Vue d'ensemble de NetFlow

Gestion et Supervision de Réseau

Sommaire

- Netflow
  - Qu’est-ce que Netflow et comment fonctionne-t-il ?
  - Utilisations et applications
- Configurations et mise en œuvre fournisseur
  - Cisco et Juniper
- Outils de flux
  - Problèmes d’architecture
  - Logiciels, outils, etc.
- Autres thèmes / Démonstrations

Flux de réseau

- Paquets ou trames présentant un attribut commun.
- Politique de création et d'expiration – conditions de démarrage et d'arrêt d'un flux.
- Compteurs – paquets, octets, temps.
- Informations d'acheminement – système autonome (AS), masque de réseau, interfaces.

Flux de réseau

- Unidirectionnels ou bidirectionnels.
- Les flux bidirectionnels peuvent contenir d’autres informations telles que le temps d'aller-retour, 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.

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 - Outils 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 signifie :
  - Plus de temps de post-traitement pour générer 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/ fin.
- Informations d’acheminement réseau – masques et numéro de système autonome.

Génération/collecte de flux

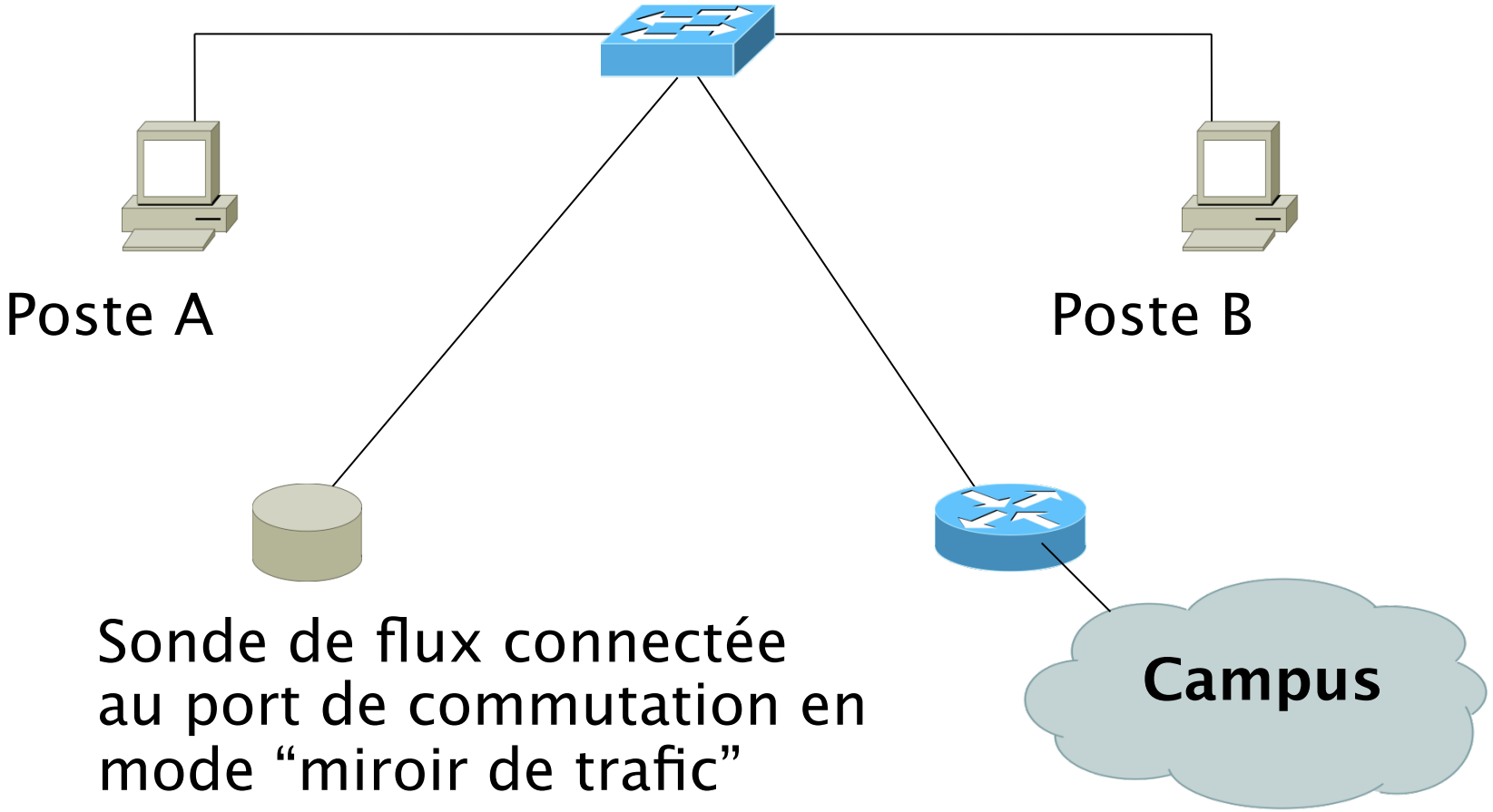
Moniteur passif

- Un moniteur passif (généralement un hôte Unix) reçoit l'ensemble des données et génère les flux.
- Gourmand en ressources

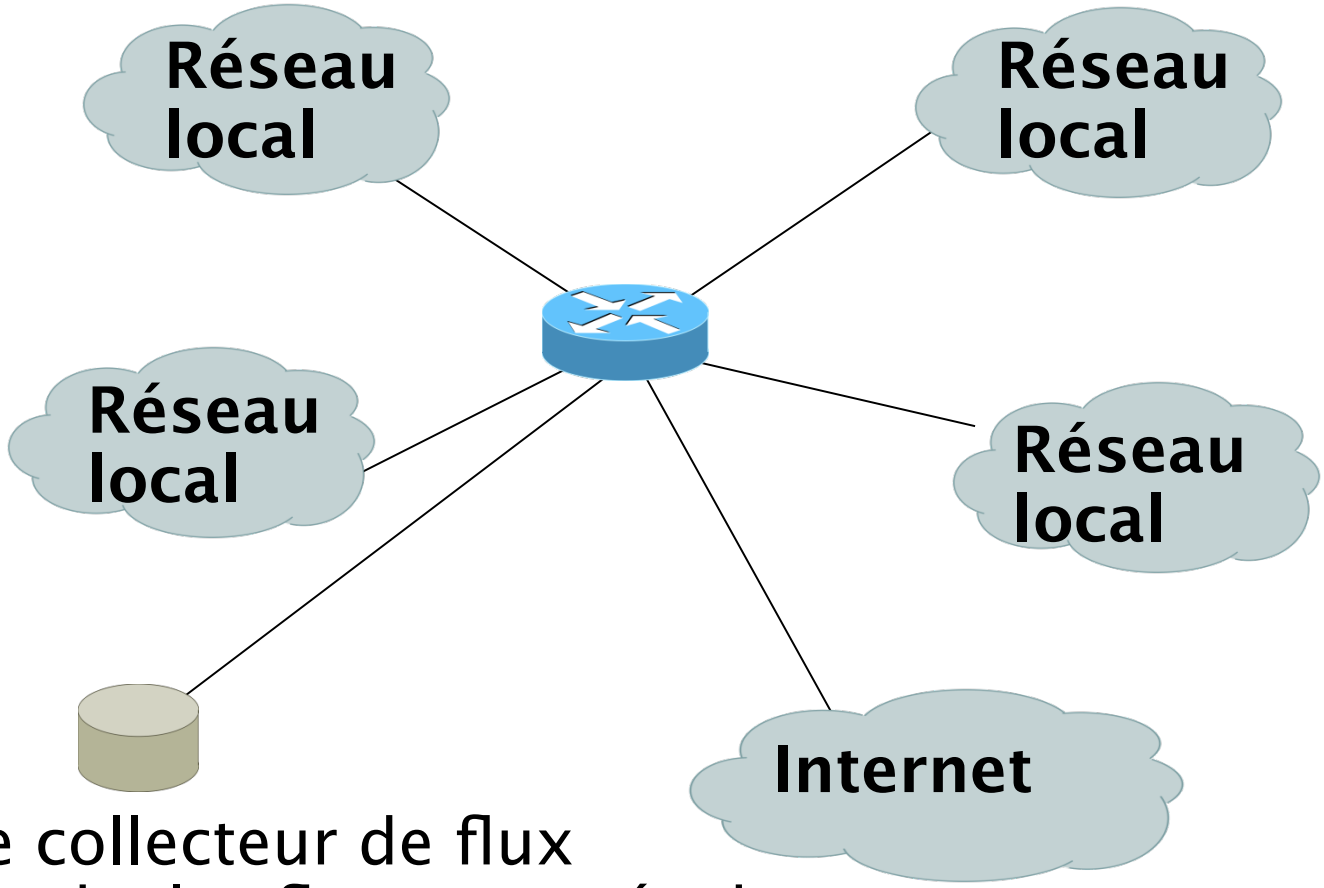
Routeur ou autre périphérique existant du réseau

- Génération des flux par un routeur ou d'autres équipements existants tels qu'un commutateur
- Possibilités d'échantillonnage
- Pas d'investissements en nouveaux équipements

Collecte par un moniteur passif



Collecte par un routeur



Le collecteur de flux
stocke les flux exportés du routeur

Mises en œuvre vendeurs

Cisco NetFlow

- Flux unidirectionnels.
- IPv4 unicast et multicast.
- Agrégé et non agrégé.
- Flux exportés par UDP.
- Supporté sur plates-formes IOS et CatOS.
- Mise en œuvre différente de NetFlow Catalyst.

Versions Cisco NetFlow

- 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 plate-forme Catalyst.

NetFlow v1

- Champs clés : 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.

NetFlow v5

- Champs clés : 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.

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

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

```
gw-169-223-2-0#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         169.223.2.2     Fa0/0         169.223.11.33   06 0050 0B64  3444K
Fa0/1         169.223.2.2     Fa0/0         169.223.11.33   06 0050 0B12  3181K
Fa0/0         169.223.11.33   Fa0/1         169.223.2.2     06 0B12 0050    56K
Fa0/0         169.223.11.33   Fa0/1         169.223.2.2     06 0B64 0050    55K
Fa0/1         169.223.2.2     Local         169.223.2.1     01 0000 0303    18K
Fa0/1         169.223.2.130   Fa0/0         64.18.197.134   06 9C45 0050    15K
Fa0/1         169.223.2.130   Fa0/0         64.18.197.134   06 9C44 0050    12K
Fa0/0         213.144.138.195 Fa0/1         169.223.2.130   06 01BB DC31  7167
Fa0/0         169.223.15.102  Fa0/1         169.223.2.2     06 C917 0016  2736
Fa0/1         169.223.2.2     Local         169.223.2.1     06 DB27 0016  2304
10 of 10 top talkers shown. 49 flows processed.
```

Synthèse des commandes Cisco

- Activation de CEF (par défaut)
  - **`ip cef`**
- Activation des flux sur chaque interface

```
ip route cache flow OR
ip flow ingress
ip flow egress
```

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

Synthèse des commandes Cisco (suite)

- Exportation des flux vers un collecteur

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

- Exportation de flux agrégés

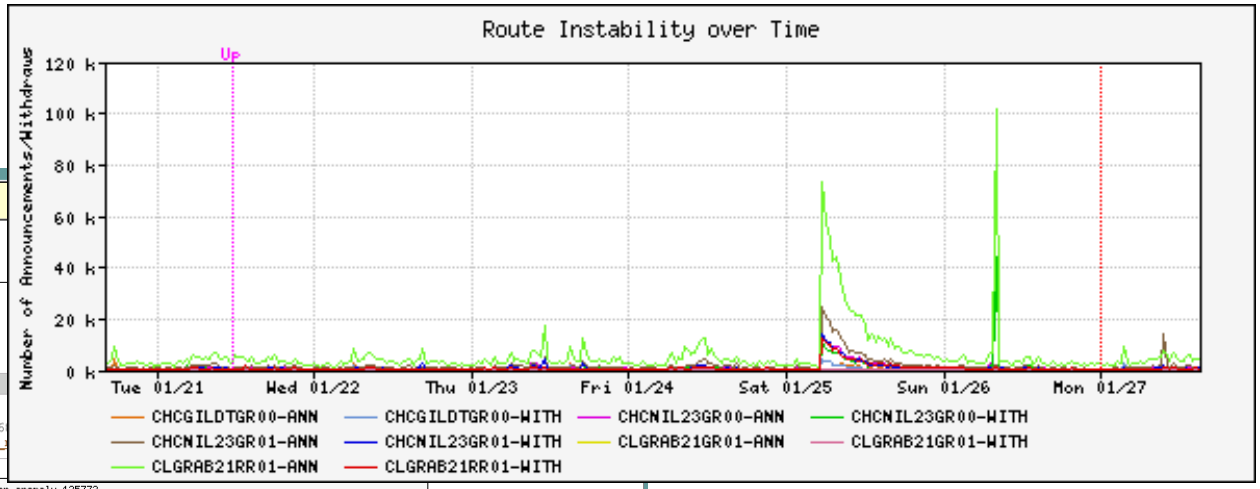
```
ip flow-aggregation cache as|prefix|dest|source|proto
  enabled
  export destination x.x.x.x <udp-port>
```

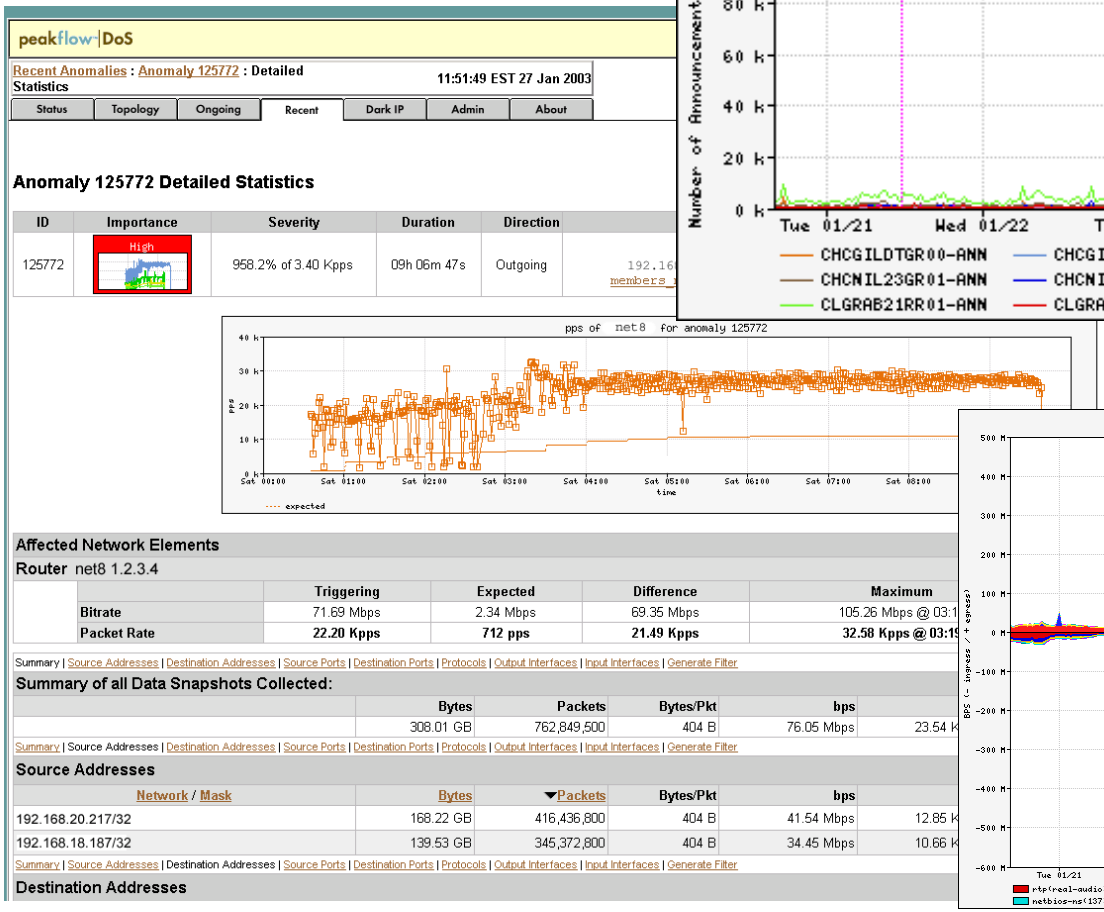
Flux et applications

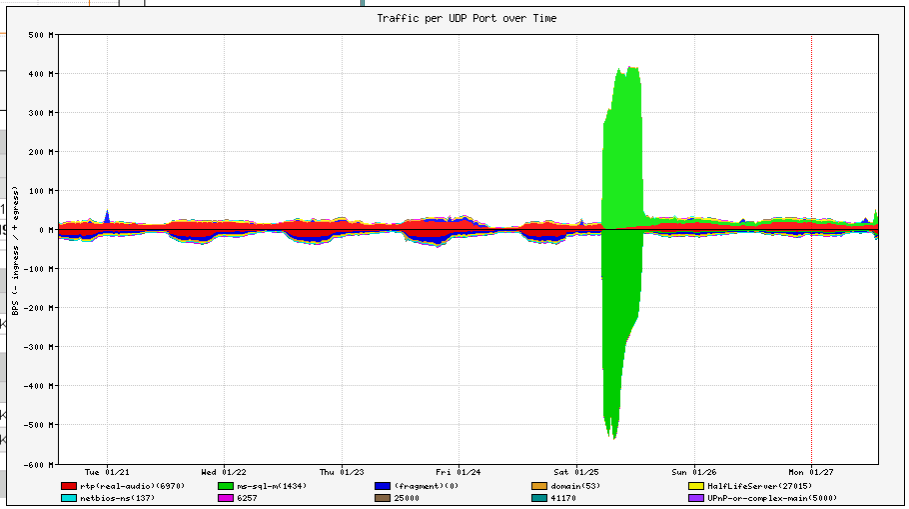
Utilisations des flux

- Identification / résolution des problèmes
  - Classification du trafic
  - Traçage des dénis de service (quelques diapositives de Danny McPherson)
- Analyse du trafic
  - Analyse du trafic inter-AS (systèmes autonomes)
  - Rapport sur les serveurs mandataires (proxies)
- Comptabilisation
  - Vérification croisée à partir d'autres sources
  - Possibilité de vérification croisée avec les données SNMP

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







Détection basée sur les flux (suite)*

Une fois posées les bases, les activités présentant des anomalies peuvent être détectées

- Les **anomalies de débit** (pps ou bps) peuvent être légitimes ou malveillantes
- Bon 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" (ex : protocole udp et port 1434 et 404 octets (charge 376) == slammer!)
- Des signatures temporelles peuvent être définies afin d'obtenir une détection plus précise

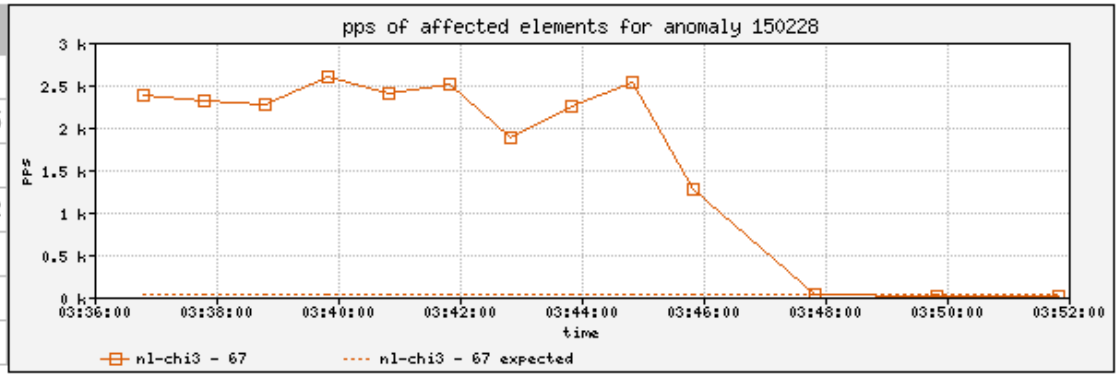
Outils commerciaux basés sur les flux…*

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

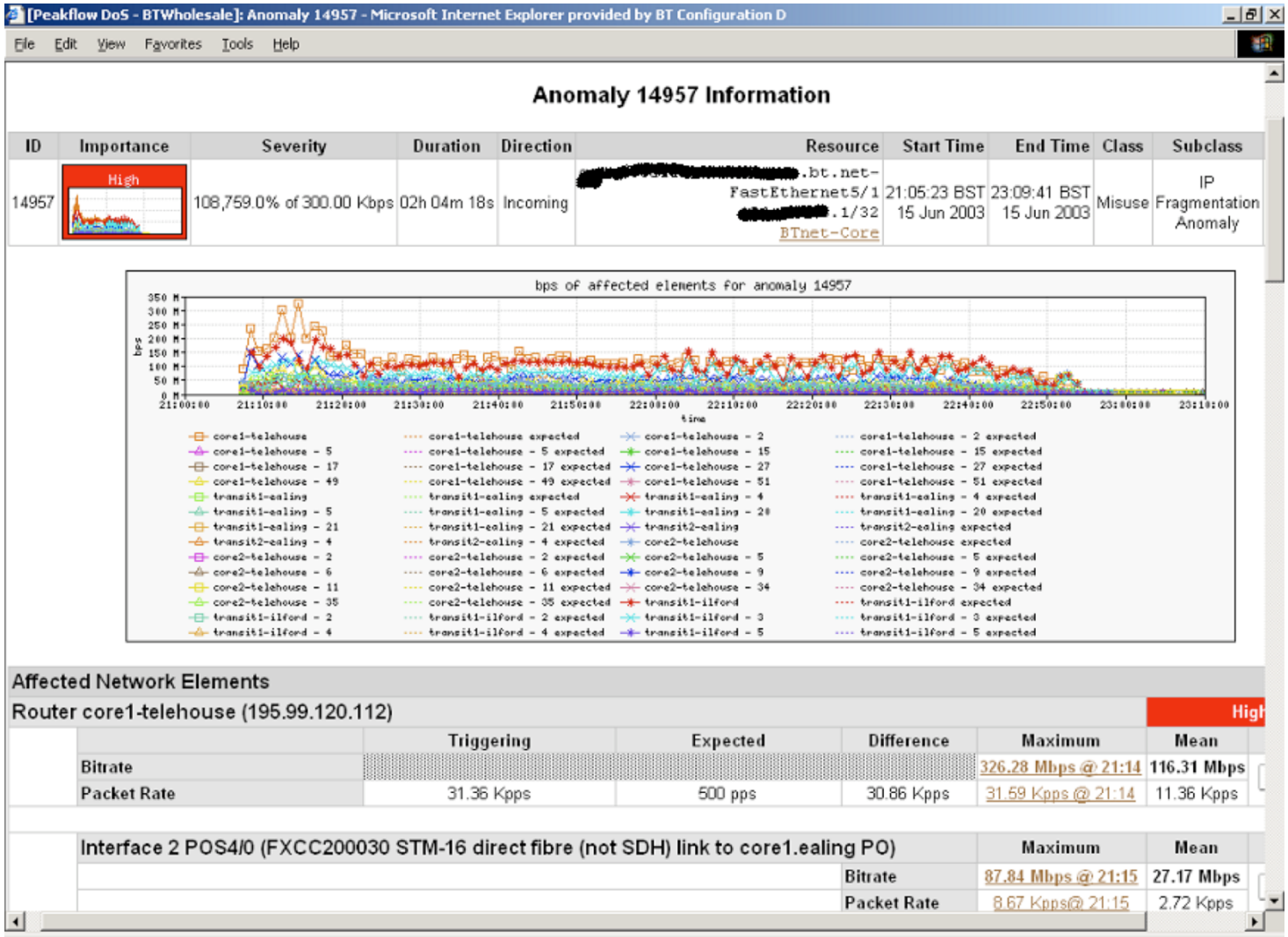
Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)



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*



Comptabilisation

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

Références

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

  http://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
- Guide utilisateur du collecteur Cisco NetFlow
  http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/6.0/tier_one/user/guide/user.html