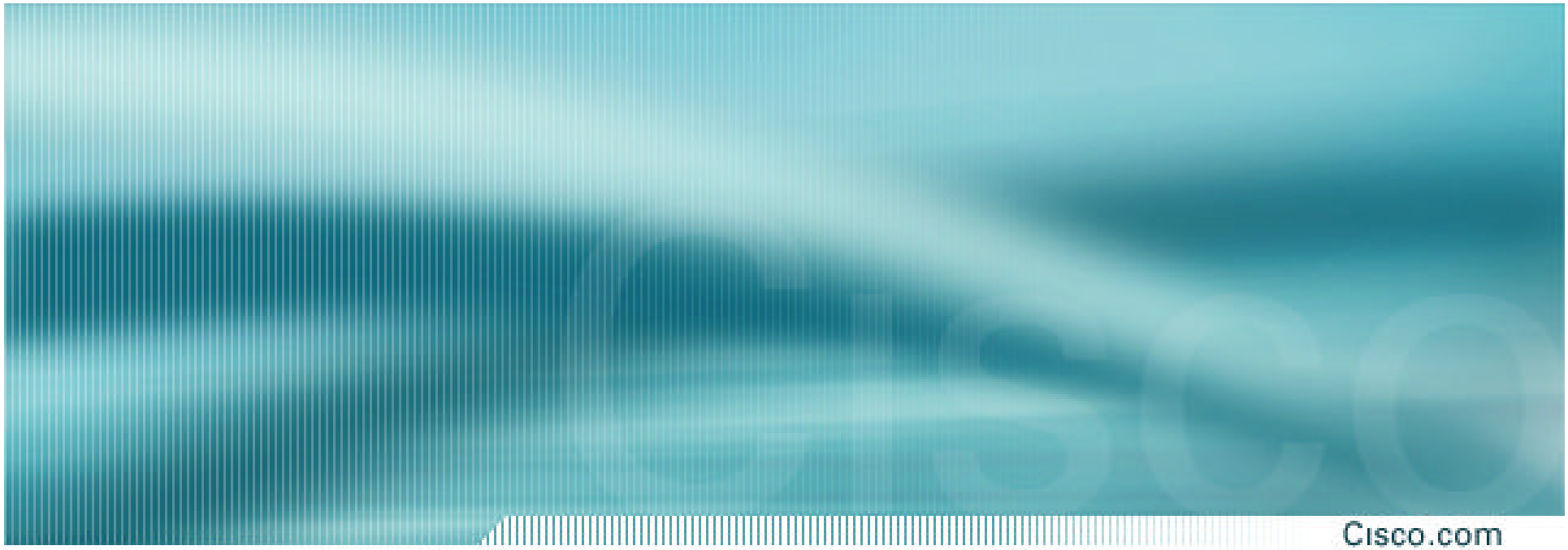

Cisco Systems



NetFlow Services

Benoit Claise

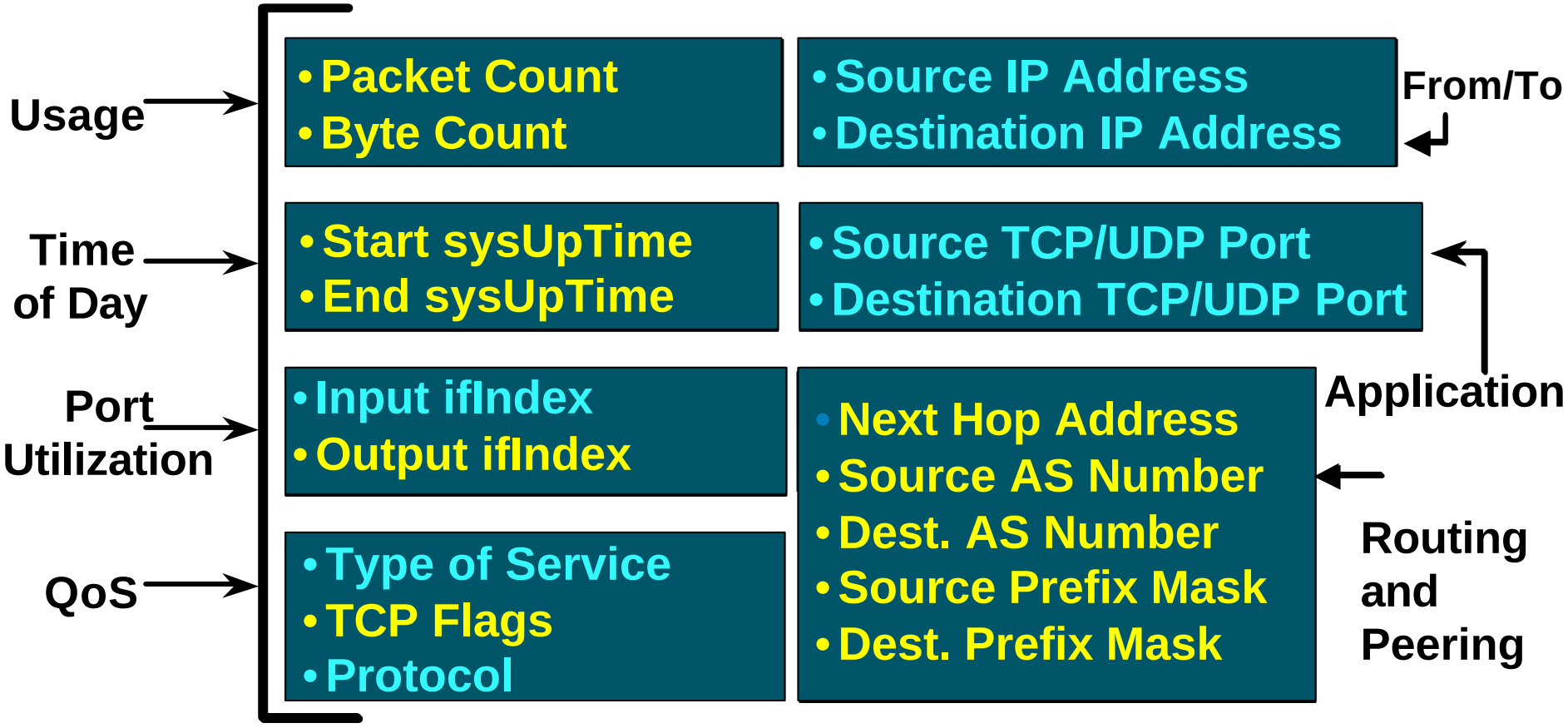
bclaise@cisco.com

RIPE 44, Amsterdam

NetFlow Services

- Look at packets arriving on interface
- Capture traffic statistics per flow
- The who, what, where, when, and how much IP traffic questions are answered

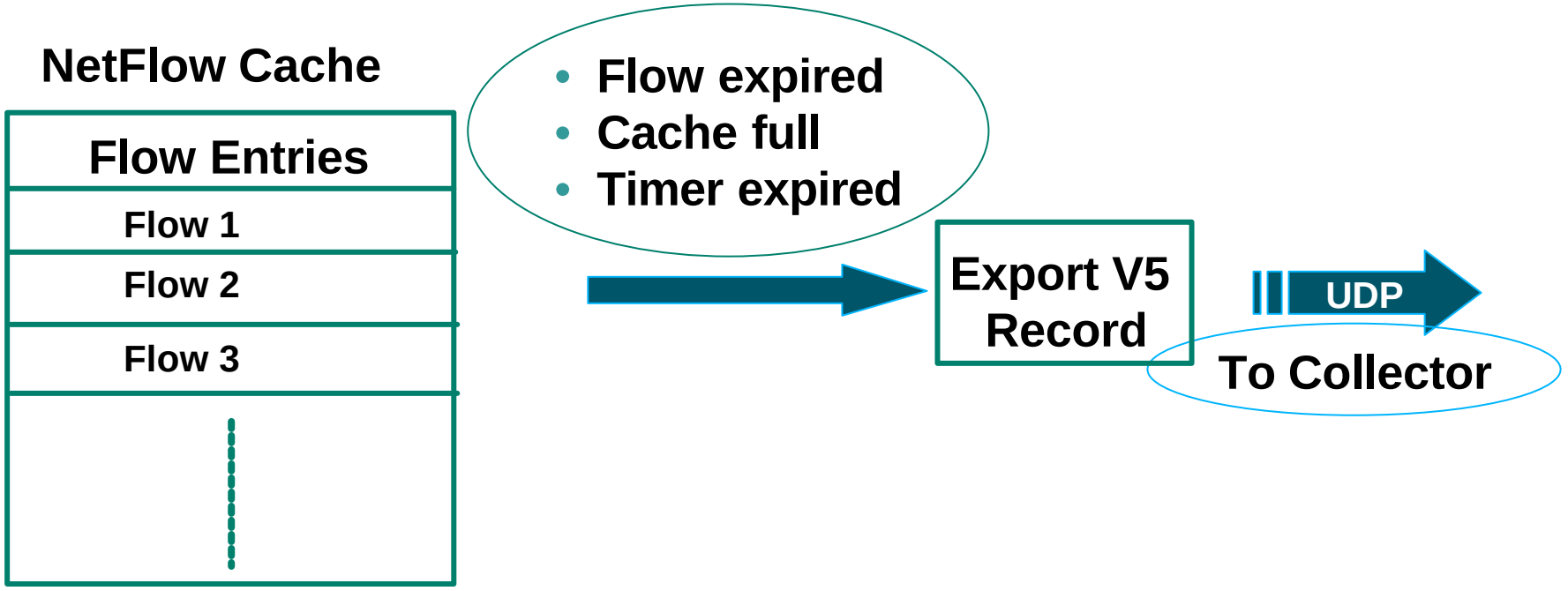
Version 5 Flow Format



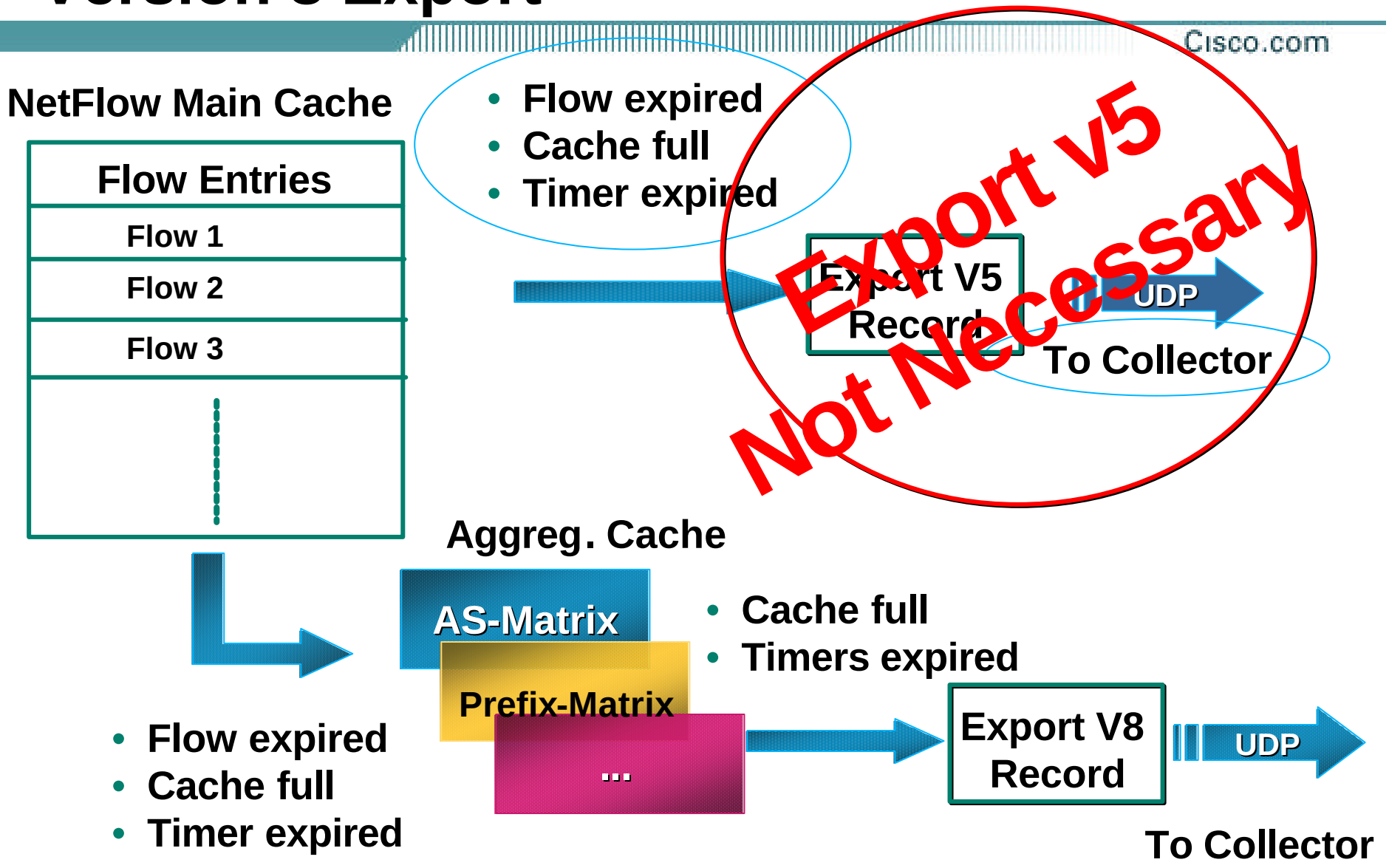
NetFlow Possible Applications

	NetFlow
Network Monitoring	X
Network Planning	X
Security Analysis	X
Application Monitoring	X
User Monitoring	X
Traffic Engineering	X
Peering Agreement	X
Usage-based Billing	X
Destination Sensitive Billing	X

Version 5 Export



Version 8 Export



Version 8 - Flow Format

Cisco.com

	AS	Protocol-Port	Source-Prefix	Destination-Prefix	Prefix
Source Prefix			·		·
Source Prefix Mask			·		·
Destination Prefix				·	·
Destination Prefix Mask				·	·
Source App Port		·			
Destination App Port		·			
Input Interface	·		·		·
Output Interface	·			·	·
IP Protocol		·			
Source AS	·		·		·
Destination AS	·			·	·
First Timestamp	·	·	·	·	·
Last Timestamp	·	·	·	·	·
# of Flows	·	·	·	·	·
# of Packets	·	·	·	·	·
# of Bytes	·	·	·	·	·

Version 8 - Flow Format

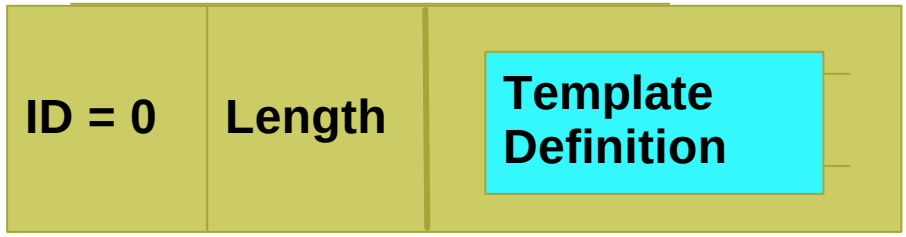
Cisco.com

	AS-TOS	Protocol-Port-TOS	Source-Prefix-TOS	Destination-Prefix-TOS	Prefix-TOS	Prefix-Port
Source Prefix			·		·	·
Source Prefix Mask			·		·	·
Destination Prefix				·	·	·
Destination Prefix Mask				·	·	·
Source App Port		·				·
Destination App Port		·				·
Input Interface	·	·	·		·	·
Output Interface	·	·		·	·	·
IP Protocol		·				·
Source AS	·		·		·	
Destination AS	·			·	·	
TOS	·	·	·	·	·	·
First Timestamp	·	·	·	·	·	·
Last Timestamp	·	·	·	·	·	·
# of Flows	·	·	·	·	·	·
# of Packets	·	·	·	·	·	·
# of Bytes	·	·	·	·	·	·

NetFlow Version 9, extensible and flexible

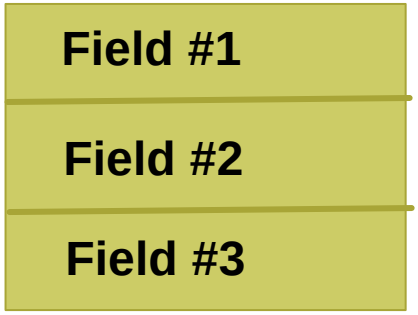
Packet

Template Definition (Template FlowSet)



Flow Records (Data FlowSet)

Record

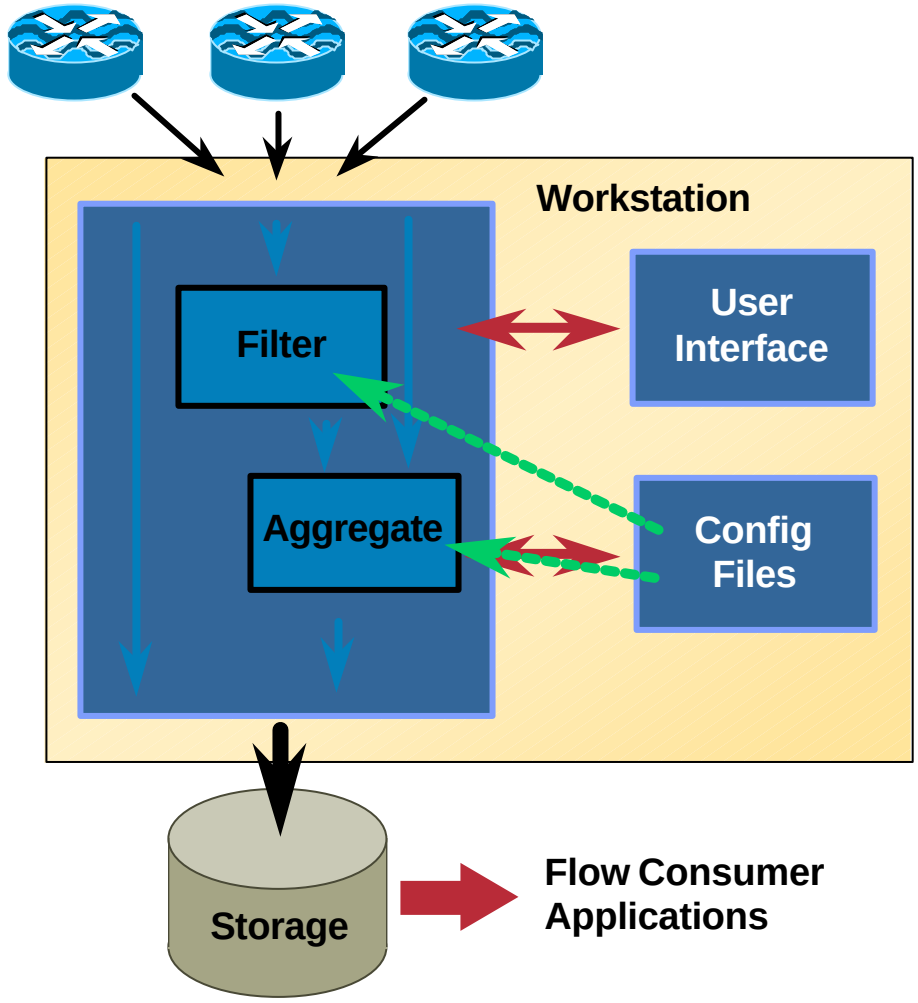


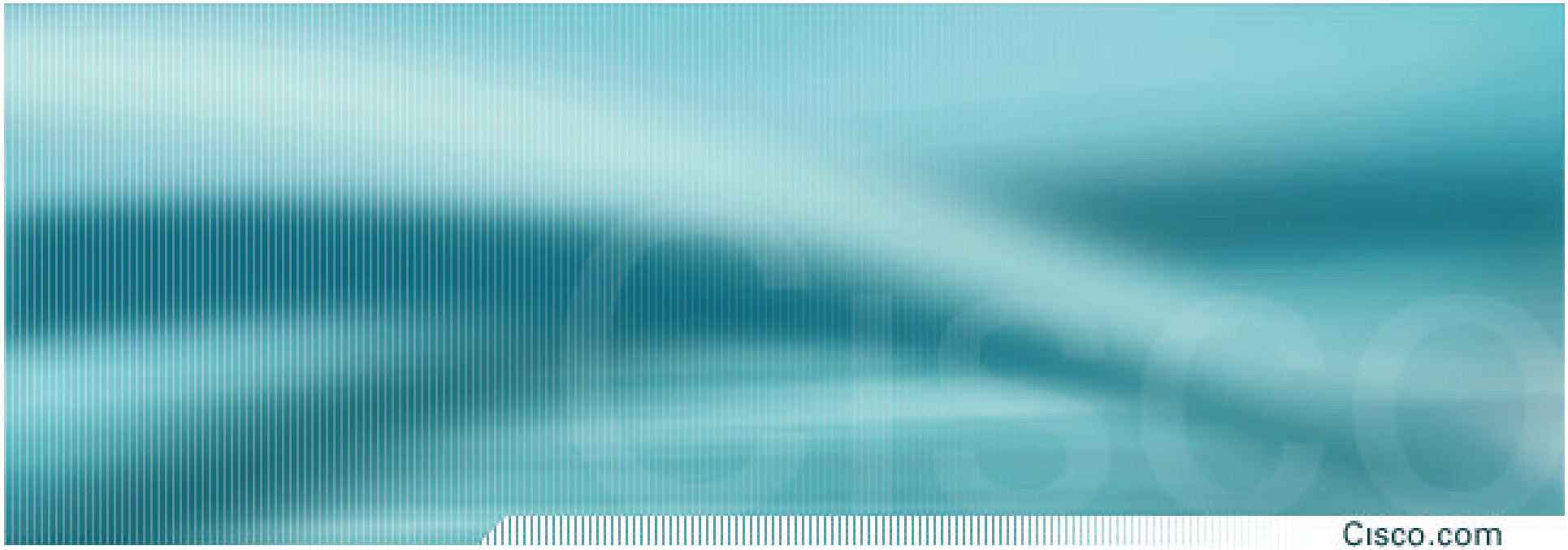
NetFlow FlowCollector

- Flow record reception
- Data volume reduction

  Filtering, Aggregation
- Flexible thread language
- File storage

  Flat or binary and compression in 3.0
- File cleanup
- Solaris, HP-UX, Linux appliance
- No flow de-duplication



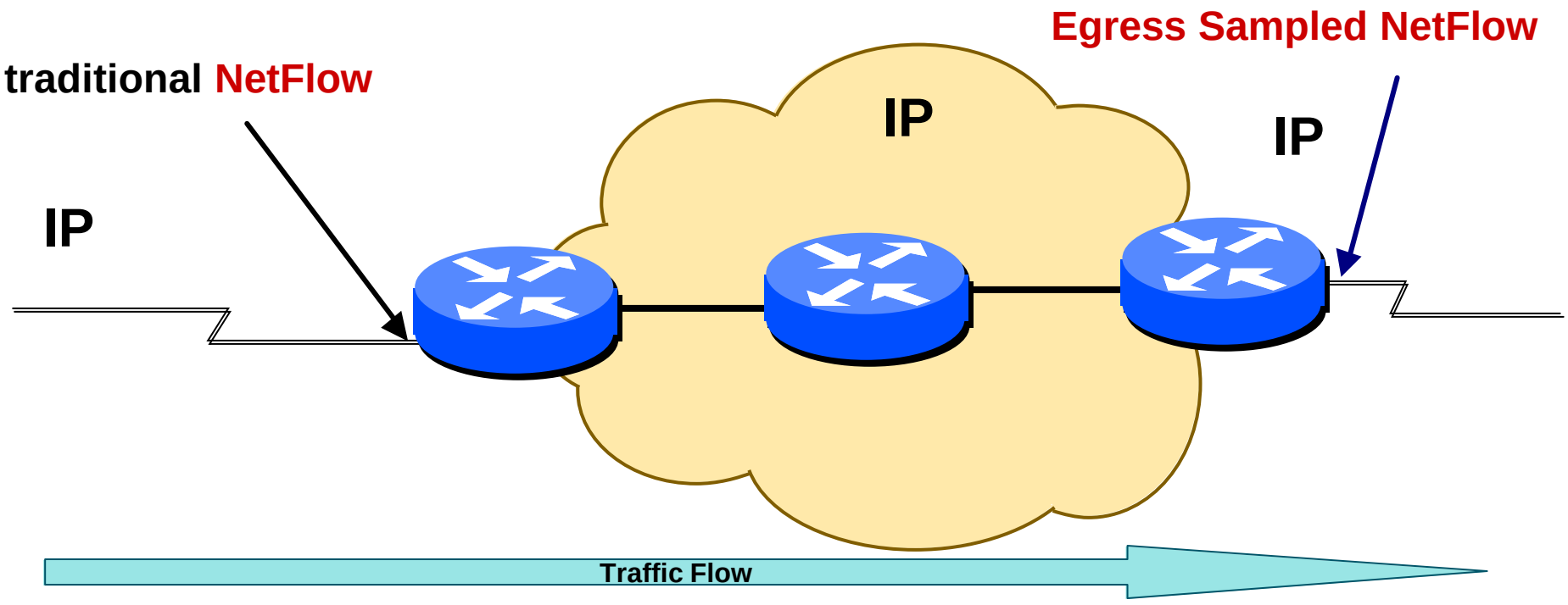


Key Features

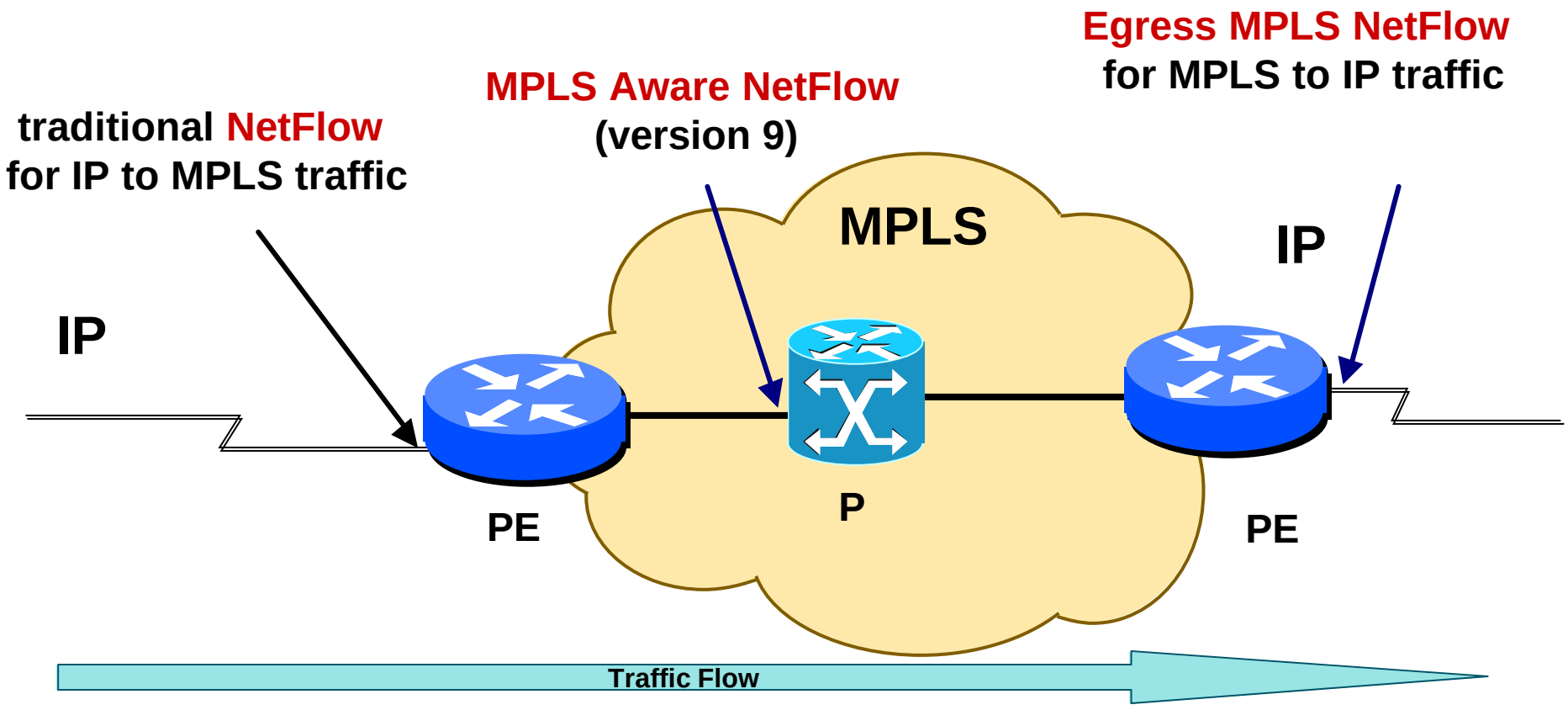
Sampled NetFlow

- Collects and exports NetFlow data for a sample of the traffic passing through the router, instead of the entire traffic
- Only for the 12000 router so far
- Sampled NetFlow exports the same information as full NetFlow
- Sampling advantages: CPU reduced and possible reduced exported Data
- Sampling disadvantage: no billing possible?

Where/How to enable NetFlow?

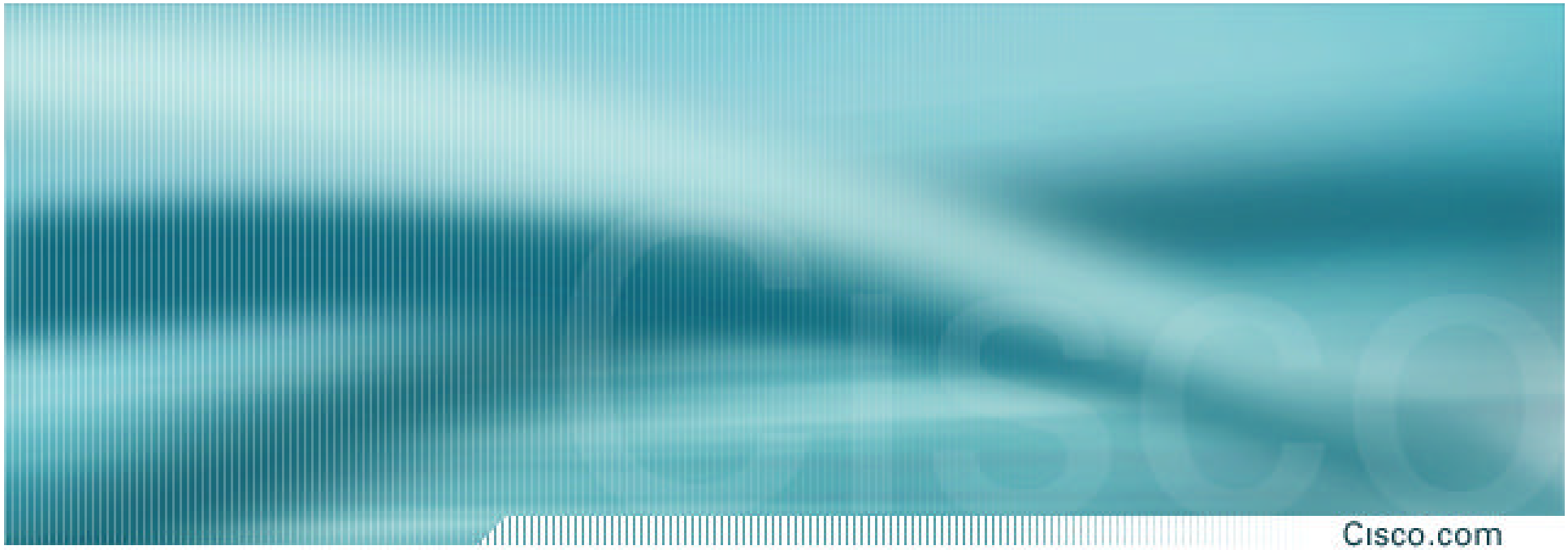


Where/How to enable NetFlow?



NetFlow MPLS Aware

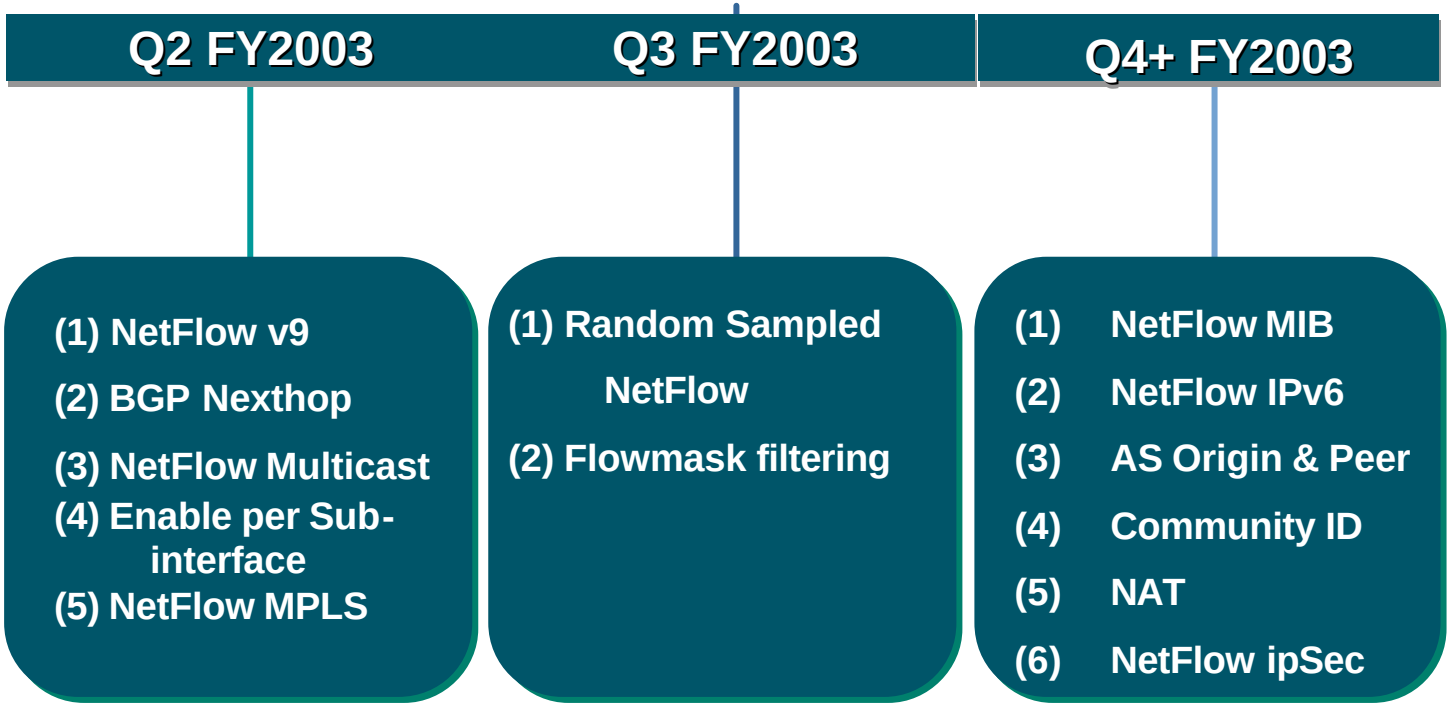
- **Flow Key (Uniquely Identifies the flow)**
  - **Source IP address**
  - **Destination IP address**
  - **IP Protocol**
  - **Input ifIndex**
  - **Source Application Port**
  - **Destination Application Port**
  - **DSCP**
  - **Up to 3 incoming MPLS labels of interest with experimental bits and end-of-stack bit**
  - **Positions of the above labels in the packet label stack**
- **Additional Export Fields**
  - **Flows**
  - **Packets**
  - **Bytes**
  - **First SysUptime**
  - **Last SysUptime**
  - **Output interface**
  - **NetFlow version 5 fields of the underlying IP packet**
  - **Type of the top label: LDP, BGP, VPN, ATOM, TE Tunnel MID-PT, unknow**
  - **The Forwarding Equivalent Class mapping to the top label**



Roadmap, Conclusion and References

External Roadmap for NetFlow

Scalability & Flexibility | **Optimizing data for Flow processing** | **Technology Coverage**



Conclusion

- **NetFlow is a nice complement to the test-box!**
- **NetFlow is not a replacement for the test-box!**
- **Getting more flow information in case of packet loss, delay, etc…**

NetFlow References

- **Netflow Services and Applications**

  http://www.cisco.com/go/netflow

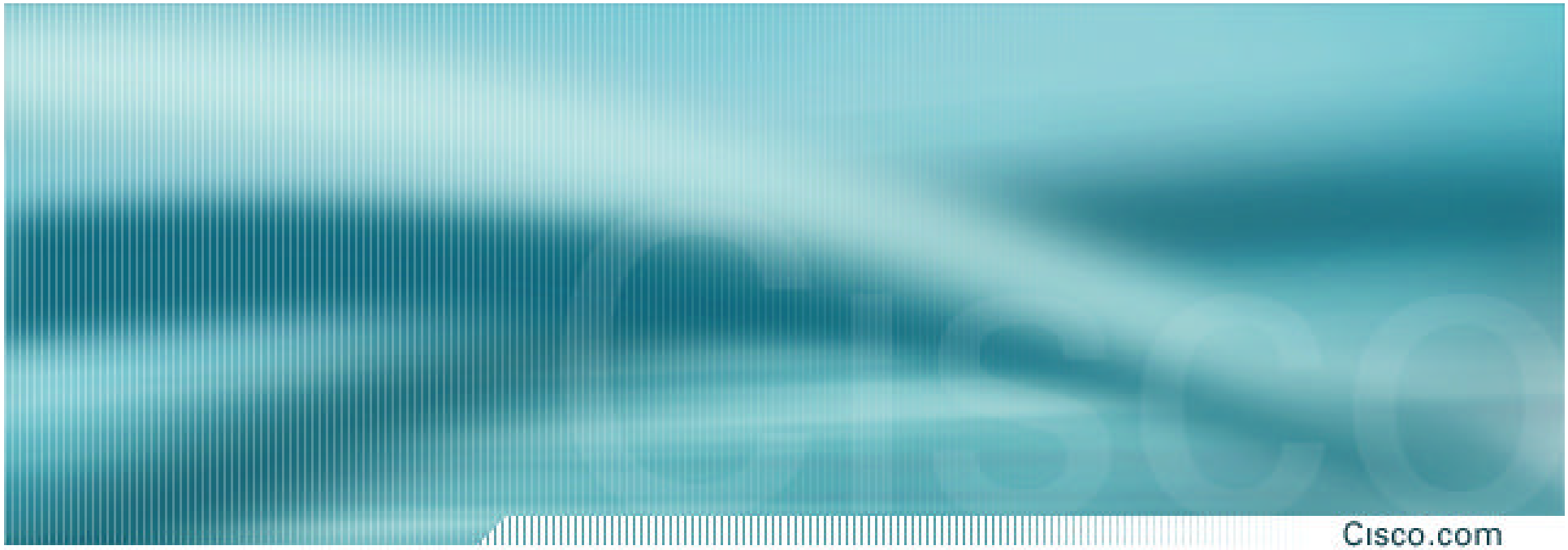
- **A complete white paper**

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm

- **An official Cisco Course (2 days)**

  NetFlow Service Advanced

Questions?



NetFlow Services

Benoit Claise

bclaise@cisco.com

RIPE 44, Amsterdam


Cisco Systems