocole



Flux actifs

Flux	IP source	IP destination	prot	PortSrc	PortDest
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Flux bidirectionnel avec clé IP, port, protocole



Flux actifs

Flux	IP source	IP destination	prot	Portsrc	tPortdst
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.1	10.0.0.2	ICMP	0	0

Flux d'application

Flux actifs

Flux	IP source	IP destination	Application
1	10.0.0.1	10.0.0.2	HTTP

Flux agrégé

Table de flux actif principale

Flux	IP	IP destination	prot	Portsrc	Portdst
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

IP source/destination – agrégé

Flux	IP source	IP destination
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Travailler avec les flux

- Génération et affichage des flux
- Exportation de flux à partir de périphériques
  - types de flux
  - taux d'échantillonnage
- Collecte
  - outils de collecte de flux
- Analyse
  - utiliser les outils existants ou en créer

Descripteurs de flux

- Plus la clé comporte d'éléments plus elle génère de flux.
- Un nombre supérieur de flux induit plus de temps de post-traitement pour produire les rapports, plus de mémoire et de capacité d'UC pour les équipements générateurs de flux.
- Dépendant de l'application. Ingénierie du trafic ou détection des intrusions.

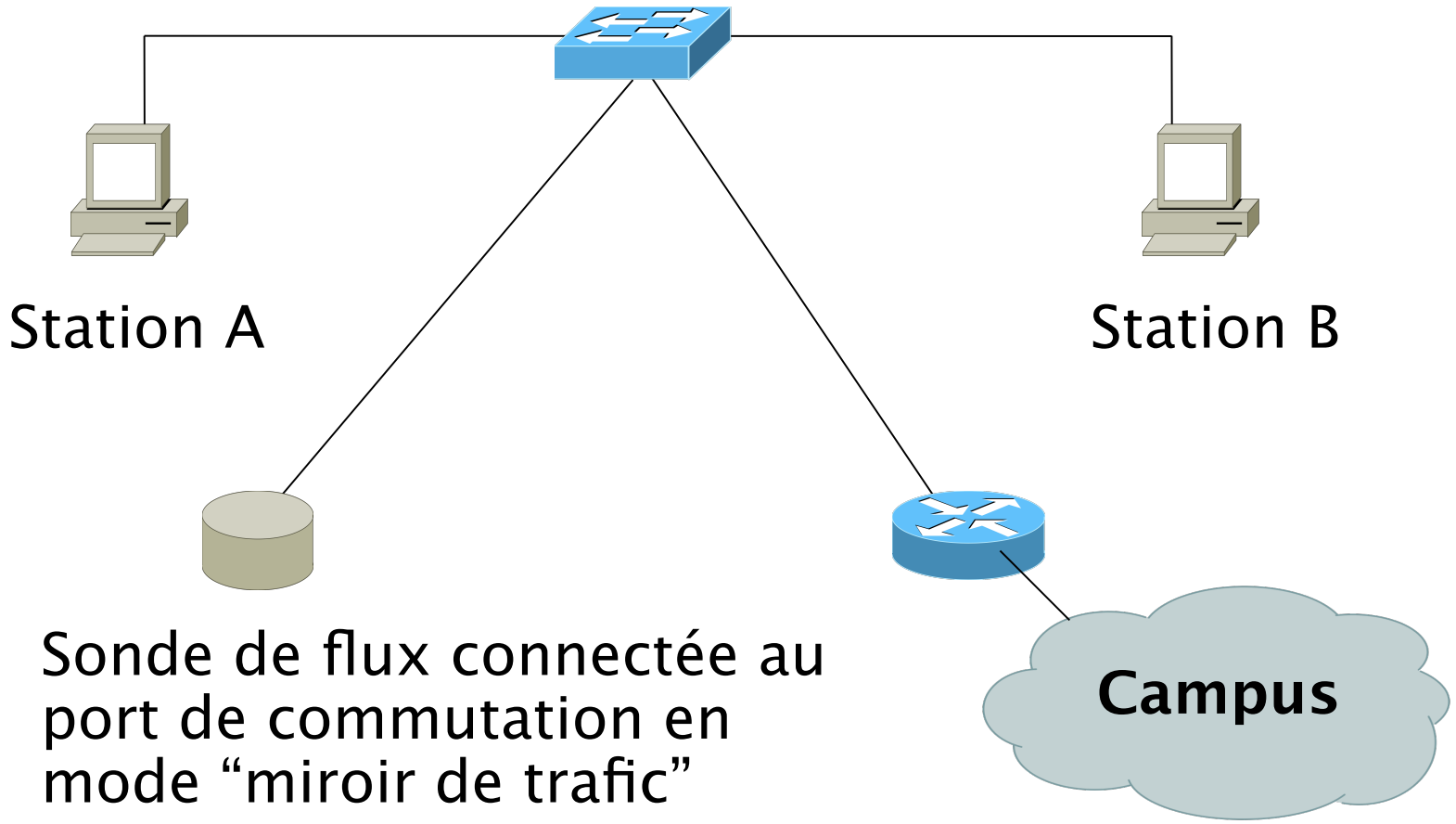
Comptabilisation des flux

- Informations de comptabilisation accumulées avec les flux.
- Paquets, octets, temps de démarrage/ d'arrêt.
- Informations d'acheminement de réseau – masques et nombre de systèmes autonomes.

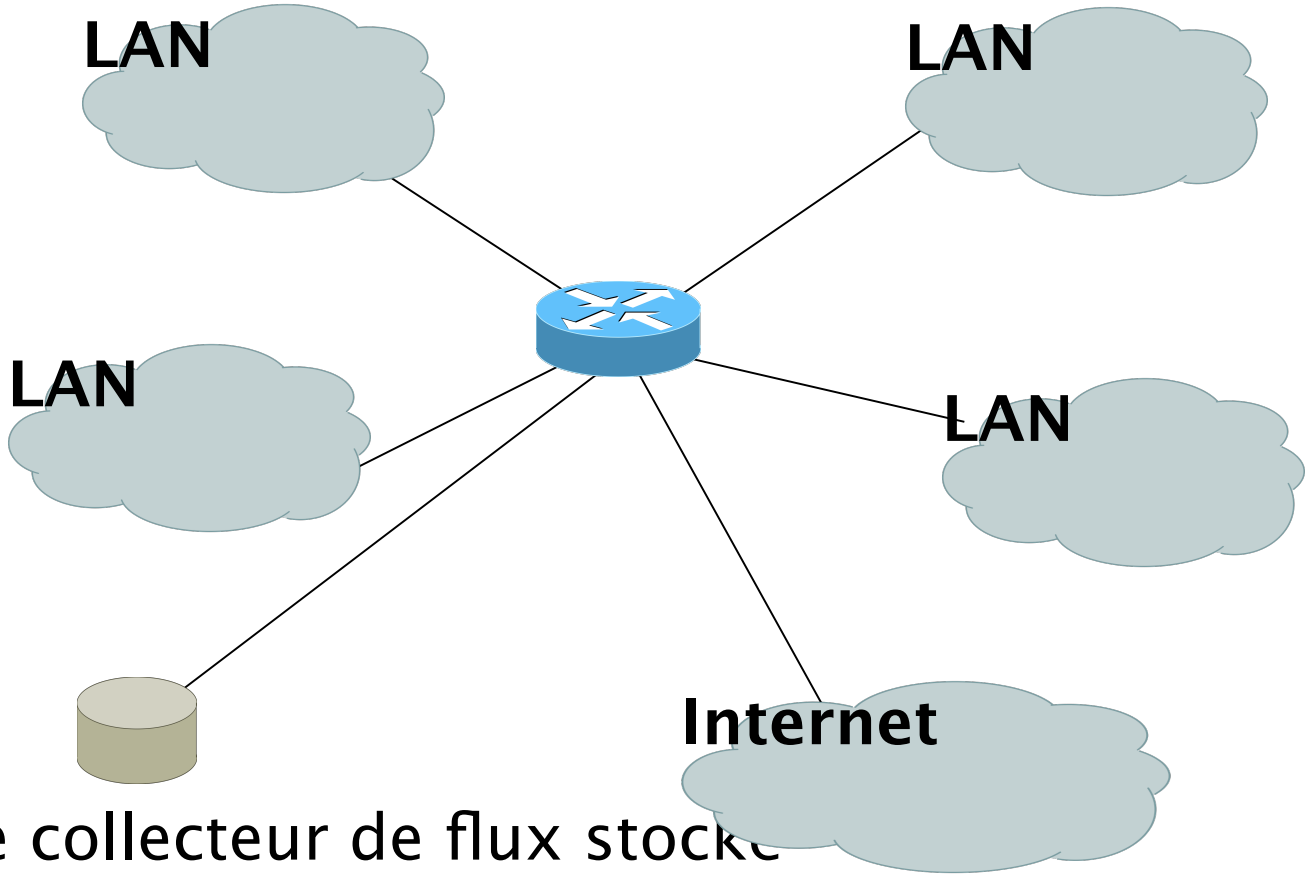
Génération/collecte de flux

- Equipement passif :
  - un équipement passif (généralement un hôte unix) reçoit l'ensemble des données et génère les flux.
  - gourmand en ressources ; nouveaux investissements.
- Routeur ou autre périphérique existant du réseau :
  - génération des flux par un routeur ou d'autres équipements existants tels que commutateur
  - possibilités d'échantillonage
  - pas d'investissements en nouveaux équipements.

Collecte par un équipement passif



Collecte par un routeur



Le collecteur de flux stocke
les flux exportés du routeur.

Equipement passif

- Directement connecté à un segment LAN par un port de commutation en mode "miroir", séparateur optique ou segment répété.
- Génère des flux pour l'ensemble du trafic LAN local.
- Doit disposer d'une interface ou d'un moniteur sur chaque segment LAN.
- Support de flux plus détaillés – bidirectionnel et application.

Collecte par un routeur

- Le routeur génère des flux pour le trafic dirigé vers le routeur.
- Les flux ne sont pas générés pour le trafic LAN local.
- Limité à des critères de flux “simples” (en-têtes de paquets).
- Généralement plus facile à déployer – pas de nouveaux équipements.

Mises en oeuvre vendeurs

NetFlow Cisco

- Flux unidirectionnels
- IPv4 *unicast* et *multicast*
- Agrégé et non agrégé
- Flux exportés par UDP
- Supporté sur platesformes IOS et CatOS
- NetFlow Catalyst diffère de IOS.

Versions NetFlow Cisco

- 4 types non agrégés (1,5,6,7).
- 14 types agrégés (8.x, 9).
- Chaque version se caractérise par son propre format de paquets
- La version 1 ne comporte pas de numéros de séquence – aucun moyen de détecter les flux perdus
- La “version” détermine le type de données du flux
- Certaines versions sont propres à la plateforme Catalyst.

NetFlow v1

- Champs clé : IP source/destination, port source/destination, protocole IP, ToS, interface d'entrée.
- Comptabilisation : paquets, octets, temps de démarrage/fin, interface de sortie.
- Autre : opérations OR sur les bits de drapeaux TCP.

NetFlow v5

- Champs clé : IP source/destination, port source/destination, protocole IP, ToS, interface d'entrée.
- Comptabilisation : paquets, octets, temps de démarrage/fin, interface de sortie.
- Autres : opérations OR sur les bits de drapeaux TCP, AS source/destination et masque IP
- Le format de paquets ajoute des numéros séquentiels permettant de détecter les paquets exportés perdus.

NetFlow v8

- Flux v5 agrégés
- Certains types de flux ne sont pas disponibles sur tous les équipements.
- Beaucoup moins de données en post-traitement, mais perte de la granularité fine de la version 5 – pas d'adresses IP.

NetFlow v8

- AS
- Protocole/port
- Préfixe source
- Préfixe de destination
- Préfixe
- Destination
- Source/destination
- Flux complet

NetFlow v8

- ToS/AS
- ToS/Protocole/Port
- ToS/préfixe source
- ToS/préfixe de destination
- Tos/préfixe source/destination
- ToS/Préfixe/port

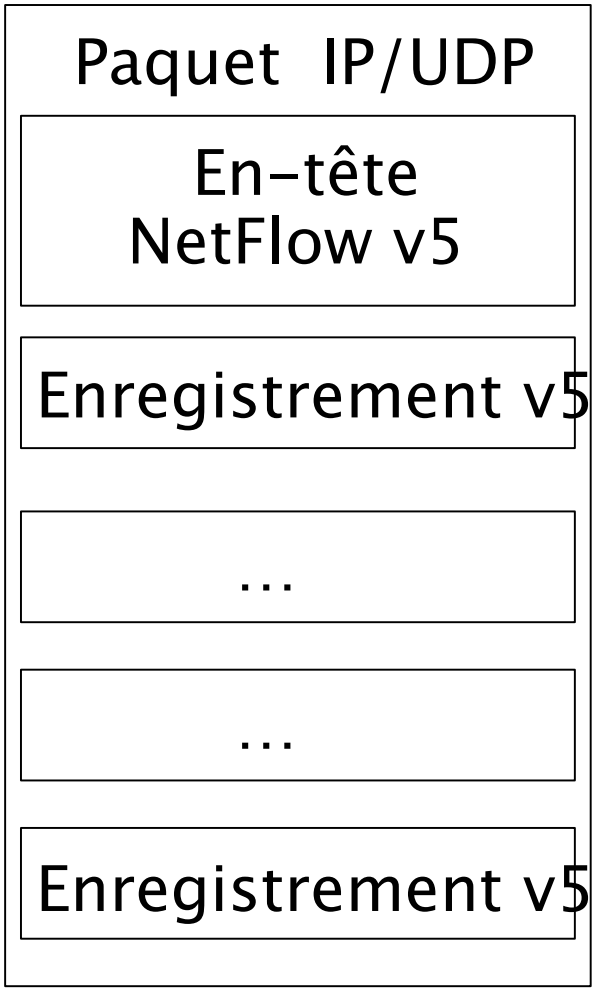
NetFlow v9

- Formats d'enregistrement définis par des modèles
- Le descriptif des modèles est communiqué par le routeur au moteur de collecte NetFlow.
- Les enregistrements de flux sont envoyés du routeur au moteur de collecte NetFlow avec un minimum d'informations de modèle permettant au moteur de collecte NetFlow de faire le lien entre les enregistements et le modèle approprié.
- La version 9 est indépendante du transport sous-jacent (UDP, TCP, SCTP, etc).

Format de paquets NetFlow

- En-tête commun parmi les versions d'export.
- Toutes les versions hormis la v1 assurent la numérotation séquentielle des paquets.
- Champ de données propre à la version prévoyant l'exportation de N enregistrements de types de données
- N est déterminé par la taille de la définition de flux. La taille des paquets est inférieure à ~1480 octets. Aucune fragmentation sur Ethernet.

Exemple de paquets NetFlow v5



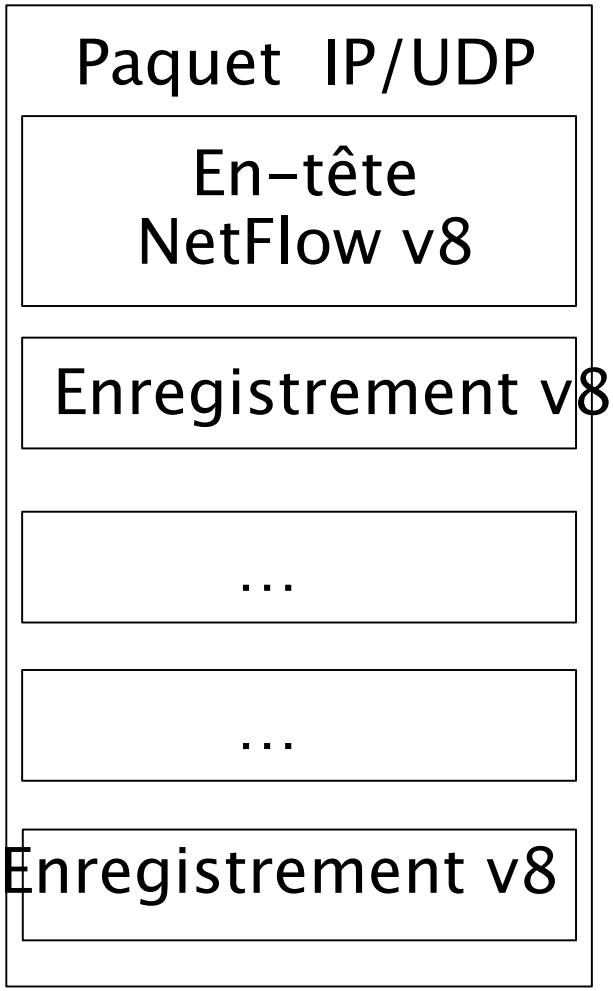
Paquet NetFlow v5 (en-tête)

```
struct ftpdu_v5 {
  /* 24 byte header */
  u_int16 version;        /* 5 */
  u_int16 count;          /* The number of records in the PDU */
  u_int32 sysUpTime;      /* Current time in millisecs since router booted */
  u_int32 unix_secs;      /* Current seconds since 0000 UTC 1970 */
  u_int32 unix_nsecs;     /* Residual nanoseconds since 0000 UTC 1970 */
  u_int32 flow_sequence; /* Seq counter of total flows seen */
  u_int8  engine_type;    /* Type of flow switching engine (RP,VIP,etc.) */
  u_int8  engine_id;      /* Slot number of the flow switching engine */
  u_int16 reserved;
```

Paquet NetFlow v5 (enregistrements)

```
/* 48 byte payload */
 struct ftrec_v5 {
   u_int32 srcaddr;    /* Source IP Address */
   u_int32 dstaddr;    /* Destination IP Address */
   u_int32 nexthop;    /* Next hop router's IP Address */
   u_int16 input;      /* Input interface index */
   u_int16 output;     /* Output interface index */
   u_int32 dPkts;      /* Packets sent in Duration */
   u_int32 dOctets;    /* Octets sent in Duration. */
   u_int32 First;      /* SysUptime at start of flow */
   u_int32 Last;       /* and of last packet of flow */
   u_int16 srcport;    /* TCP/UDP source port number or equivalent */
   u_int16 dstport;    /* TCP/UDP destination port number or equiv */
   u_int8  pad;
   u_int8  tcp_flags;  /* Cumulative OR of tcp flags */
   u_int8  prot;       /* IP protocol, e.g., 6=TCP, 17=UDP, ... */
   u_int8  tos;        /* IP Type-of-Service */
   u_int16 src_as;     /* originating AS of source address */
   u_int16 dst_as;     /* originating AS of destination address */
   u_int8  src_mask;   /* source address prefix mask bits */
   u_int8  dst_mask;   /* destination address prefix mask bits */
   u_int16 drops;
 } records[FT_PDU_V5_MAXFLOWS];
};
```

Exemple de paquet NetFlow v8 (agrégation AS)



Paquet AS agrégé NetFlow v8

```
struct ftpdu_v8_1 {
  /* 28 byte header */
  u_int16 version;         /* 8 */
  u_int16 count;           /* The number of records in the PDU */
  u_int32 sysUpTime;       /* Current time in millisecs since router booted */
  u_int32 unix_secs;       /* Current seconds since 0000 UTC 1970 */
  u_int32 unix_nsecs;      /* Residual nanoseconds since 0000 UTC 1970 */
  u_int32 flow_sequence;   /* Seq counter of total flows seen */
  u_int8  engine_type;     /* Type of flow switching engine (RP,VIP,etc.) */
  u_int8  engine_id;       /* Slot number of the flow switching engine */
  u_int8  aggregation;     /* Aggregation method being used */
  u_int8  agg_version;     /* Version of the aggregation export */
  u_int32 reserved;
  /* 28 byte payload */
  struct ftrec_v8_1 {
    u_int32 dFlows;      /* Number of flows */
    u_int32 dPkts;       /* Packets sent in duration */
    u_int32 dOctets;     /* Octets sent in duration */
    u_int32 First;       /* SysUpTime at start of flow */
    u_int32 Last;        /* and of last packet of flow */
    u_int16 src_as;      /* originating AS of source address */
    u_int16 dst_as;      /* originating AS of destination address */
    u_int16 input;       /* input interface index */
    u_int16 output;      /* output interface index */
  } records[FT_PDU_V8_1_MAXFLOWS];
};
```

Configuration IOS Cisco

- Configuré sur chaque interface d'entrée
- Définit la version
- Définit l'adresse IP du collecteur (où envoyer les flux).
- Active le cas échéant les tables d'agrégation
- Configure le cas échéant les délais d'attente de flux et la taille de la principale table de flux (v5)
- Peut configurer le taux d'échantillonnage.

Configuration IOS Cisco

```
interface FastEthernet0/0
 description Access to backbone
 ip address 169.223.132.10 255.255.255.0
 ip flow egress
 ip flow ingress
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Access to local net
 ip address 169.223.142.1 255.255.255.224
 duplex auto
 speed auto


ip flow-export version 5
ip flow-export destination 169.223.142.3 2002
ip flow top-talkers
  top 10
  sort-by bytes
```

Configuration IOS Cisco

- Version IOS

```
interface FastEthernet0/0
 ip route-cache flow       ! Prior to IOS 12.4
 ip flow [ingress|egress] ! From IOS 12.4
```

Configuration IOS Cisco

```
Flow export v5 is enabled for main cache
  Exporting flows to 169.223.142.3 (2002)
  Exporting using source IP address 169.223.142.1
  Version 5 flow records
  127480 flows exported in 6953 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup
failures
```

Configuration IOS Cisco

```
bb-gw#sh ip cache flow
IP packet size distribution (1765988 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .538 .113 .049 .027 .006 .002 .006 .002 .001 .001 .001 .017 .002 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .002 .018 .204 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  105 active, 3991 inactive, 127794 added
  2151823 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  105 active, 919 inactive, 127726 added, 127726 added to flow
  0 alloc failures, 0 force free
  1 chunk, 8 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          62      0.0        60    50      0.0      15.7      14.3
TCP-FTP              1      0.0         3    60      0.0       8.9      15.2
TCP-WWW          54359      0.1        14   658      2.3       5.3       5.1
TCP-SMTP            20      0.0       103    47      0.0       6.3      13.5
...
```

Configuration IOS Cisco

```
TCP-X              1991       0.0          32    40       0.1         0.5       14.3
TCP-other          8069       0.0          61   214       1.5         7.8        8.9
UDP-DNS           24371       0.0           1    69       0.0         0.1       15.4
UDP-NTP            7208       0.0           1    74       0.0         0.0       15.4
UDP-Frag             14       0.0           1   508       0.0         1.2       15.4
UDP-other          27261       0.0          11   105       0.9         0.4       15.4
ICMP                4457       0.0          17    83       0.2        16.9       15.4
IP-other               1       0.0           1    50       0.0         0.0       15.6
Total:            128017       0.3          13   373       5.3         3.5       10.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
Fa0/0         210.118.80.41   Fa0/1         169.223.142.112 11 0627 059A
1
Fa0/1         169.223.142.3   Fa0/0*        169.223.35.48   06 0050 C166
1
Fa0/0         169.223.35.175  Local         169.223.142.1   06 EFFD 0016
145
Fa0/0         169.223.35.175  Local         169.223.142.1   06 EFFC 0017
1
Fa0/0         169.223.35.175  Fa0/1         169.223.142.3   06 EE61 0016
79
Fa0/1         169.223.142.102 Fa0/0*        216.34.181.71   06 E058 0050
6
Fa0/1         169.223.142.70  Fa0/0*        66.220.146.18   06 CBD3 0050
6
Fa0/0         208.81.191.110  Fa0/1         169.223.142.70  06 0050 DABD
13
…
```

Configuration IOS Cisco

```
ip flow-top-talkers
 top 10
 sort-by bytes
```

```
bb-gw#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
   Bytes
Fa0/1         169.223.142.39  Fa0/0*        169.223.35.139  06 0050 D804
   33K
Fa0/0         169.223.32.102  Fa0/1         169.223.142.37  06 816E 0016
   28K
Fa0/1         169.223.142.39  Fa0/0*        169.223.35.139  06 0050 D805
   26K
Fa0/1         169.223.142.39  Fa0/0*        169.223.35.139  06 0050 D807
   24K
Fa0/1         169.223.142.39  Fa0/0*        169.223.35.139  06 0050 D806
   23K
Fa0/1         169.223.142.37  Fa0/0*        169.223.32.102  06 0016 816E
   23K
Fa0/0         169.223.35.139  Fa0/1         169.223.142.39  06 D804 0050
   6675
Fa0/1         169.223.142.70  Fa0/0*        208.81.191.110  06 ABE7 0050
   4341
Fa0/0         169.223.35.175  Fa0/1         169.223.142.3   06 EE61 0016
   3140
Fa0/1         169.223.142.3   Fa0/0*        169.223.35.175  06 0016 EE61
   2528
10 of 10 top talkers shown. 122 flows processed.
```

Synthèse des commandes Cisco

- Activation des flux sur chaque interface

```
ip route-cache flow

OU

ip flow ingress
ip flow egress
```

- Affichage des flux
  - `show ip cache flow`
  - `show ip flow top-talkers`

Synthèse des commandes Cisco (suite)

- Exportation de flux

```
ip flow-export version 5 [origin-as|peer-as]
ip flow-export destination x.x.x.x <udp-port>
```

- Exportation de flux agrégés

```
ip flow-aggregation cache as|prefix|dest|source|proto
  enabled
  export destination x.x.x.x <udp-port>
```

Flux et applications

Usages pour les flux

- Identification / résolution des problèmes
  - classification du trafic
  - DoS Traceback (some slides by Danny McPherson)
- Analyse du trafic
  - Analyse du trafic inter-AS
  - Rapport sur les serveurs mandataires (*proxies*)
- Comptabilisation
  - vérification croisée d'autres sources
  - possibilité de vérification croisée avec les données SNMP.

Classification du trafic

- Basée sur le protocole et les ports source / destination
  - Identifie le protocole (TCP, UDP, ICMP)
  - peut définir les ports bien connus
  - peut définir les ports P2P bien connus
  - utilisation les plus courantes
    - mesures sur les *proxies* - http , ftp
    - trafic pair à pair (*P2P*) limitant le débit.

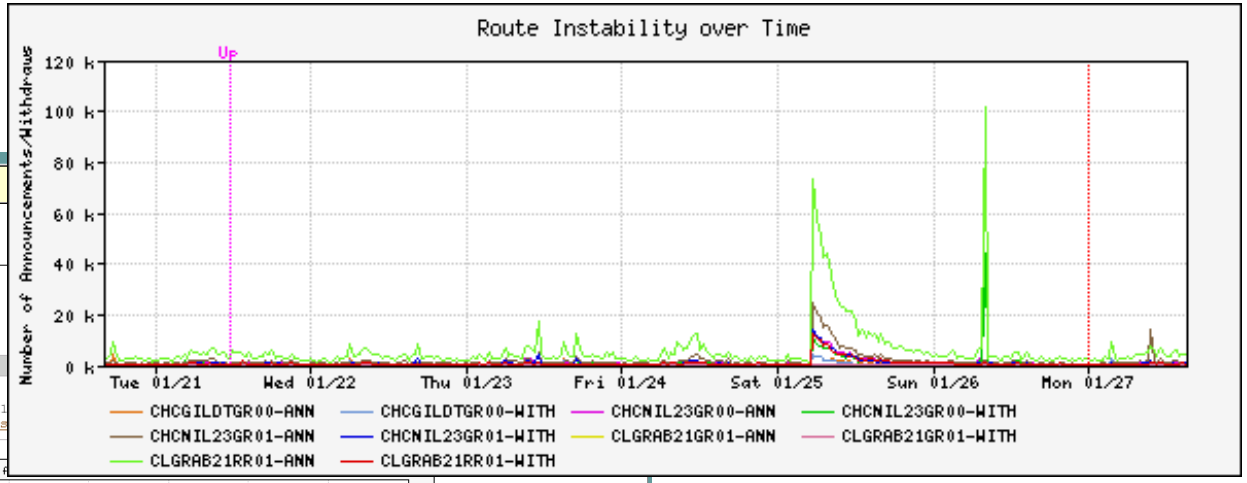
Traceback : basé sur les flux*

- Suivi des attaques par identification de l'empreinte/la signature sur chaque interface par supervision passive :
  - données de flux (NetFlow, cflowd, sFlow, IPFIX par exemple)
  - données de plages
  - PSAMP (échantillonnage de paquets, IETF PSAMP WG)
- Produits libres et payants sur le marché
- Non-intrusif, largement pris en charge

Détection basée sur les flux*

- Supervision des flux (transactions sur les couches réseau et transport) du réseau et définition de bases de référence en matière de comportement :
  - par interface
  - par préfixe
  - par protocole et ports de la couche transport
  - “Build time-based buckets” (toutes les 5 minutes, 30 minutes, 1 heure, 12 heures, selon jours de la semaine, du mois, de l’année).

Détection d'anomalies : ver "Slammer" sur serveur SQL*



peakflow DoS

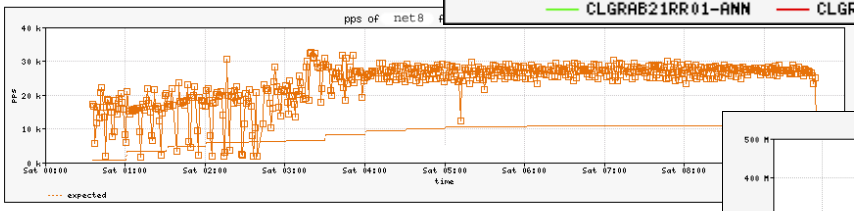
Recent Anomalies : Anomaly 125772 : Detailed Statistics

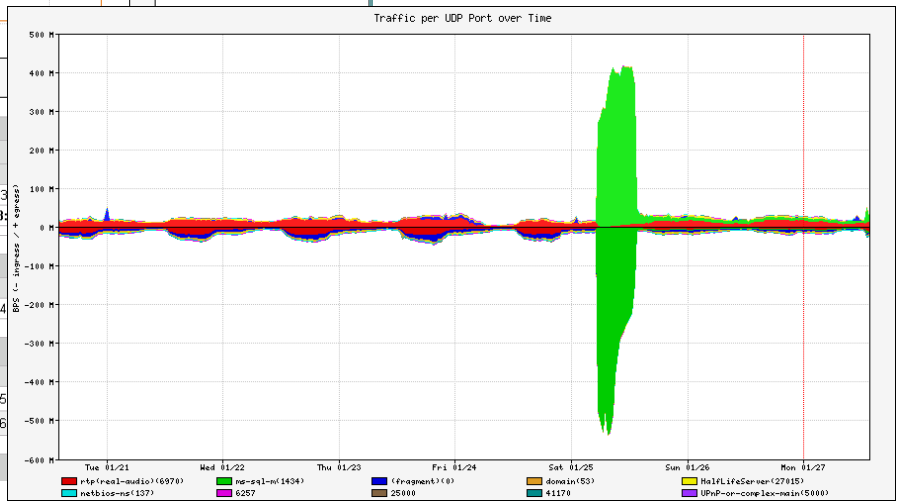
11:51:49 EST 27 Jan 2003

Status | Topology | Ongoing | Recent | Dark IP | Admin | About

Anomaly 125772 Detailed Statistics

ID	Importance	Severity	Duration	Direction	
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing	192.1 members





Affected Network Elements

Router net8 1.2.3.4

	Triggering	Expected	Difference	Maximum
Bitrate	71.69 Mbps	2.34 Mbps	69.35 Mbps	105.26 Mbps @ 03
Packet Rate	22.20 Kpps	712 pps	21.49 Kpps	32.58 Kpps @ 03:

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Summary of all Data Snapshots Collected:

	Bytes	Packets	Bytes/Pkt	bps	
	308.01 GB	762,849,500	404 B	76.05 Mbps	23.54

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Source Addresses

Network / Mask	Bytes	▼Packets	Bytes/Pkt	bps	
192.168.20.217/32	168.22 GB	416,436,800	404 B	41.54 Mbps	12.85
192.168.18.187/32	139.53 GB	345,372,800	404 B	34.45 Mbps	10.66

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Destination Addresses

Détection basée sur les flux (suite)*

- Une fois posées les bases, les activités présentant des anomalies peuvent être détectées :
  - anomalies de **débit** (pps, *pure-rated based* or bps) légitimes ou malveillantes
  - nombre d'attaques **abusives** peuvent être immédiatement reconnues, même **sans** bases de référence (inondations TCP SYN ou RST, par exemple)
  - des **signatures** peuvent être également définies afin d'identifier des données transactionnelles "intéressantes" (proto udp et port 1434 et 404 octets (376 payload) == slammer! par exemple)
  - Des signatures temporelles peuvent être définies afin d'obtenir une détection plus précise.

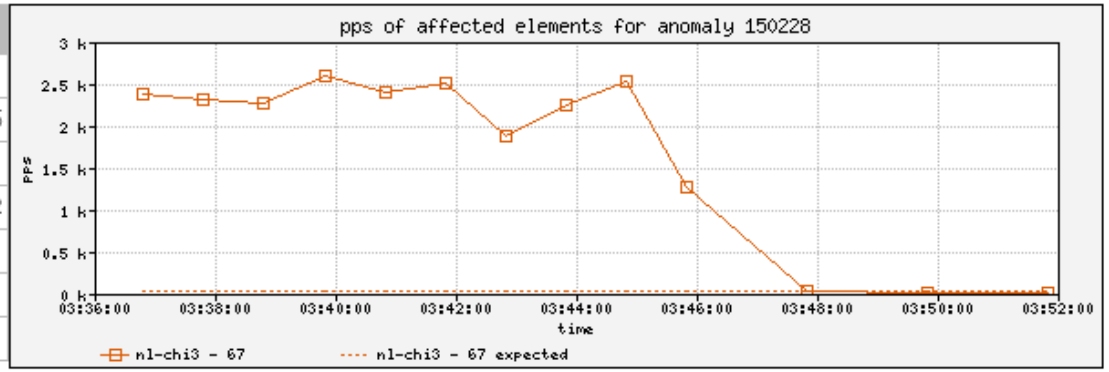
Outils commercialisés basés sur les flux…*

Anomaly 150228 — Get Report: PDF XML

ID	Importance	Duration	Start Time	Direction	Type	Resource
150228	High 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 windowsupdate.com

Traffic Characterization

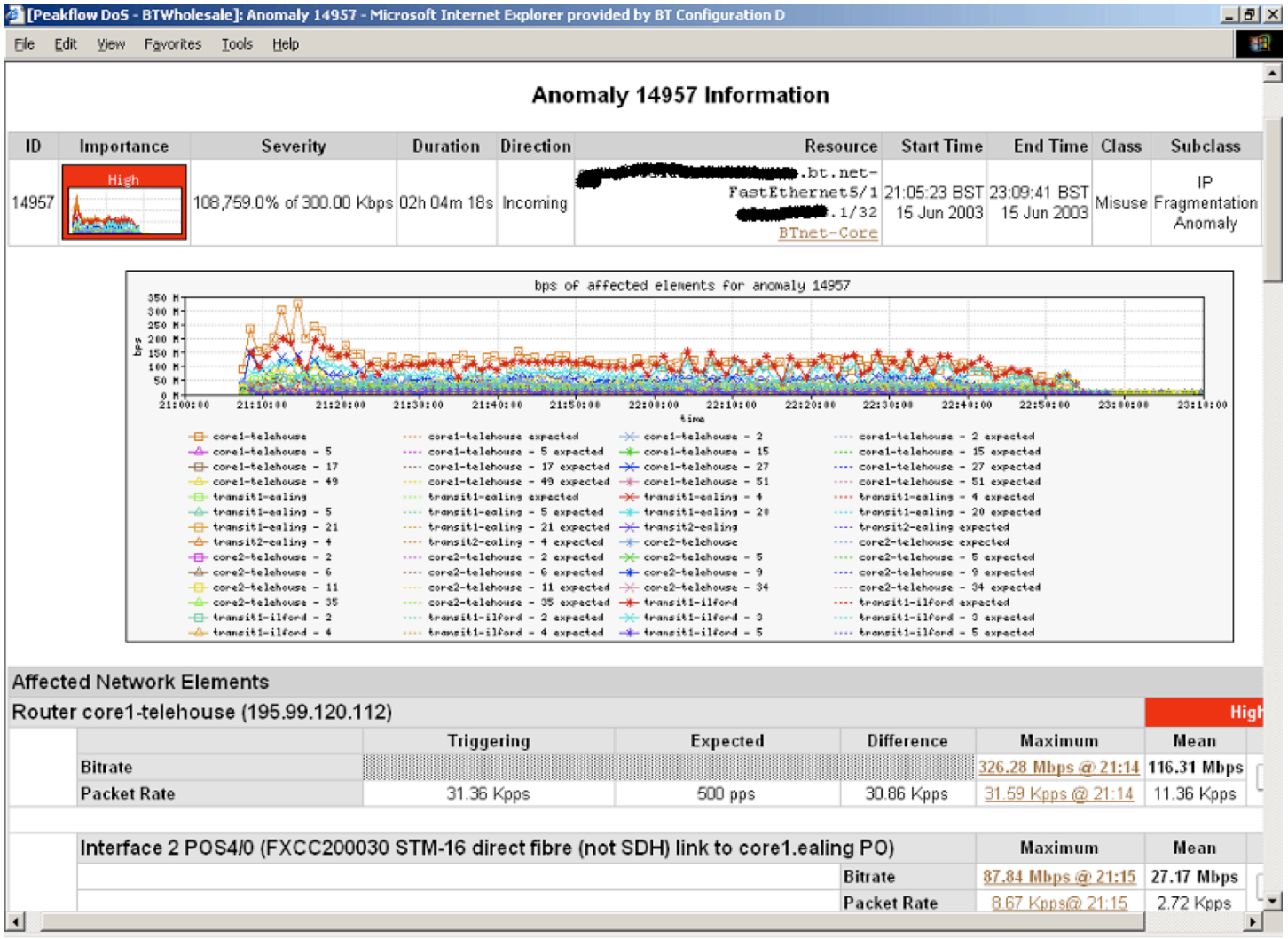
Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)



Affected Network Elements	Importance	Expected pps	Observed bps Max	Observed bps Mean	Observed pps Max	Observed pps Mean	
Router nl-chi3 198.110.131.125	High						
Interface 67 at-1/1/0.14 *pvc to WMU*		26	832 K	563.1 K	2.6 K	1.7 K	Details

Anomaly Comments

Détection commerciale
Attaque DOS à grande échelle*



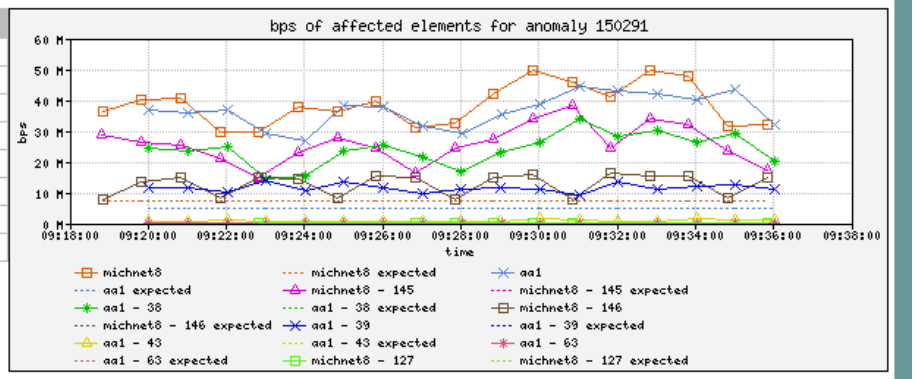
Traceback : commercial*

Anomaly 150291 — Get Report: PDF XML

ID	Importance	Duration	Start Time	Direction	Type	Resource
150291	High 124.6% of 40 Mbps	19 mins	09:16, Aug 17	Incoming	Protocol TCP (Profiled)	[redacted]

Traffic Characterization

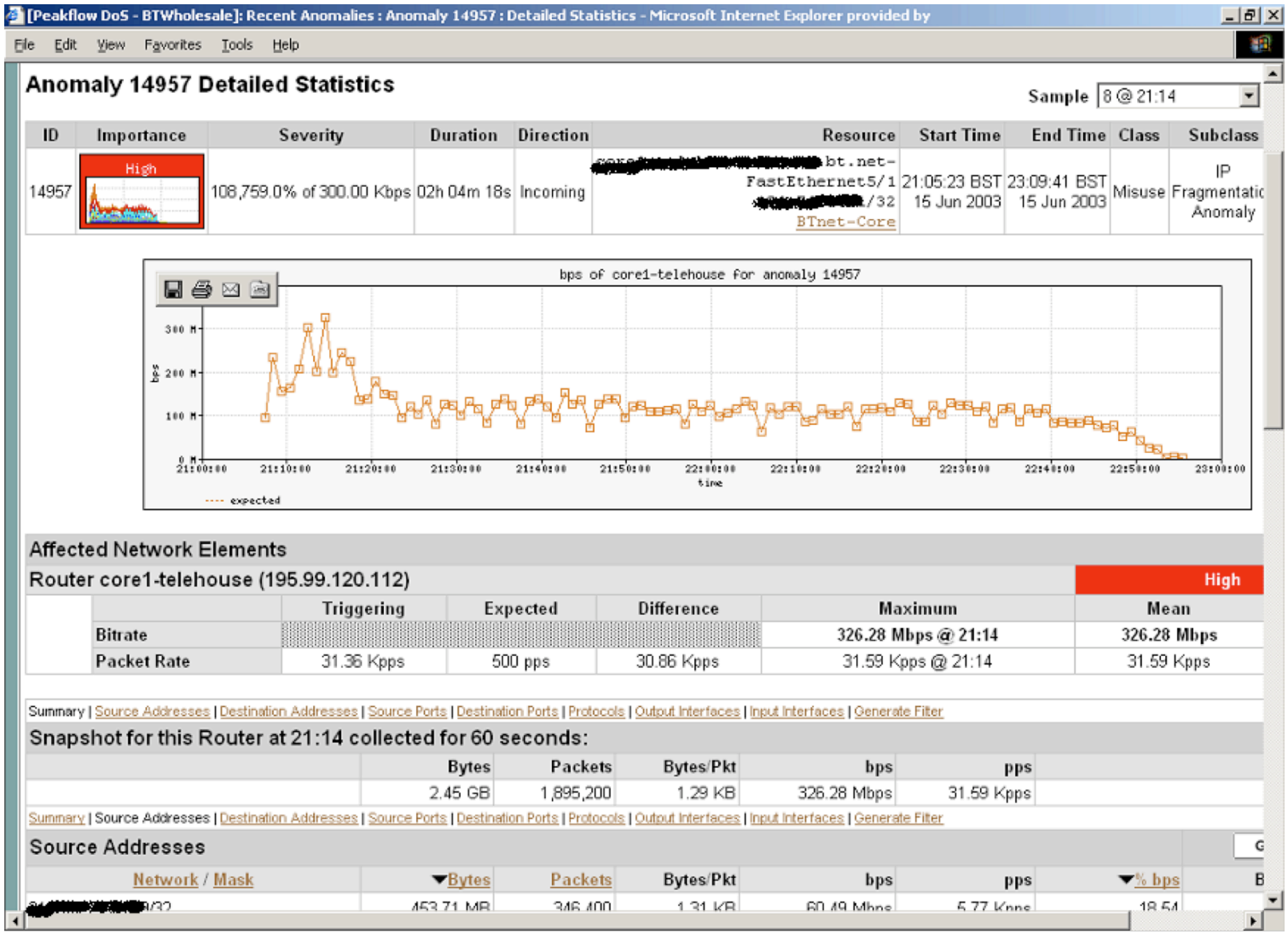
Sources	136.165.56.151/32
	69.1.194.74/32
	0 - 4095
Destination	[redacted]
	1409 (here-lm)
Protocols	tcp (6)
TCP Flags	AP (0x18) A (0x10)



Affected Network Elements

	Importance	Expected bps	Observed bps Max	Observed bps Mean	Observed pps Max	Observed pps Mean	
Router michnet8 198.108.90.125	High	7.2 M	49.9 M	38.7 M	5.3 K	4.2 K	Details
Interface 127 ATM1/0.27-aal5 layer 198.108.22.181 *pvc to NLR-PORTI*		-	3.3 K	1.2 K	5	2.4	Details
Interface 145 GigabitEthernet5/0.22 - 802.1q vlan subinterface 198.108.23.153 *vlan to MichBin*		-	38.4 M	25.8 M	3.7 K	2.6 K	Details
Interface 146 GigabitEthernet5/0.24 - 802.1q vlan subinterface 198.108.23.245 *CHI-ANN_Bin*		-	16.6 M	12.8 M	1.9 K	1.6 K	Details
Router aa1 198.108.90.21	High	5.1 M	44.4 M	36.6 M	4.5 K	3.8 K	Details
Interface 38 so-0/2/0.1 192.122.183.9 *pvc to Abilene Indianapolis*		-	34.0 M	24.0 M	3.0 K	2.2 K	Details
Interface 39 so-0/2/0.2 63.149.0.186 *pvc to Qwest Chicago*		-	13.9 M	11.6 M	1.3 K	1.1 K	Details
Interface 43 so-1/0/0.0 208.172.10.138 *OC3 to C&W (Chicago)*		-	1.6 M	959.6 K	600	408.8	Details
Interface 63 ge-0/1/0.11 198.108.90.17 *vlan to Comcast*		-	411.5 K	56.9 K	83.3	41.7	Details

Traceback commercial : détails*



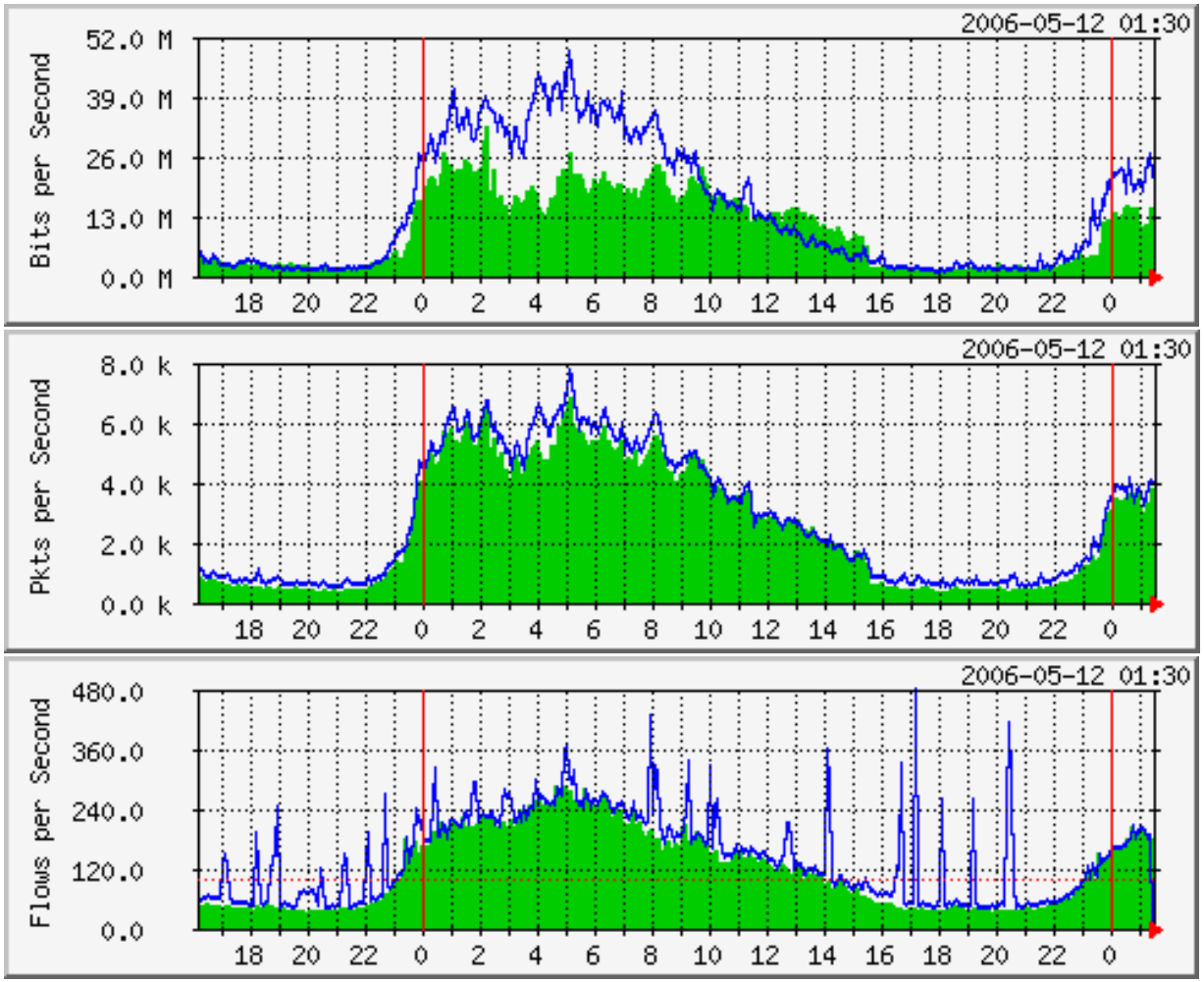
Analyse du trafic

- Voir le trafic sur la base des AS source et de destination
  - AS source et de destination issu de la table de routage du routeur
  - nécessite un maillage intégral avec protocole BGP sur des points d'échange IXP ainsi que le transit et l'appairage (*peering*)
  - Les préfixes de sites source et de destination peuvent être collectés et mis en relation avec un préfixe externe dans les données ASN.

Comptabilisation

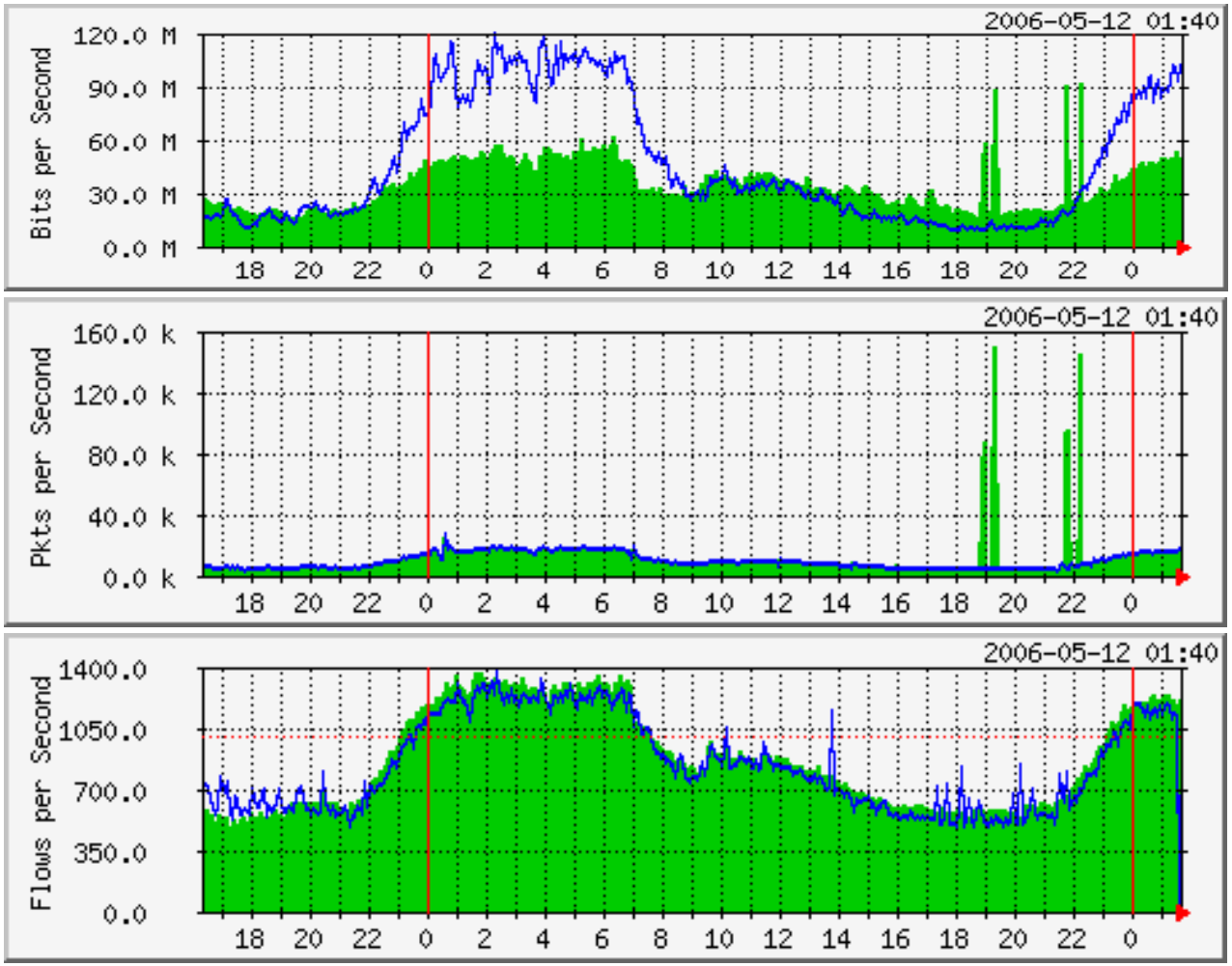
- Une comptabilisation basée sur les flux peut compléter utilement la comptabilisation basée SNMP.

SNMP et flux



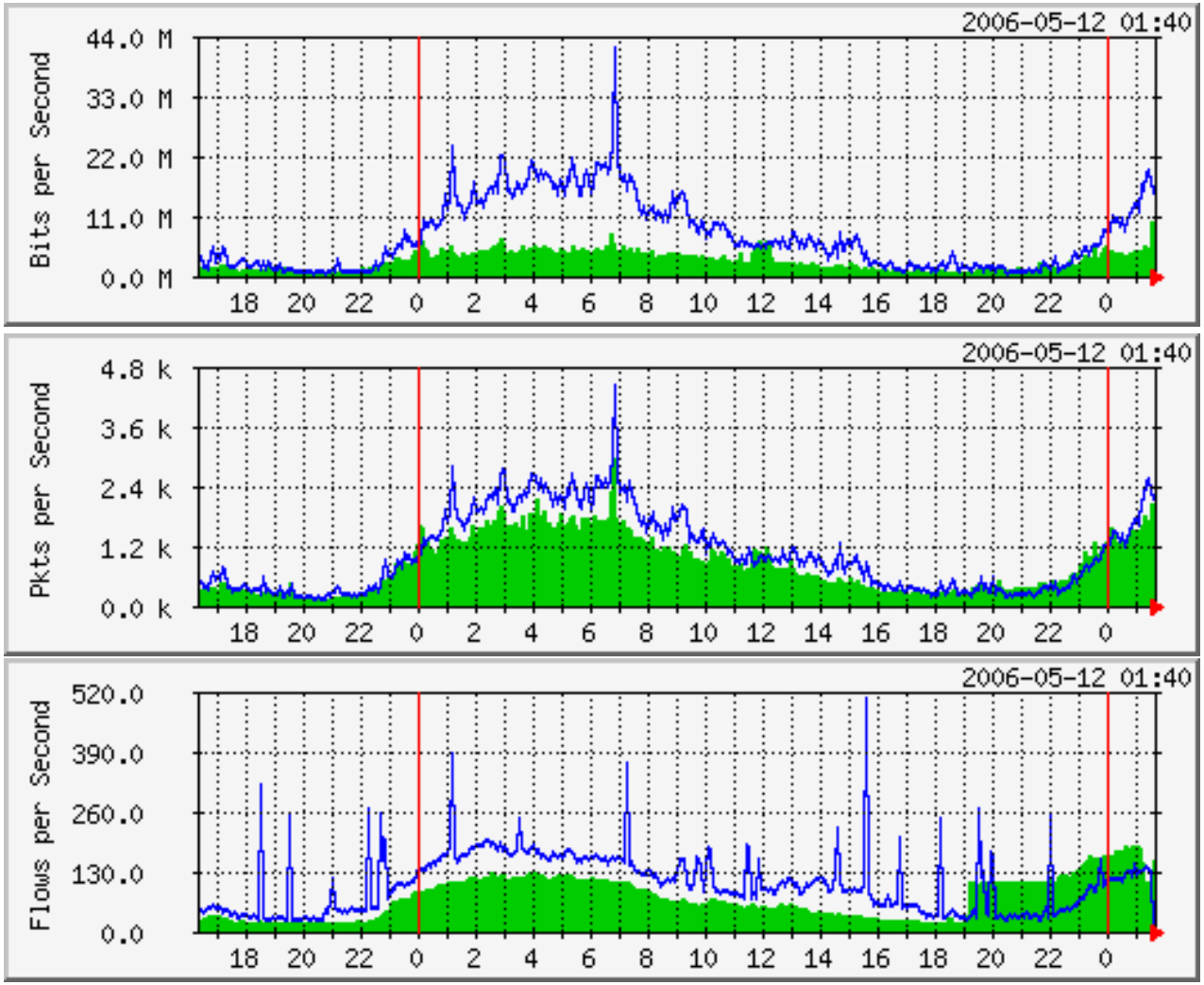
Data Courtesy AARNET, Australia and Bruce Morgan

Plus détaillé...



Data Courtesy AARNET, Australia and Bruce Morgan

SNMP et flux



Data Courtesy AARNET, Australia and Bruce Morgan

Et ensuite…

- IPFIX (*IP Flow Information Exchange*)

  Protocole pour l'échange des flux de trafic IP

  - Uniformise le format des flux et faciliter l'écriture d'outils d'analyse
  - http://www1.ietf.org/html.charters/ipfix-charter.html
  - Requirements for IP Flow Information Export (RFC 3917)
  - Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX) (RFC 3955)

Références

- Outils de flux
  http://www.splintered.net/sw/flow-tools
- Applications NetFlow

  ttp://www.inmon.com/technology/

  netflowapps.php
- Netflow HOW-TO
  http://www.linuxgeek.org/netflow-howto.php
- Effort de normalisation IETF
  http://www.ietf.org/html.charters/ipfix-charter.html

Références (suite)

- Page Abilene NetFlow
  http://abilene-netflow.itec.oar.net/
- Liste de diffusion d'outils de flux
  flow-tools@splintered.net
- Communauté Cisco Centric Open Source
  http://cosi-nms.sourceforge.net/related.html

Références (suite)

- http://ensight.eos.nasa.gov/FlowViewer/
- http://nfsen.sourceforge.net/
- http://www.netflowdashboard.com/