

# IPFIX

(Internet Protocol Information eXport)

gt-metro, réunion du 20/11/06

Lionel.David@rap.prd.fr

# Plan

- Définition d'IPFIX
- Le groupe de travail IPFIX
- Les protocoles candidats
- Les conditions requises par IPFIX
- Spécifications d'IPFIX
- Architecture d'IPFIX
- Autres drafts..

# Définition d'IPFIX

- IPFIX est un protocole en cours de standardisation par le groupe de travail IPFIX de l'IETF  
(<http://www.ietf.org/html.charters/ipfix-charter.html>)
- Principale motivation :
  - Le besoin d'un standard commun d'export, via le réseau, de l'information sur les flux IP par un équipement de type routeur, sonde, switch...vers un collecteur (système) pour analyse du trafic.

# Le groupe de travail (WG) IPFIX

- Statut actif du WG depuis sept. 2001
- Objectifs du WG :
  - Évaluation des protocoles candidats : OK
    - RFC 3955 : « *Evaluation of Candidate Protocols for IP Flow Information eXport* »
  - Spécifier les requis pour ce protocole : OK
    - RFC 3917 : « *Requirements for IP Flow Information eXport* »
  - Spécifications du protocole : En cours
    - Draft accepté (17/11/06) par l'IESG pour publication Proposed Standard RFC :
      - draft-ietf-ipfix-protocol-24 « *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »
    - Drafts en cours d'évaluation IESG pour publication Proposed Standard RFC :
      - draft-ietf-ipfix-architecture-12 « *Architecture for IP Flow Information eXport* »

# Le groupe de travail (WG) IPFIX

- Spécifications du protocole (suite) : En cours
  - Drafts en cours d'évaluation IESG pour publication Informational RFC :
    - draft-ietf-ipfix-as-10 « *IPFIX Applicability* »
    - draft-ietf-ipfix-info-14 « *Information Model for IP Flow Information eXport* »
  - Drafts actifs :
    - draft-ietf-ipfix-testing-00 « *IP Flow Information eXport (IPFIX) Testing* »
    - draft-ietf-ipfix-biflow-00 « *Bidirectional Flow Export using IPFIX* »
    - draft-ietf-ipfix-implementations-guidelines-01 « *IPFIX Implementation Guidelines* »
    - draft-ietf-ipfix-reducing-redundancy-01 « *Reducing redundancy in IPFIX and PSAMP reports* »
- Une 20aine d'autres documents actifs en relation avec les spécifications d'IPFIX : Cf. <http://tools.ietf.org/wg/ipfix>

# RFC 3955 : Protocoles candidats

« *Evaluation of Candidate Protocols for IP Flow Information eXport* »

- 5 candidats pour un protocole de base à IPFIX :
  - **CRANE** ( Common Reliable Accounting for Network Element Protocol), **Diameter** (Évolution du protocole RADIUS), **LFAP** (Lightweight Flow Admission), **NetFlow v9** (Cisco-s NetFlow protocol), **Streaming IPDR** ( développé par l'organisme « Internet Protocol Detail Record »)
- Critères de classification et d'évaluation :
  - **Qualité du processus de mesure (metering)**, **sampling**, comportement en cas de **congestion**, marquage de la **date** (timestamp), **synchronisation**, mécanisme **d'expiration des flux**, **modèle de l'information** exportée, **modèle des données encodées** dans l'information exportée, le **transport de l'information** (UDP/TCP/SCTP, qualité et prise en compte de la congestion), **sécurité** (IPSec, TLS..)
- Candidat retenu : NetFlow v9
  - **Malgré ses points faibles** : sécurité, qualité de transport de l'information (NetFlowv9 est indépendant du protocole de transport MAIS seul UDP est pour le moment utilisé)
  - **Il reste incontournable** :
    - «Standardiser la pratique déjà existante» : il est le plus implémenté et utilisé
    - NetFlow est simple et bien conçu
    - Un collecteur NetFlow est facile à écrire
  - On prend NetFlow v9 et on **comble ses lacunes dans IPFIX**

# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- Le RFC 3917 a été créé dans le but de définir :
  - La notion de flux IP standard et autre terminologie
  - Les applications nécessitant l'utilisation d'IPFIX
  - Un processus de comptage (metering process) pour traitement et enregistrement des données observées dans les flux IP
  - Un processus d'export de l'information sur les flux IP
  - Le transport de l'information sur les flux IP
  - Le(s) moyen(s) de sécuriser les informations exportées
  - ...

# RFC 3917 : Les conditions requises par IPFIX

« Requirements for IP Flow Information eXport »

- La notion de flux IP standard :

« Un flux est défini comme étant un ensemble de paquets IP passant par un point d'observation du réseau pendant un certain intervalle de temps. Tous les paquets appartenant à un flux en particulier ont un ensemble de propriétés en commun. Chaque propriété est définie par l'une des conditions suivantes :

- Un ou plusieurs champ de l'en-tête du paquet (IP\_DST...), de transport (PORT\_DST...) ou de l'application ( en-tête RTP...) en commun
- Une ou plusieurs caractéristiques du paquet en commun (label MPLS...)
- Le traitement du paquet en commun (OUTPUT\_IF...)

Un paquet appartient à un flux s'il comporte toutes les propriétés définies pour ce flux. »



# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- **Terminologie :**

- « Observation point » : Point d'observation
  - Point du réseau où les paquets peuvent être observés (ex: le port d'un routeur ou une carte d'interface...)
  - 1 ou plusieurs points d'observation sur un équipement
- « Metering process » : Un processus de mesure
  - Processus qui enregistre les flux à un point d'observation. Il observe l'en-tête d'un paquet et son traitement. Après échantillonnage (sampling), si un paquet correspond à un flux, le processus en capture l'en-tête, marque la date (timestamping), le classe dans le(s) flux correspondant et maintient ce dernier.
  - La Maintenance d'un flux comprend l'ajout d'infos dans l'enregistrement d'un flux (Flow Record), la création d'un nouvel enregistrement de flux, des statistiques sur les flux, la détection de l'expiration d'un flux, le transfert de l'enregistrement d'un flux au processus d'export, la suppression de l'enregistrement d'un flux.
  - 1 ou plusieurs processus par équipement

# RFC 3917 : **Les conditions requises par IPFIX**

## « *Requirements for IP Flow Information eXport* »

- Terminologie (suite) :
  - « Flow Record » : Enregistrement de flux
    - Un enregistrement de flux contient les informations sur un flux spécifique qui a été comptabilisé à un point d'observation.
  - « Exporting Process » : Processus d'export
    - Processus qui envoie les enregistrements de flux (dans un message IPFIX) à un ou plusieurs processus de collecte. Un enregistrement de flux peut de même être généré par un ou plusieurs processus de comptage.
  - « Collecting Process » : Processus de collecte
    - Ce processus reçoit les enregistrements de flux de la part de un ou plusieurs processus d'export.

# RFC 3917 : **Les conditions requises par IPFIX**

## « *Requirements for IP Flow Information eXport* »

- Les applications nécessitant IPFIX :
  - Comptabilité basée sur les usages :
    - Facturation par service, application, classe de service...
  - Profiler le trafic :
    - Analyse du trafic (volume des flux, durée des flux...) pour organiser, dimensionner au mieux le réseau
  - Ingénierie du trafic :
    - Mesures, modélisation, caractérisation et contrôle du réseau pour optimiser la gestion des ressources et la performance du réseau.
  - Détection d'attaques et d'intrusion :
    - Mieux connaître les attaques et en tirer une stratégie de défense.
  - Contrôle de la QoS

# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- Metering process (processus de mesure) :
  - Comment distinguer les paquets pour les classer dans un ou plusieurs flux ? En fonction d'un ou plusieurs des paramètres suivants (« Flow Key »):
    - Interface d'entrée ou de sortie
    - Les champs de l'en-tête IP :
      - Source IP
      - Destination IP
      - Type de protocole (TCP, UDP, ICMP...)
    - Les champs de l'en-tête de la couche transport (port)
    - Label MPLS
    - DiffServ Code Point
    - Un paquet crypté n'est pas pris en compte.

# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- Metering process (Processus de mesure) :
  - Caractéristiques requises :
    - Fiabilité : détection et rapport d'un incident (ex: surcharge)
    - Échantillonnage (sampling) possible et paramétrable
    - Adaptation en cas de surcharge
    - Étiquetage de la date ( timestamp) pour chaque paquet d'un flux
    - Synchronisation de la date avec l'UTC
    - Détection de l'expiration d'un flux (les bits FIN ou RST...)
    - Distinguer les flux multicasts : les paquets d'un flux multicast peuvent être répliqués vers plusieurs interface de sortie = plusieurs flux
    - Prise en compte des paquets fragmentés
    - Ignorer le port-mirroring

# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- Metering process (Processus de mesure) :
  - Paramètres obligatoirement configurables :
    - Spécification du point d'observation
    - Spécification des flux à traiter
    - Expiration des flux
  - Paramètres pouvant être configurables :
    - La méthode d'échantillonnage
    - Le comportement en cas de surcharge

# RFC 3917 : **Les conditions requises par IPFIX**

## « *Requirements for IP Flow Information eXport* »

- **Export process (Processus d'export) :**
  - Le modèle de l'information : (Information Model)
    - Liste (extensible) des attributs d'un flux qui peuvent être contenus dans un rapport d'enregistrements de flux :
      - IP version, IP\_SRC/DST, IP\_PROT\_TYPE, PORT\_SRC/DST, byte counter, packet counter, ToS, Flow Label, label MPLS, timestamp du premier paquet, timestamp du dernier paquet, le sampling configuré, identificateur unique du point d'observation, identificateur unique du processus d'export, ICMP type/code, input interface, output interface, TTL...next hop IP, next hop BGP...
  - Le modèle de donnée : (Data model)
    - Modèle décrivant comment l'information est représentée dans un enregistrement de flux
    - Modèle extensible pour gérer de nouveaux attributs de flux.
  - Ces modèles sont fournis aux collecteurs pour décodage

# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- Export process (Processus d'export) :
  - Paramètres configurables :
    - Le format des données exportées en fonction des attributs sélectionnés
    - Le(s) processus de collecte destinataire(s)
    - L'intervalle d'envoi de l'export de l'information sur les flux
    - Notifications à envoyer au collecteur en cas d'évènement spécifique
    - Rendre anonyme les flux



# RFC 3917 : **Les conditions requises par IPFIX**

« *Requirements for IP Flow Information eXport* »

- **Le transport de l'information** sur les flux d'un processus d'export vers un processus de collecte :
  - Support d'un protocole de contrôle de congestion
  - Fiabilité :
    - Détection et rapport en cas de perte d'information sur les flux
    - Retransmission de l'information perdue
    - Acquiescement de la part du collecteur
  - Sécurité : Confidentialité, Intégrité, Authenticité
  - Envoi de l'information en mode Push (Push Mode) :
    - Pas besoin de requête de la part du collecteur pour exporter
  - Envoi de notification au collecteur en cas d'évènement spécifique (premier paquet d'un nouveau flux...)
  - Rendre anonyme les informations contenues dans les enregistrements de flux...

# RFC 3917 : **Les conditions requises par IPFIX**

## « *Requirements for IP Flow Information eXport* »

- Le(s) moyen(s) de sécuriser les informations exportées :
  - Divulgarion des informations contenus dans les enregistrements exportés :
    - Confidentialité :
      - Cryptage des données
      - Mécanisme permettant de rendre anonyme les informations (en cours de spécif)
  - Information forgée :
    - Authentification et Intégrité
  - Attaques par « Deny » de service :
    - Utiliser le mode Push pour le processus d'export
    - Le collecteur peut être inonder par des enregistrement de flux

# Spécifications

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Statut : Approuvé par l'IESG le 17/11/06 pour devenir RFC
- Résumé :
  - Spécifications du protocole IPFIX permettant la transmission de l'information sur des flux IP par le réseau. Ce document décrit comment les données IPFIX transmises du processus d'export vers le processus de collecte sont représentées, ce qu'elles signifient, le moyen de les transporter et de les sécuriser.

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

## « *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Ajout de terminologie :
  - « Observation Domain » :
    - Ensemble de points d'observation pour lequel l'information sur un flux peut être agrégé par le metering process (ex : Line Card d'un routeur).
  - « Flow Key » :
    - Clé permettant de définir un flux :
      - Champ(s) de l'en-tête d'un paquet (IP\_DST...) et/ou propriété(s) d'un paquet (taille du paquet...), et/ou info(s) dérivée(s) du traitement du paquet (AS number...)
  - « Exporter » :
    - Équipement hébergeant au moins un processus d'export
  - « IPFIX Device » :
    - Équipement hébergeant au moins un processus d'export, un point d'observation et un metering process.
  - « IPFIX Message » :
    - Message contenant des enregistrement sur les flux envoyé par un processus d'export à destination d'un processus de collecte

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Ajout de terminologie :
  - « Template » :
    - Permet de spécifier la structure et la sémantique d'un ensemble d'information contenu dans un message IPFIX.
  - « Message Header » :
    - Première partie d'un message IPFIX qui fournit des informations basiques comme version IPFIX, longueur du message, numéro de séquence du message...
  - « Template Record » :
    - Permet de définir la structure et l'interprétation des champs dans un « Data Record »
  - « Data Record » :
    - Enregistrement contenant les valeurs des paramètres correspondant à un « Template Record »
  - « Options Template Record » :
    - Template Record qui définit la structure et l'interprétation de champs dans un « Data Record » mais concernant un certain champ d'applicabilité (scope).

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Ajout de terminologie :
  - Set :
    - Ensemble d'enregistrements qui ont une structure identique. Dans un message IPFIX, un ou plusieurs Set peuvent suivre l'en-tête. Trois différents types de Set : Template Set, Options Template Set, Data Set.
  - Template Set :
    - Ensemble de « Template Record » ayant été groupés dans un même message IPFIX
  - Options Template Set :
    - Ensemble d' « Options Template Record » ayant été groupés dans un même message IPFIX
  - Data Set :
    - Un ou plusieurs « Data Record », du même type, regroupé dans un même message IPFIX. Chaque Data Record est au préalable défini par un Template Record ou un Option template Record.

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

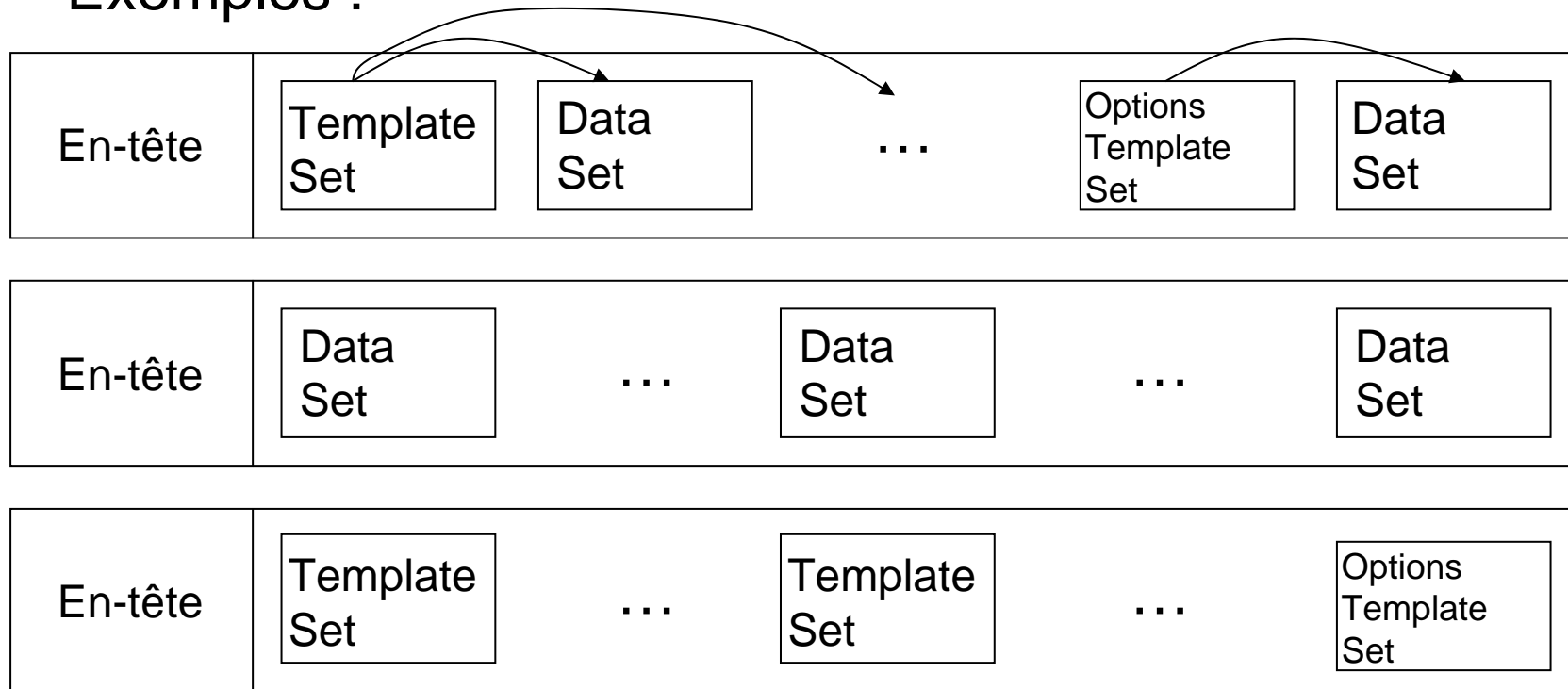
Set	Contenu	
	Template	Record
Data Set	/	Data Record(s)
Template Set	Template Record(s)	/
Options Template Set	Options Template Record(s)	/



# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Format d'un message IPFIX = En-tête + Set(s)
- Exemples :



# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Format de l'en-tête d'un message IPFIX :

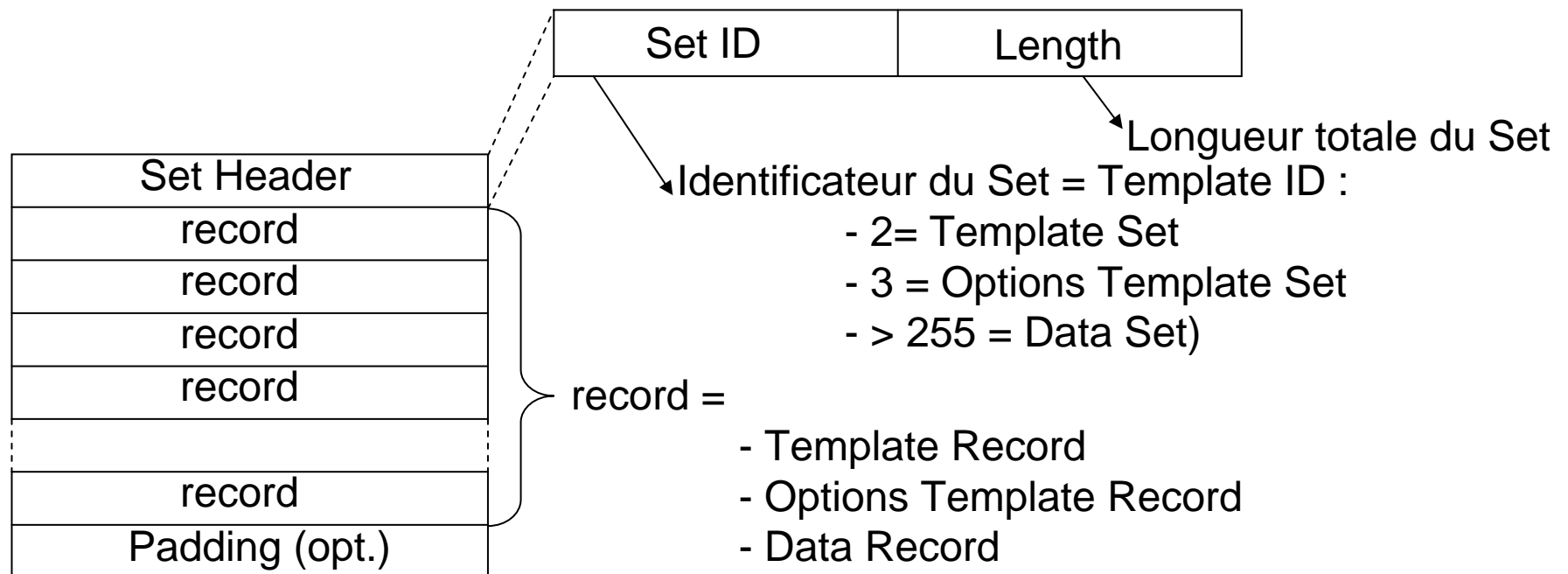
Version Number	Lenght
Export Time	
Sequence Number	
Observation Domain ID	

- Dans l'ordre :
  - Version IPFIX = 0x000a = 10
  - Longueur = longueur totale du message IPFIX
  - Export Time = Date en seconde UTC au moment de l'export du message
  - Sequence = numéro de séquence
  - Observation Domain ID = De quel domaine d'observation le message provient, est égale à 0 si aucun domaine n'est défini.

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- **Format d'un Set** (Data Set/Template Set/Options Template Set) :

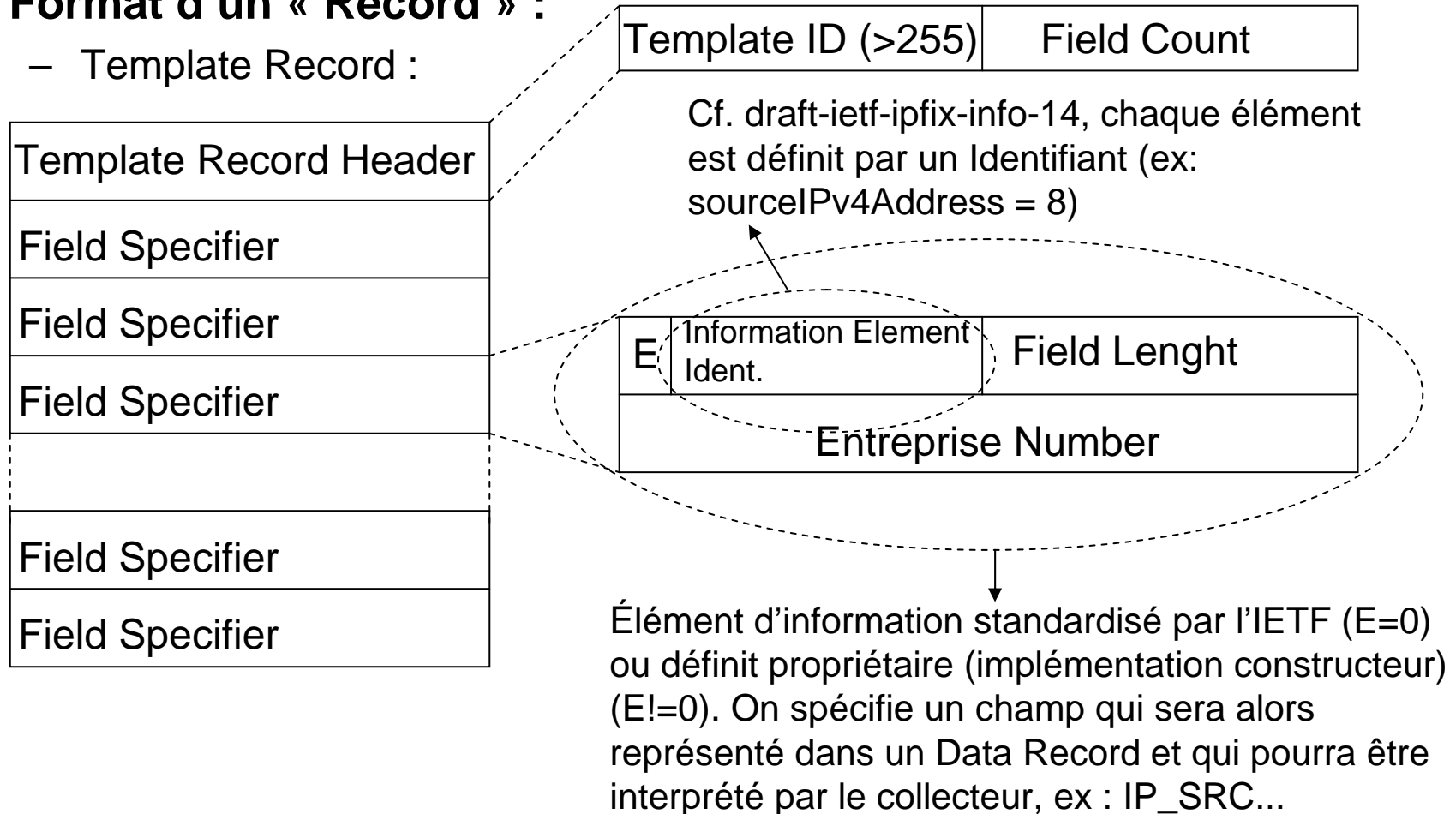


# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

## « Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information »

- **Format d'un « Record » :**

- Template Record :

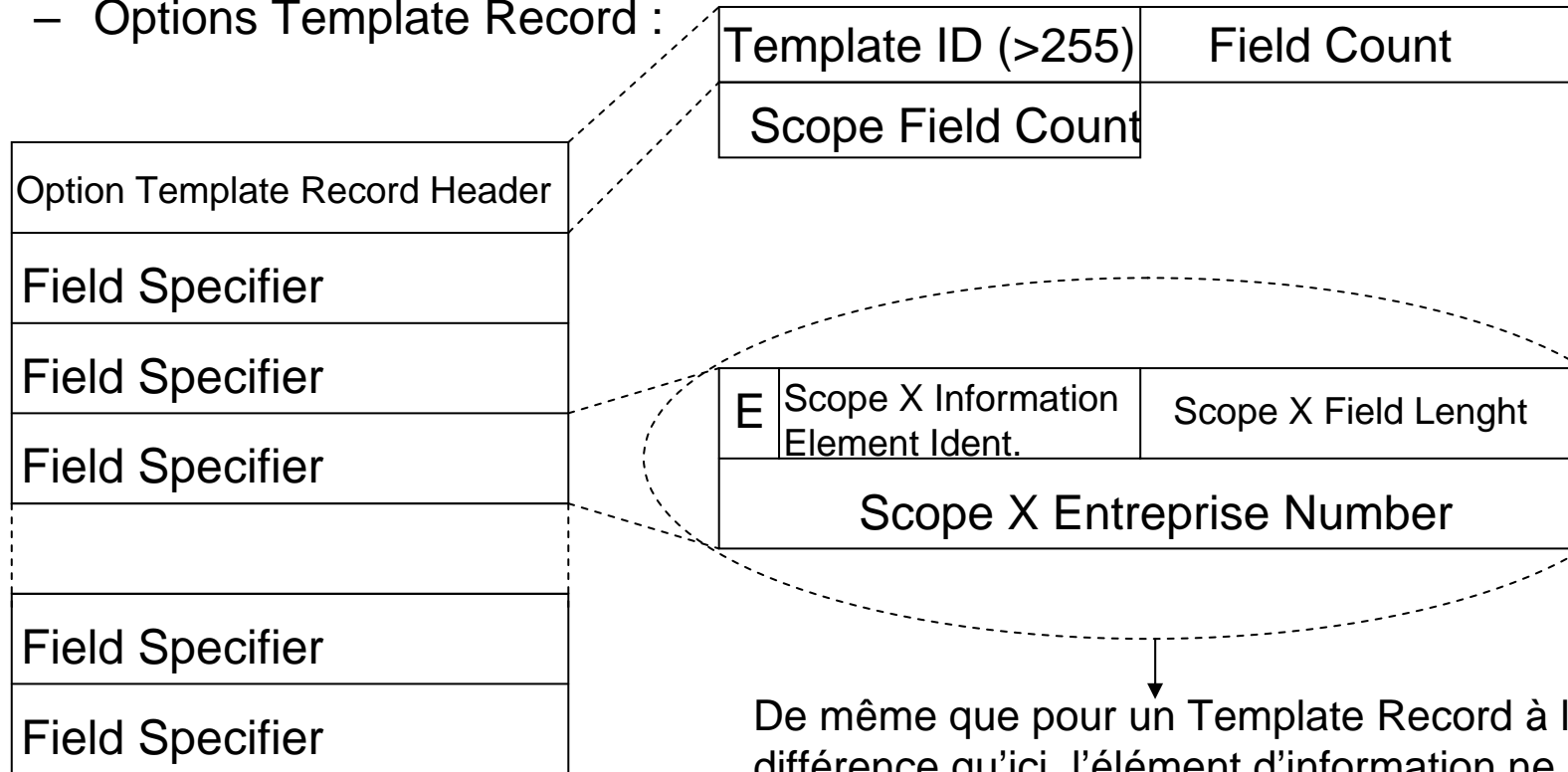


# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

## « Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information »

- **Format d'un « Record » :**

- Options Template Record :



De même que pour un Template Record à la différence qu'ici, l'élément d'information ne concerne qu'un certain champ d'applicabilité (scope). Ex : LineCardId, TemplateId, ingressInterface, meteringProcessId...

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

## « Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information »

- **Format d'un « Record » :**

- Data Record :

Field Value
Field Value
Field Value
Field Value
Field Value
Field Value

Field Value = Valeur du champ représentant un élément d'information (IP\_SRC, AS number, PORT TCP...)

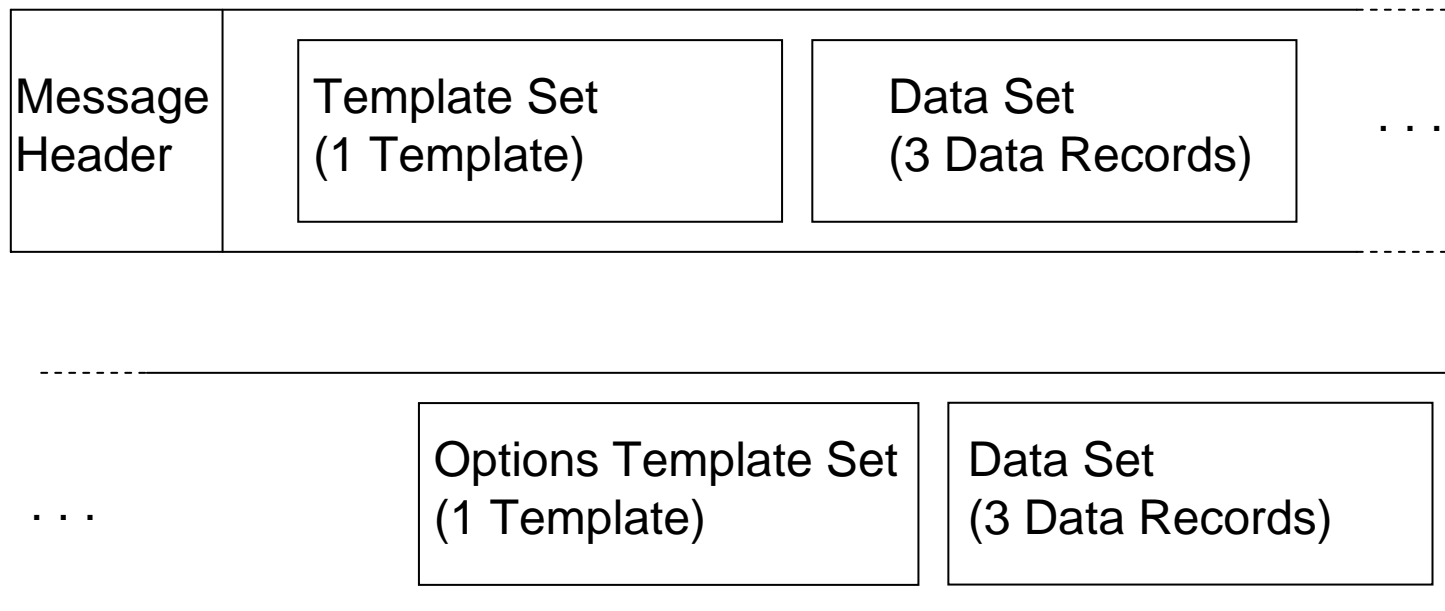
- **Format d'un « Data Set » :**

<b>Set ID = Template ID</b>	Lenght
Record 1 – Field Value 1	Record 1 – Field Value 2
Record 1 – Field Value 3	...
Record 2 – Field Value 1	Record 2 – Field Value 2
Record 2 – Field Value 3	...
...	...
...	Padding (optional)

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Exemple d'un message IPFIX :



# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Exemple d'un message IPFIX : le Template Set
  - Utilisation d'éléments d'information standardisés par l'IETF (draft info)
    - Source IPv4 : sourceIPv4Address (ID = 8)
    - Destination IPv4 : destinationIPv4Address (ID = 12)
    - Next-hop IPv4 : ipNextHopIPv4Address (ID = 15)
    - Nombre de paquets dans le flux : inPacketDeltaCount (ID = 2)
    - Nombre d'octets dans le flux : inOctetDeltaCount (ID = 1)

Set ID = 2		Length = 28 octets
Template ID 256		Field Count = 5
0	sourceIPv4Address = 8	Field Length = 4
0	destinationIPv4Address = 12	Field Length = 4
0	ipNextHopIPv4Address = 15	Field Length = 4
0	inPacketDeltaCount = 2	Field Length = 4
0	inOctetDeltaCount = 1	Field Length = 4

IETF



# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Exemple d'un message IPFIX : le Data Set

Src IP addr.	Dst IP addr.	Next Hop addr.	Packet number	Octets number
192.0.2.12	192.0.2.254	192.0.2.1	5009	5344385
192.0.2.27	192.0.2.23	192.0.2.2	748	388934
192.0.2.56	192.0.2.65	192.0.2.3	5	6534

Set ID = 256		Length = 64	
Record 1	}	192.0.2.12	
		192.0.2.254	
		192.0.2.1	
		5009	
		5344385	
Record 2	}	192.0.2.27	
		192.0.2.23	
		192.0.2.2	
		748	
		388934	
Record 3	}	192.0.2.56	
		192.0.2.65	
		192.0.2.3	
		5	
		6534	

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Exemple d'un message IPFIX : l' Options Template Set
  - Utilisation d'éléments d'information standardisés par l'IETF (draft info) :
    - Par Line Card (lineCardId), on rapporte les éléments suivants :
      - Nombre total de messages IPFIX : exportedPacketCount (ID = 41)
      - Nombre total de flux exportés : exportedFlowCount

Set ID = 3	Length = 24	
Template ID 258	Field Count = 3	
Scope Field Count = 1	0	lineCardId = 141
Scope 1 Field Length = 4	0	exportedPacketCount = 41
Field Length = 2	0	exportedFlowCount = 42
Field Length = 2	Padding	

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Le processus de collecte :
  - La réception d'un « Template Record » ou un « Options Template Record » permet au processus de collecte d'avoir la sémantique d'un « Data Record » puisque ce dernier fait référence à un « Template Record » ou un « Options Template Record ».

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Le transport de l'information (message IPFIX) :
  - Le processus de collecte n'est pas obligatoirement sur le même lien que le processus d'export.
  - IPFIX est indépendant du protocole de transport
  - L'utilisation de SCTP et PR-SCTP **doit** être possible
  - L'utilisation de TCP et UDP **peut** être possible.
  - PR-SCTP et TCP prennent en compte la congestion, pas UDP
  - L'utilisation de PR-SCTP est très fortement préférée :
    - Permet une meilleure gestion de l'utilisation des Template Record
      - Établissement d'une association SCTP (Export – Collecte) :
        - » Stream zero = Template Record/Options Template Record
        - » Reste = Data Record
    - Optimisation dans l'export des messages IPFIX vers le processus de collecte
      - Fonctionnement par association SCTP :
        - » Nouveau Template Record = nouvelle association...système plus optimal
    - Un processus d'export peut établir plusieurs associations SCTP vers un ou plusieurs processus de collecte.

# Le protocole IPFIX : draft-ietf-ipfix-protocol-24

« *Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information* »

- Sécurité :
  - TLS / DTLS :
    - TLS = Transport Layer Security pour TCP
    - DTLS = « Datagram TLS » pour sécuriser UDP et SCTP
    - Authentification, Intégrité et Confidentialité sont fournies
  - Protection contre le « deny » de service :
    - SCTP = mécanisme d'échange de cookies
    - TCP = mécanisme « SYN cookie »
    - DTLS = mécanisme d'échange de cookies
  - Le processus doit fournir un mécanisme de log basé sur les numéros de séquence des messages IPFIX
  - Sécuriser le système hébergeant le processus de collecte

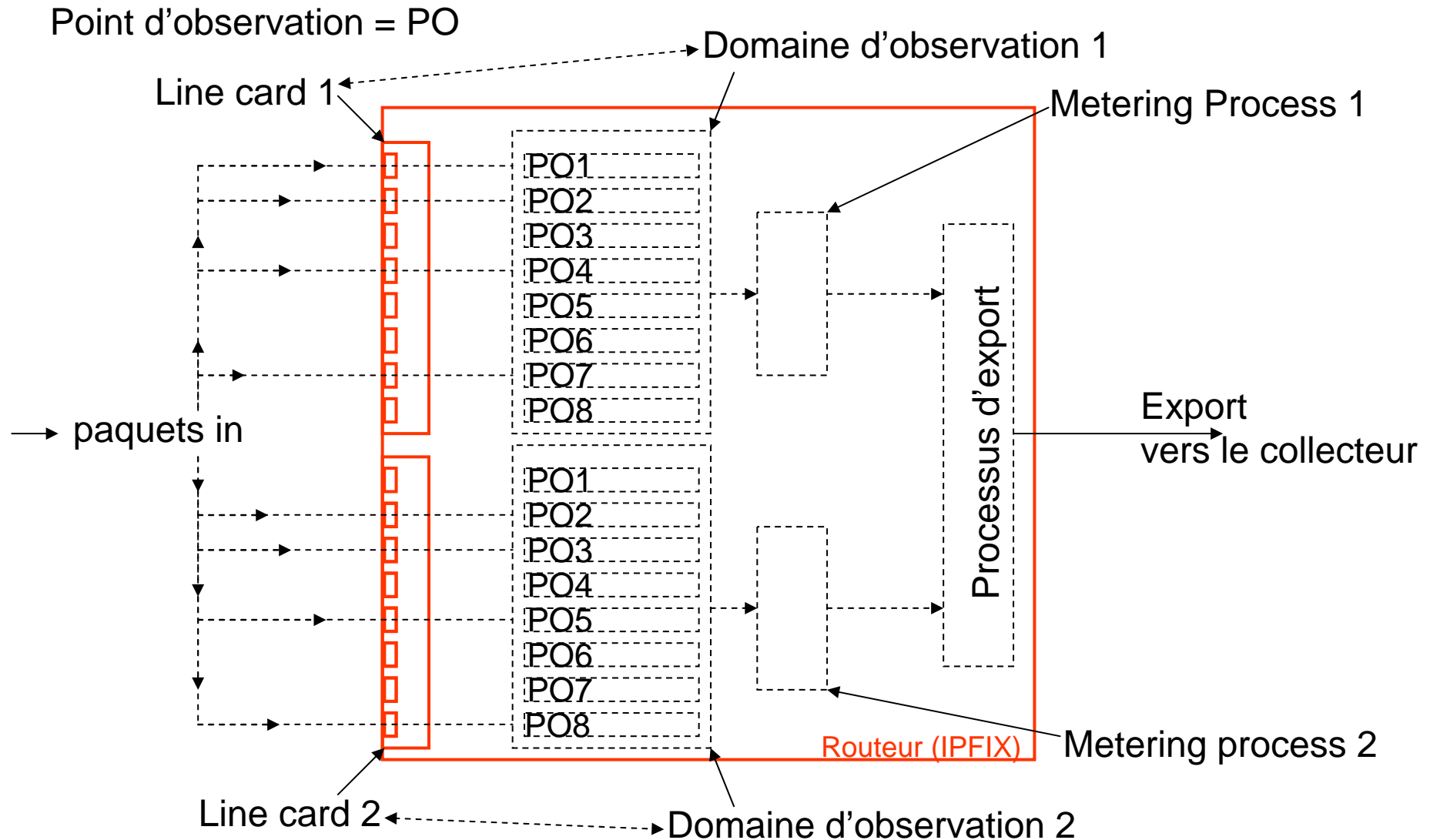
# Architecture d'IPFIX : draft-ietf-ipfix-architecture-12

« *Architecture for IP Flow Information Export* »

- Statut : en cours d'évaluation IESG, expire le 10 Mars 2007
- Résumé :
  - Description de l'architecture d'IPFIX pour la mesure des flux et l'export de l'information sur ces flux depuis un équipement réseau qui utilise IPFIX vers un collecteur pour analyse.

# Architecture d'IPFIX : draft-ietf-ipfix-architecture-12

« Architecture for IP Flow Information Export »



# draft-ietf-ipfix-as-10

## « *IPFIX Applicability* » :

- Statut : en cours d'évaluation IESG, expires en Janvier 2007
- Résumé :
  - Description du champ d'application du protocole IPFIX. Comment des applications peuvent utiliser IPFIX. Décrit la pertinence des éléments d'informations d'un message IPFIX et montre les possibilités mais aussi les limitations du protocole IPFIX.



# draft-ietf-ipfix-info-14

## «*Information Model for IP Flow Information Export*»

- Statut : en cours d'évaluation IESG, expire le 26 Avril 2007
- Résumé :
  - Description du modèle d'information pour l'export des informations sur les flux IP (message IPFIX) :
    - Décrit tous les éléments d'information disponible (IP\_SRC...)
  - Ce modèle est employé par le protocole IPFIX pour l'encodage :
    - De l'information sur les flux IP (Template Record, Data Record)
    - De l'information concernant un point d'observation du trafic, un processus de comptage ou un processus d'export (Option Template Record Scope)
    - Ce modèle peut être réutilisable par d'autres protocoles, interfaces et applications.

# draft-ietf-ipfix-testing-00

## « *IP Flow Information eXport (IPFIX) Testing* »

- Statut : Draft actif, Expire le 19 Avril 2007
- Résumé :
  - Description d'une liste de tests pour aider à la mise en œuvre d'un système IPFIX. Ces tests aident à la validation des principales fonctionnalités d'un exporter IPFIX et d'un collecteur IPFIX. Ils servent aussi à vérifier l'interopérabilité entre des systèmes IPFIX différents.

# draft-ietf-ipfix-biflow-00

## « *Bidirectional Flow Export using IPFIX* »

- Statut : Draft actif, expire le 3 mars 2007
- Résumé :
  - Description d'une méthode efficace permettant d'exporter dans un même message IPFIX les données d'un flux bidirectionnel (Biflow).

# draft-ietf-ipfix-implementations-guidelines-01

## « *IPFIX Implementation Guidelines* »

- Statut : Draft actif, expire le 26 Avril 2007
- Résumé :
  - Directives/Indications sur l'implémentation et l'utilisation d'IPFIX. Ces directives concernent principalement la gestion des templates, les solutions de transport spécifique, l'implémentation des processus d'export et de collecte...

# draft-ietf-ipfix-reducing-redundancy-01

« *Reducing redundancy in IPFIX and PSAMP reports* »

- Statut : Draft Actif, expire le 26 Avril 2007
- Résumé :
  - Méthode pour réduire la bande passante utilisée dans l'export des messages IPFIX. Il s'agit de séparer les informations communes à plusieurs flux des informations spécifiques à un flux en particulier. Ainsi, les informations communes ne sont transmises qu'une seule fois dans un « options template record », et les informations spécifiques seront envoyées en association à une information commune grâce à un unique identificateur.

# Autres drafts : Ajouts, Modifications, Évolutions...

- Cf. <http://tools.ietf.org/wg/ipfix> :
  - draft-bclaise-ipfix-reliability-01.txt-01
  - draft-boschi-ipfix-biflow-00.txt-00
  - draft-boschi-ipfix-implementation-guidelines-02.txt-02
  - draft-boschi-ipfix-reducing-redundancy-02.txt-02
  - draft-coene-rserpool-applic-ipfix-03.txt-03
  - draft-dietz-ipfix-mib-01.txt-01
  - draft-dressler-ipfix-aggregation-03.txt-03
  - draft-irino-ipfix-ie-order-00.txt-00
  - draft-kobayashi-ipfix-concentrator-mib-01.txt-01
  - draft-kobayashi-ipfix-concentrator-model-01.txt-01
  - draft-kobayashi-ipfix-mediator-01.txt-01
  - draft-manjunath-ipfix-shifted-feedback-00.txt-00
  - draft-muenz-ipfix-configuration-00.txt-00
  - draft-schmoll-ipfix-testing-00.txt-00
  - draft-stephan-ipfix-isp-templates-00.txt-00
  - draft-trammell-ipfix-biflow-02.txt-02
  - draft-trammell-ipfix-file-02.txt-02
  - draft-yuzhi-ipfix-transport-tls-00.txt-00