



lobster

An IST Project



Information Society
Technologies

<http://www.ist-lobster.org>

NetFlow and IPFIX overview

LOBSTER tutorial

6 May 2005

Arne Øslebø

UNINETT

arneos@uninett.no



NetFlow

- Cisco technology
 - 1996
- Provides detailed view of network behavior
- Commonly used for:
 - Security applications
 - Application and user monitoring
 - Billing
 - AS Peer monitoring
 - Traffic engineering and analysis



IP traffic flow



An IST Project

<http://www.ist-lobster.org>

- IPFIX definition:
 - A set of IP packets passing an observation point in a network during a certain time interval. All packets belonging to a particular flow have a set of common properties.
- Flow Key
 - Each of the properties that are used for defining a flow



- Flow key:
 - Source IP address
 - Destination IP address
 - Source port
 - Destination port
 - Layer 3 protocol type
 - TOS
 - Input interface



NetFlow v5 (2)

- Flow record
 - Source and destination IP address
 - Next hop router's IP address
 - Input and output interface index
 - Packets and bytes in the flow
 - sysUptime at start and end of flow
 - TCP/UDP source and destination port number
 - Type of service
 - TCP flags
 - IP protocol
 - Source and destination AS number
 - Source and destination address prefix mask bits



Flow expiration

- Inactive timer
 - 15 seconds
- Active timer
 - 30 minutes
- Full cache
 - Oldest flows are expired
- RST or FIN TCP flag

- NetFlow v1
 - Original, no longer used
- NetFlow v5
 - Most commonly used today
- NetFlow v7
 - Specific to Cisco switches
- NetFlow v8
 - Aggregated NetFlow
- NetFlow v9
 - Basis for IPFIX



- IETF working group for standardizing NetFlow
 - Based on NetFlow v9
- Flexible flow key
 - The properties used for distinguishing flows can be configured
- Flexible flow export
 - Information in flow records is not fixed
- Reliable transport
 - SCTP standard protocol



Flow templates

- Defines the contents of flow records
- Each template is identified by a unique ID number
- Each flow record refers to a template ID
- Can have different templates for different interfaces

Header
Set1
Set2
Set3
....
SetN

- Three different types of sets:
 - Data
 - Flow record
 - Template
 - Template information
 - Options
 - Metering process information
 - Sampling rate and method for a specific interface



Summary

- NetFlow aggregates network traffic by collecting packets with the same attributes into flow records.
- NetFlow v5 is currently the most commonly used
- IETF IPFIX is standardizing NetFlow
 - Flexible flow records
 - Templates
 - Reliable transport protocol
 - SCTP