

# Architecture Draft: Changes in -02.txt

## Overview

- Definitions
- Protocol
- Security

## Definitions

- Definition of 'Flow'
  - IP packets replaces packets
- *Added* a third set of properties to those defining a flow
  1. One or more of packet header fields (e.g. destination IP address)
  2. One or more properties of the packet itself (e.g. packet length)
  3. One or more of fields derived from packet treatment (e.g. AS number)
- *Deleted* definition of 'IPFIX Device'

# Protocol

- Control Information, Data Stream replaces Control Stream, Data Stream
- IPFIX Protocol on IPFIX Device (At Export Process):  
*added*
  4. Exchange control information from the collector, monitor export process and detect any overload in the process of exporting
- IPFIX Protocol on Collector: *added*
  2. Ability to indicate flow record losses to the exporting IPFIX device and/or IPFIX users

## Security

3. For long aging flows, the exporter SHOULD export the flow records on regular basis, in order to:  
*added*
  - c. Prevent an attacker from indefinitely delaying the delivery of flow information to an IDS application by intentionally generating packets which fall within long aging flows.