Cisco IOS Flexible NetFlow

TREX 2009

Timo Perttula

tperttul@cisco.com

Cisco IOS NetFlow – Historiaa

- Developed and patented at Cisco® Systems in 1996
- NetFlow is the defacto standard for acquiring IP operational data
- Provides network and security monitoring, network planning, traffic analysis, and IP accounting
- IOS (myös XR) standardi ominaisuus - ei erillistä lisenssiä
- Yleensä moderneissa laitteissa HW-tuki

NetFlow Käyttökohteita

Service Provider
Network Infrastructure Optimization and Planning
Peering Arrangements
Traffic Engineering
Accounting and Billing
Security Monitoring and Incident (DDoS) Detection

Enterprise
Internet Access Monitoring
User Monitoring/Profiling
Application Monitoring
Billing for Departments
Security Monitoring and Incident (DDoS) Detection

Data at ANY granularity to understand network use: who, what, where, when and how

Cisco IT käyttää NetFlowta “Eat your own dog food”

- **Characterize IP traffic and account for how and where it flows**
  - **Capacity Planning**
  - **Detection of Unauthorized WAN Traffic**
  - **Reduction in Peak WAN Traffic**
  - **Validation of QoS Parameters and BW allocation**
  - **Calculating Total Cost of Ownership for Applications**
  - **Analysis of VPN Traffic and Tele-Commuter Behavior**
  - **Total Avoidance of SQL Slammer Worm**
  - **Transition from Managed DSL service to Internet VPN**

Use of NetFlow	NMS and Usage
Security Monitoring	Network traffic analysis by application with BGP. Anomaly detection, Arbor Networks
WAN Aggregation and Edge	Network traffic analysis by application, for capacity planning using NetQoS
Core routers and NAT Gateway	Collection of historical data, useful for forensics and diagnostics with Flow Tools

Rautatuki läpi tuotelinjan

Enterprise & aggregation/edge

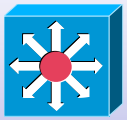
Core

Cisco IOS Software Release 12.2S

Cisco 7200/7500 Series

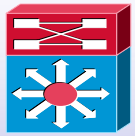
Cisco 7300 Series

Cisco ASR 1000 Series



Cisco 4500 Series ASIC

Cisco 10000 Series ASIC



Cisco Catalyst 6500; Cisco 7600 Series ASIC

Release 12.0S/IOS-XR

Cisco 12000 Series ASIC

CRS-1 ASRxk ASIC

Access

Cisco IOS Software Releases

Cisco 800 Series

Cisco 1700 1800 Series

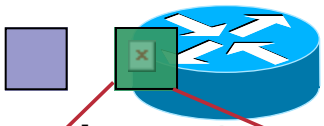
Cisco 2600 2800 Series

Cisco 3700 3800 Series

Cisco 7200/ 7300 Series

NetFlow Key Fields Creating Flow Records

Example 1



Inspect Packet

Key Fields	Packet 1
Source IP	1.1.1.1
Destination IP	2.2.2.2
Source port	23
Destination port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Create Flow record in the Cache

Source IP	Dest. IP	Dest. I/F	Protocol	TOS	…	Pkts
1.1.1.1	2.2.2.2	E1	6	0	…	11000

7 pre-defined key fields

1. **Inspect packet for key field values**
2. **Compare set of values to NetFlow cache**
3. **If the set of values are unique create a flow in cache**
4. **Inspect the next packet**

Example 2

Inspect Packet

Key Fields	Packet 2
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source port	23
Destination port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Add new Flow to the NetFlow Cache

Source IP	Dest. IP	Dest. I/F	Protocol	TOS	…	Pkts
3.3.3.3	2.2.2.2	E1	6	0	…	11000
1.1.1.1	2.2.2.2	E1	6	0	…	11000

Flow Non-Key Fields and Statistics

- *Non-key fields* are used not to define a flow and are exported along with the flow and provide additional information
- Traditional IP NF non-key fields
  - source and destination AS's
  - source and destination IP prefix masks
  - IP address of next-hop router
  - TCP flags
  - output interface
- NF features provide per flow statistics
  - number of packets and bytes in flow
  - time-stamps for first and last packets in flow

Traditional Layer 3 NetFlow Cache

Key Fields in Yellow
Non-Key Fields white

1. Create and update flows in NetFlow cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A 2	/24	5	00A2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A 1	/24	180	00A1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- Inactive Timer Expired (15 sec is default)
- Active Timer Expired (30 min is default)
- NetFlow Cache is Full (Oldest flows are expired)
- RST or FIN TCP Flag

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation

No

Yes

4. Export version

Non-aggregated flows—export version 5 or 9

ie: Protocol-Port Aggregation Scheme Becomes

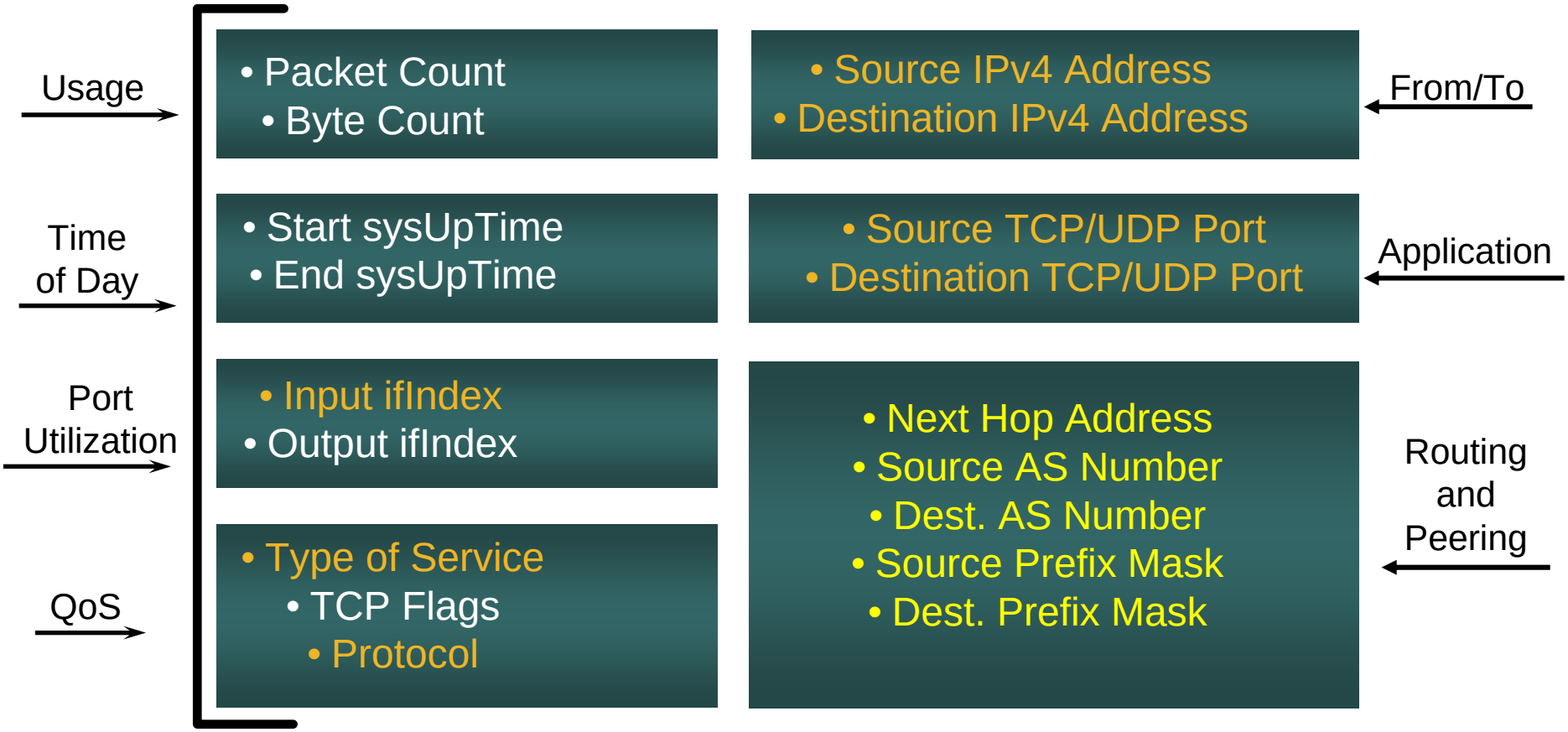
Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	00A2	1528

Aggregated Flows—Export Version 8 or 9

5. Transport protocol

Export Packet

Version 5 - Flow Export Format



Version 5 used extensively today

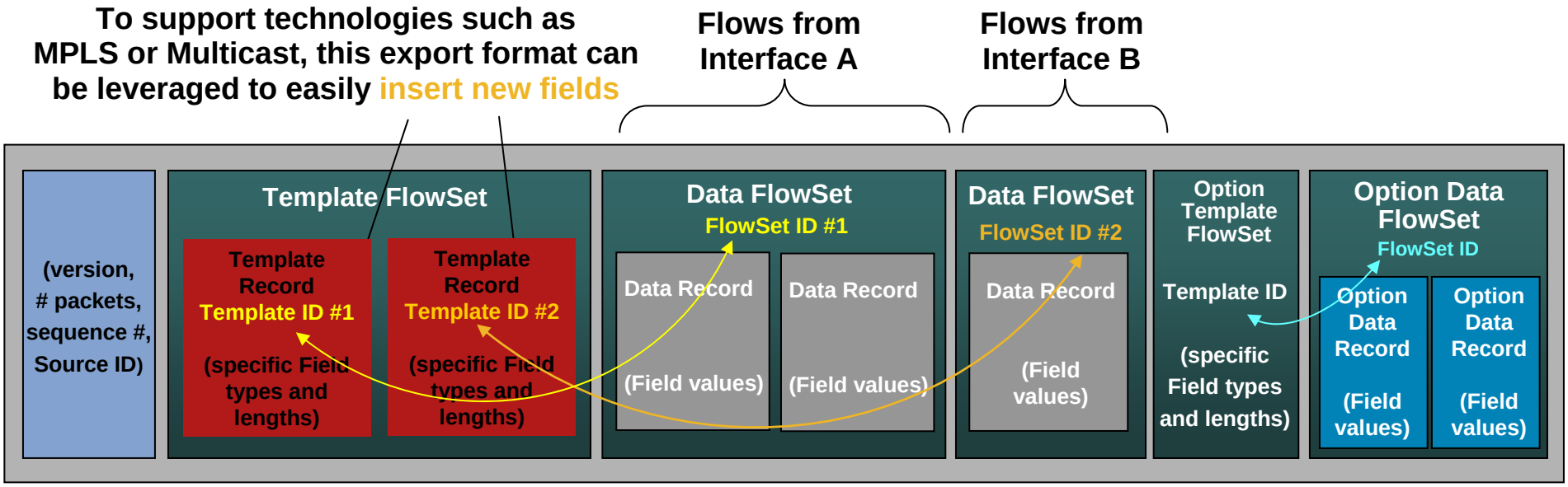
Extensibility and Flexibility Requirements Phases Approach

- New requirements: build a flexible and extensible NetFlow
- Phase 1: NetFlow version 9, completed
  - Advantages: extensibility
    - Integrate new technologies/data types quicker (MPLS, IPv6, BGP next hop, etc.)
    - Integrate new aggregations quicker
  - Note: for now, the template definitions are fixed
- Phase 2: Flexible NetFlow, completed
  - Advantages: cache and export content flexibility
    - User selection of flow keys
    - User definition of the records

Exporting Process

Metering Process

NetFlow v9 Export Packet



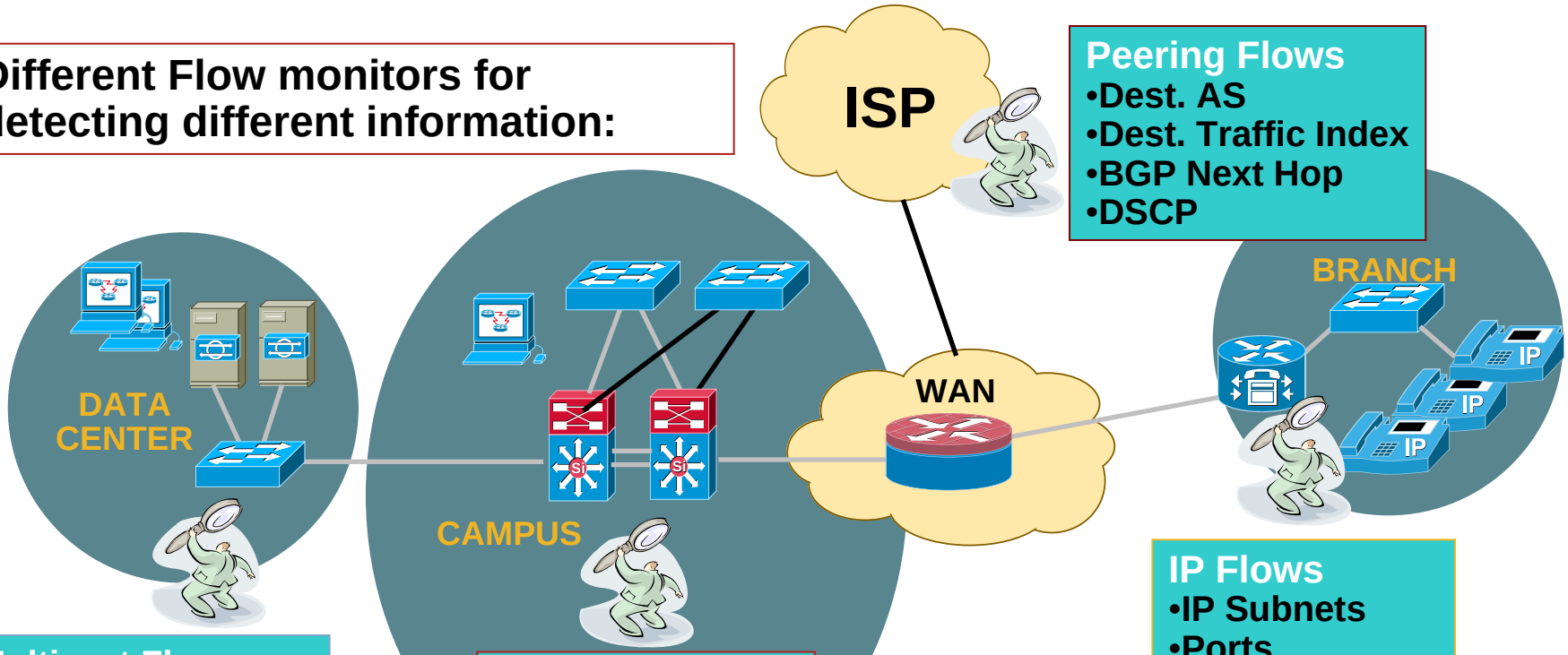
- Matching ID numbers are the way to associate template to the data records
- The header follows the same format as prior NetFlow versions so collectors will be backward compatible
- Each data record represents one flow

Flexible NetFlow Benefits

- Superset of Cisco IOS Accounting features
- Increased flexibility, scalability, customization beyond today's NetFlow
- The ability to monitor a wider range of packet information – beyond L2/L3/L4
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network attributes
- Consistent CLI across features and platforms

Flexible NetFlow Tracking data with Flow Monitors

Different Flow monitors for detecting different information:



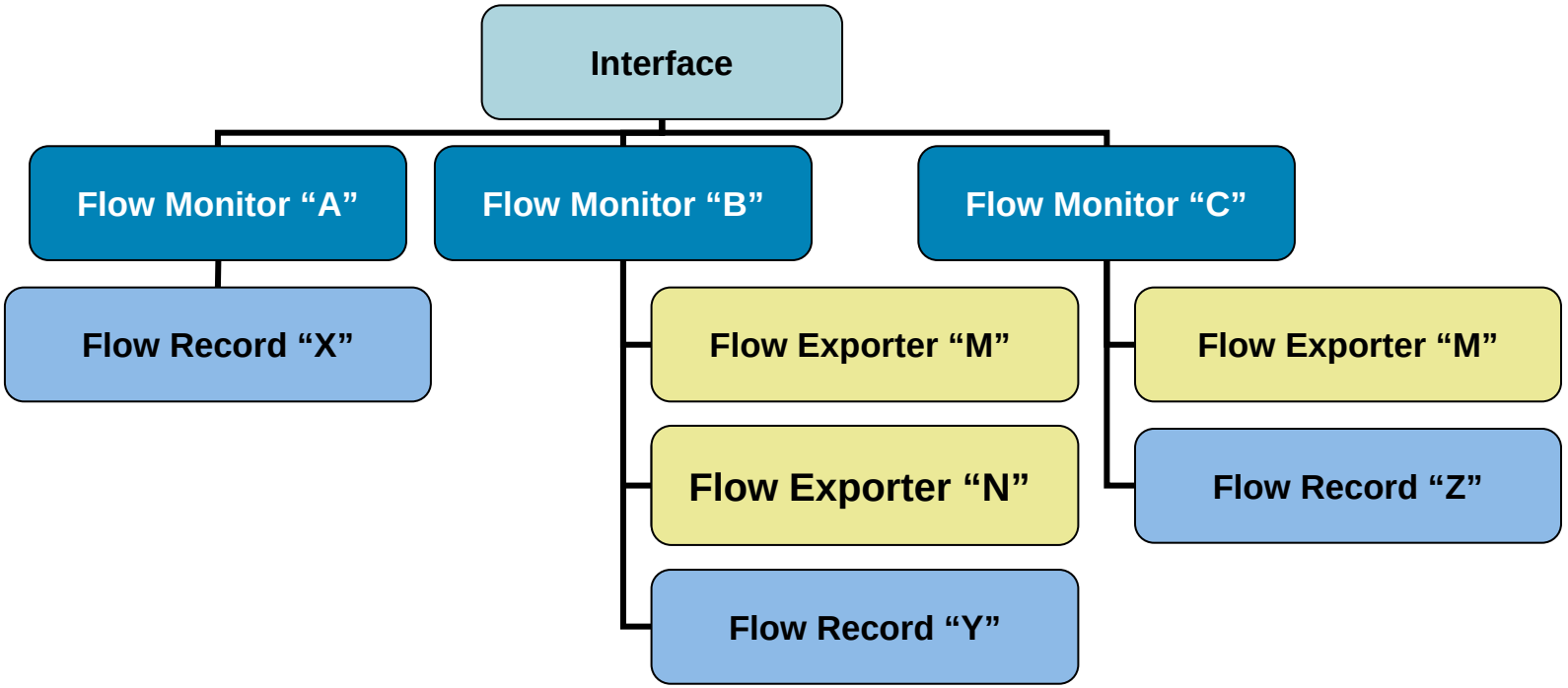
Peering Flows
- Dest. AS
- Dest. Traffic Index
- BGP Next Hop
- DSCP

IP Flows
- IP Subnets
- Ports
- Protocol
- Interfaces
- Egress/Ingress

Multicast Flows
- Protocol
- Ports
- IP Subnets
- Packet Replication

Security Flows
- Protocol
- Ports
- IP Addresses
- TCP Flags
- Packet Section

Flexible NetFlow Model



- A single record per monitor
- Potentially multiple monitors per interface
- Potentially multiple exporters per monitor

Konfigurointi

- **The key components that need to be configured:**
- 1. Configure the exporter if it is to export to a collector
- 2. Configure the user defined Flow Record with key and non-key fields
- 3. Configure the Flow Monitor with the user defined Flow Record and Flow Exporter attached to the monitor
- 4. Add the Flow Monitor to the interface to monitor either ingress (input) or egress (output traffic)

Esimerkki perinteinen netflow (flexible mutta perusformaatilla)

Configure the Exporter

```
Router(config)#flow exporter my-exporter-server
Router(config-flow-exporter)#destination 1.1.1.1
```

Configure the Flow Record

Not necessary for predefined types

Configure the Flow Monitor

```
Router(config)#flow monitor my-monitor
Router(config-flow-monitor)#exporter my-exporter-server
Router(config-flow-monitor)#record netflow original-input
```

Configure the Interface

```
Router(config)#int s3/0
Router(config-if)#ip flow monitor my-monitor input
```

Predefined Record for Traditional NetFlow

- All aggregations are possible, for quick backwards compatibility

```
Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# record netflow ipv4 ?
  as                     AS aggregation schemes
  as-tos                 AS and TOS aggregation schemes
  bgp-nexthop-tos        BGP next-hop and TOS aggregation schemes
  destination-prefix     Destination Prefix aggregation schemes
  destination-prefix-tos Destination Prefix and TOS aggregation schemes
  original-input         Traditional IPv4 input NetFlow
  original-output        Traditional IPv4 output NetFlow
  prefix                 Source and Destination Prefixes aggregation schemes
  prefix-port            Prefixes and Ports aggregation scheme
  prefix-tos             Prefixes and TOS aggregation schemes
  protocol-port          Protocol and Ports aggregation scheme
  protocol-port-tos      Protocol, Ports and TOS aggregation scheme
  source-prefix          Source AS and Prefix aggregation schemes
  source-prefix-tos      Source Prefix and TOS aggregation schemes
```

Configure a User-Defined Flow Record

Configure the Exporter

```
Router(config)#flow exporter my-exporter

Router(config-flow-exporter)#destination 1.1.1.1
```

Configure the Flow Record

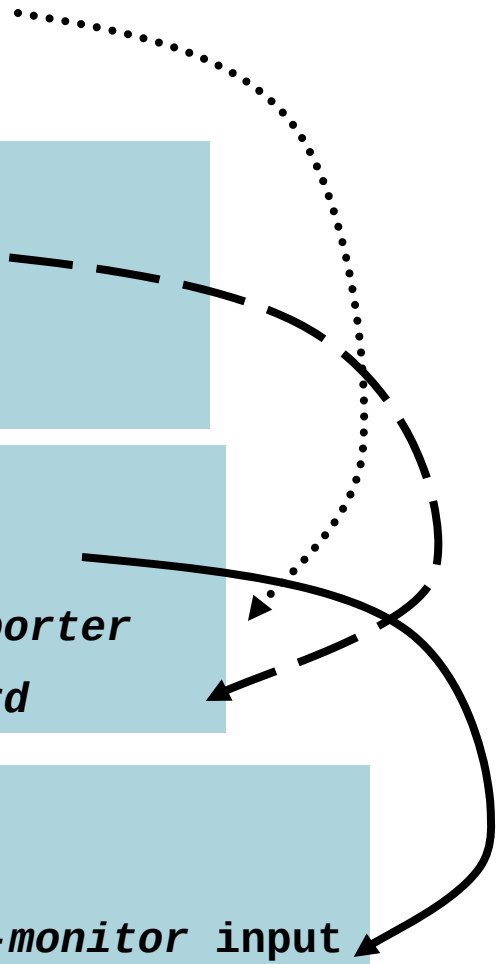
```
Router(config)#flow record my-record
Router(config-flow-record)#match ipv4 icmp type
Router(config-flow-record)#match ipv4 icmp code
Router(config-flow-record)#collect counter bytes
```

Configure the Flow Monitor

```
Router(config)#flow monitor my-monitor

Router(config-flow-monitor)#exporter my-exporter

Router(config-flow-monitor)#record my-record
```

Configure the Interface

```
Router(config)#int s3/0

Router(config-if)#ip flow monitor my-monitor input
```



Flexible Flow Record: Key Fields

IPv4	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	TTL
Protocol	Options
Fragmentation Flags	Version
Fragmentation Offset	Precedence
ID	DSCP
Header Length	TOS
Total Length	

Routing
Destination AS
Peer AS
Traffic Index
Forwarding Status
Is-Multicast
IGP Next Hop
BGP Next Hop

Flow
Sampler ID
Direction

Interface
Input
Output

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

Flexible Flow Record: Key Fields

IPv6	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	DSCP
Protocol	Extension
Traffic Class	Hop-Limit
Flow Label	Lenght
Option Header	Next-header
Header Length	Version
Payload Length	

Routing
Destination AS
Peer AS
Traffic Index
Forwarding Status
Is-Multicast
IGP Next Hop
BGP Next Hop

Flow
Sampler ID
Direction

Interface
Input
Output

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

Flexible Flow Record

- Any of the potential “key” fields: will be the value of the first packet in the flow
- Plus

Counters
Bytes
Bytes Long
Bytes Square Sum
Packet
Packet Long

Timestamp
sysUpTime First Packet
sysUpTime First Packet

IPv4
Total Length Minimum
Total Length Maximum
TTL Minimum
TTL Maximum

Sh komennot

- Show Commands Available within Flexible NetFlow
- **Show run flow [exporter | monitor | record]** Parses the show run command for output
- **Show flow [exporter | interface | monitor | record]** Shows detailed information about the Flexible NetFlow component
- **Show flow monitor [*name of monitor*] cache** Shows the contents of the Flexible NetFlow cache in comma separated format (CSV), table or record (list) format.

Flexible Flow Monitor Caches types

- Normal cache
  - Similar to today's NetFlow
  - More flexible active and inactive timers: one second minimum
- Immediate cache
  - Flow accounts for a single packet
  - Desirable for real-time traffic monitoring, DDoS detection, logging
  - Desirable when only very small flows are expected (ie: sampling)
  - Caution: may result in a large amount of export data
- Permanent cache
  - To track a set of flows without expiring the flows from the cache
  - Entire cache is periodically exported (update timer)
  - After the cache is full (size configurable), new flows will not be monitored
  - Uses update counters rather than delta counters

Complete Permanent Flexible NetFlow Configuration Example

- Per DSCP accounting flow record definition:

```
Router(config)# flow record my-dscp-record
Router(config-flow-record)# match ipv4 dscp
Router(config-flow-record)# match interface input
Router(config-flow-record)# collect counter bytes long
Router(config-flow-record)# collect counter packets long

Router(config)# flow monitor my-dscp-monitor
Router(config-flow-record)# description dscp:bytes and packets
Router(config-flow-record)# record my-dscp-record
Router(config-flow-record)# cache type permanent
Router(config-flow-record)# cache entries 256

Router(config)# interface GigabitEthernet 0/1
Router(config)# ip flow monitor my-dscp-monitor input
```

64 Bit Counter

- This would replace “IP accounting precedence”

Complete Permanent Flexible NetFlow Configuration Example

Extra Options:
CSV, Table, Record

```
Router#show flow monitor my-dscp-monitor cache
  Cache type:                               Permanent
  Cache size:                                     256
  Current entries:                                  0
  High Watermark:                                   0

  Flows added:                                      0
  Updates sent              (  1800 secs)           0

IP DSCP  INTF INPUT      bytes long perm    pkts long perm
=======  ==========   ==================   ===============

 0x00     Gi0/1                    1000                 10
 0x01     Gi0/1                     500                  5
```

Flow Keys in Upper Case

Packet Section Fields

- Contiguous chunk of a packet of a user configurable size, used as a key or a non-key field
- Sections used for detailed traffic monitoring, DDoS attack investigation, worm detection, other security applications
- Chunk defined as flow key, should be used in sampled mode with immediate aging cache
- Starts at the beginning of the IPv4 header

```
collect or match ipv4 header <size in bytes>
```

- Immediately follows the IPv4 header

```
collect or match ipv4 payload <size in bytes>
```

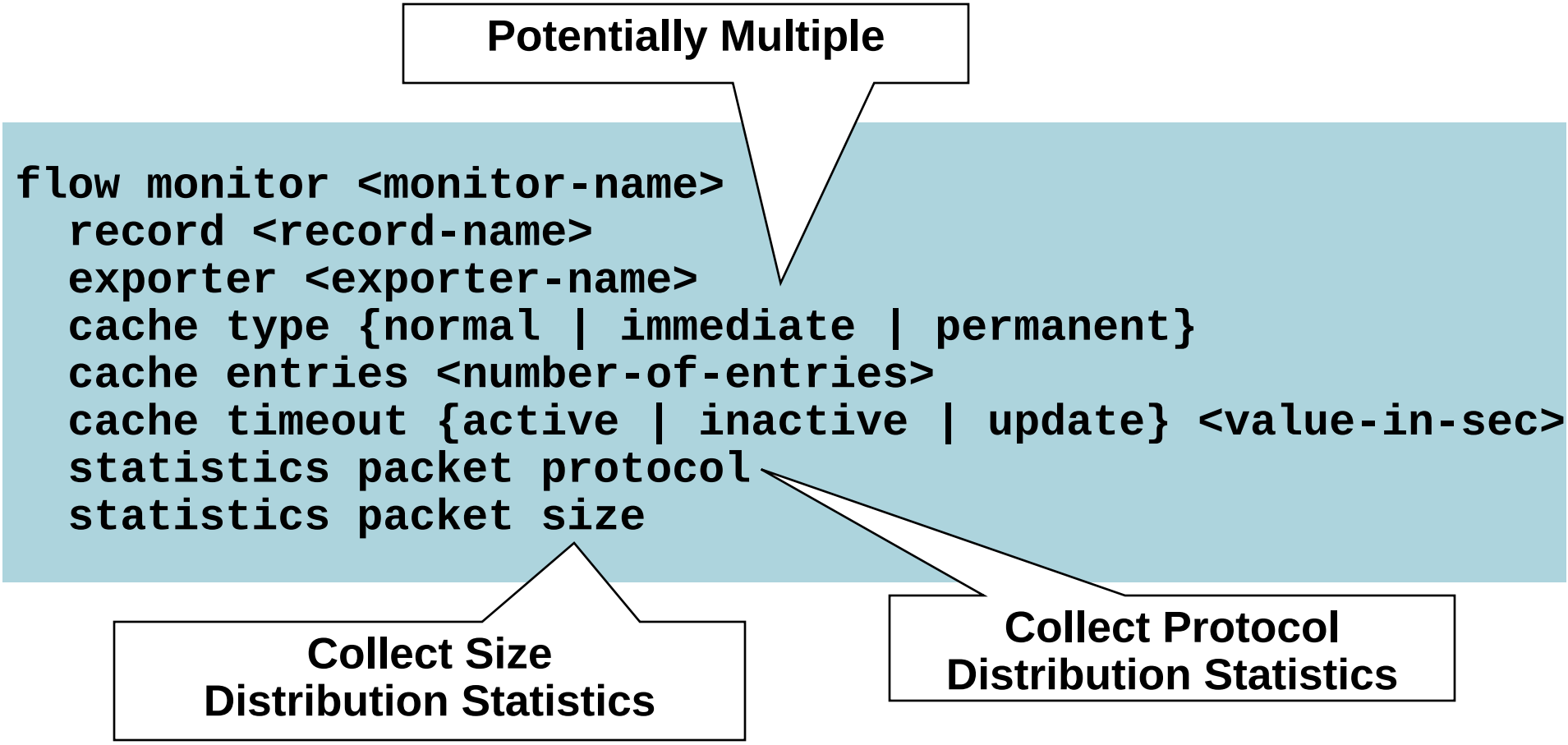
Flow Exporter Configuration

```
flow exporter <exporter-name>
     destination <ipv4-address> [vrf <vrf-name>]
     dscp <value>
     option {exporter-stats | interface-table | sampler-table}
       timeout <value in sec>
   source <interface-name>
     template resend timeout <value in sec>
     transport udp <destination-port>
     ttl <value>
```

3 Types of Options Data Record

(Option) Template Sent Every X Seconds

Flexible Monitor Configuration



Flexible NetFlow Activation on Interface

Send the "sampler-table" Option

```
Router(config-if)# ip flow monitor <monitor-name>
                                  [sampler <sampler-name>]
                                [input | output]
```

For the Input or Output Traffic Does Not Determine the Flow Key

- Deterministic or random is available

```
Router(config)# sampler <sampler-name>
mode [deterministic | random] <value N> out-of <value M>
```

NetFlow Performance Paper Tests

- NetFlow performance on software platforms depends on number of flows in the cache
- NetFlow Performance paper covers data on the topic

  Paper at www.cisco.com/go/netflow under “White Papers”

  ✓0, 1, and 2 NetFlow data export destinations

  ✓Initial performance after enabling

  ✓V8 Aggregation vs. v5, V9 performance

  ✓“Full” NetFlow vs. 1:100 sampled NetFlow

  ✓Hardware: Cisco 1841, 2600, 2800, 3600, 3800, 7200, 7300, 6500, 12k

Updated Performances document available for Flexible NetFlow + new platforms Cisco1800, Cisco2800, Cisco3800, Cisco 7200 NPE-G2