Not to miss

small-amount but important traffic

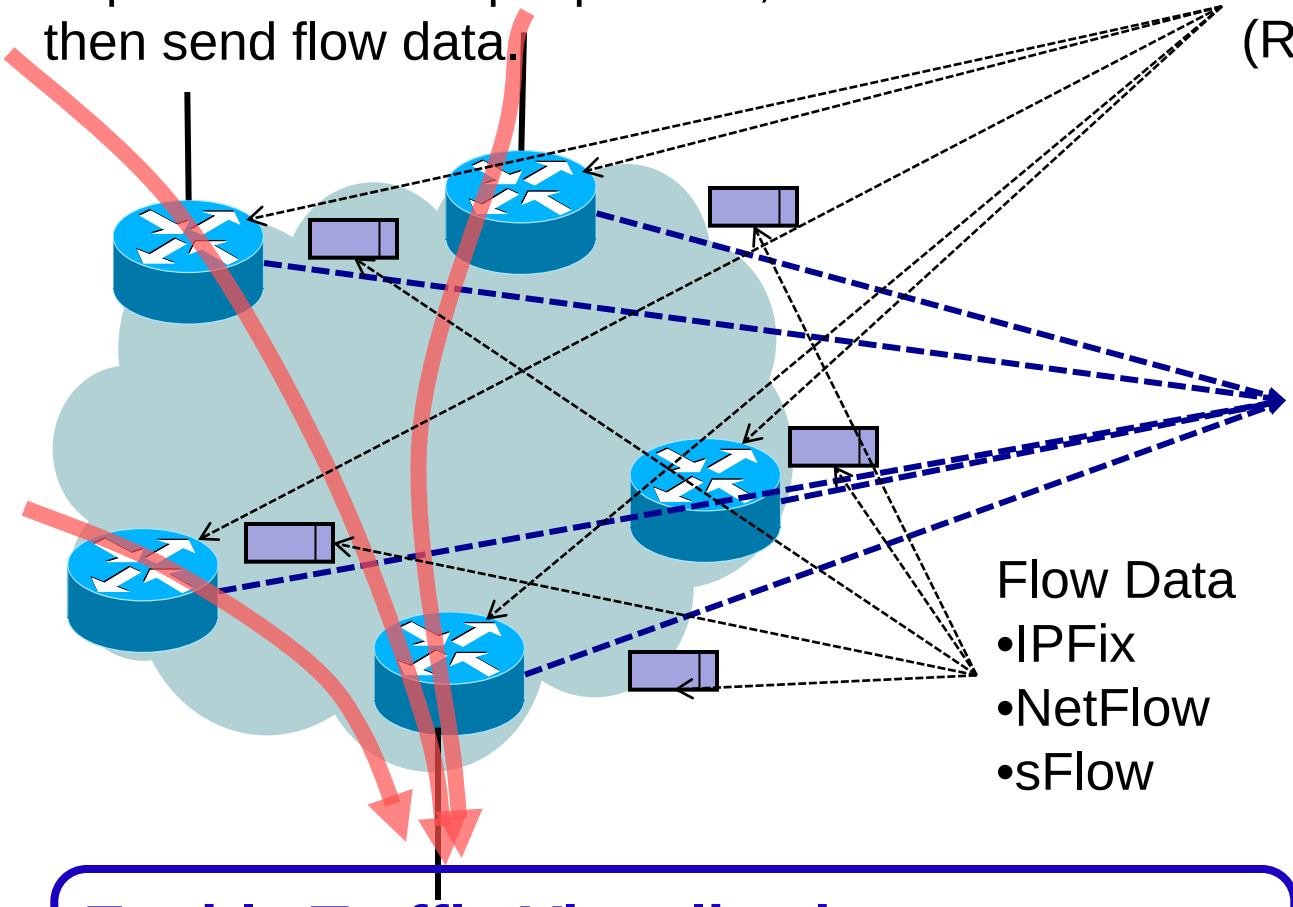
NTT Communications

Kazunori Kamiya

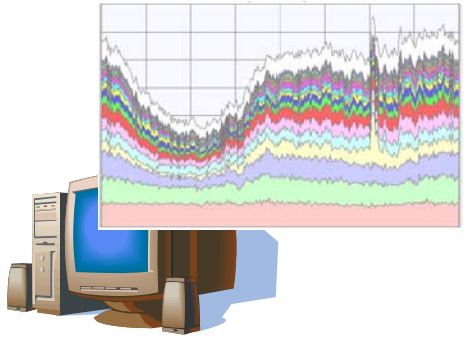
© NTT Communications

Using Flow Data

Exporters can sample packets, then send flow data.



Exporters (Router/Switch)



Flow Collector
Flow Analyzer

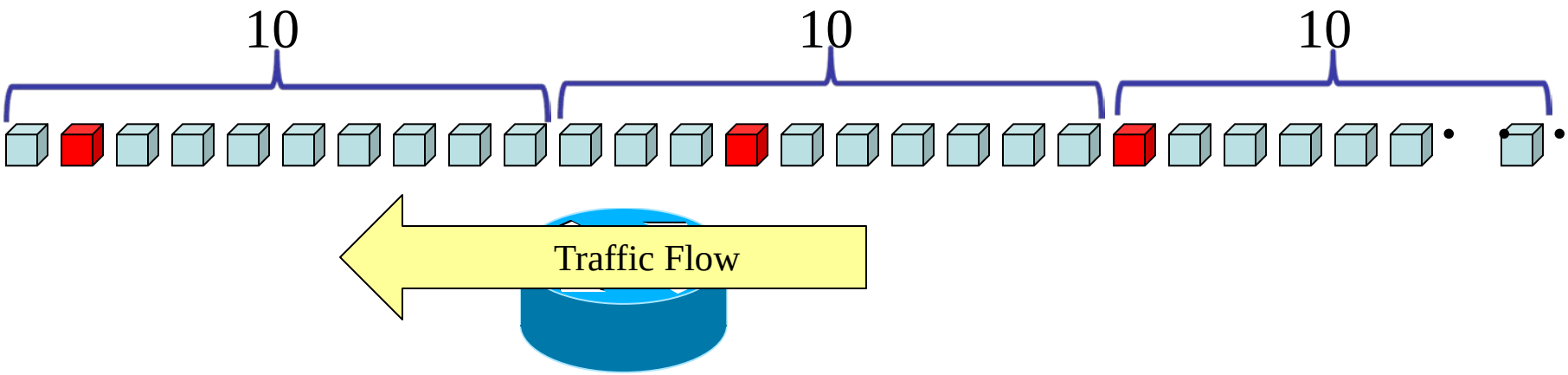
Flow Data
- IPFix
- NetFlow
- sFlow

Enable Traffic Visualization
Enable DDoS Attack Detection

Flow Sampling

- Sampling Rate : X
  - Sample 1 packets from X packets

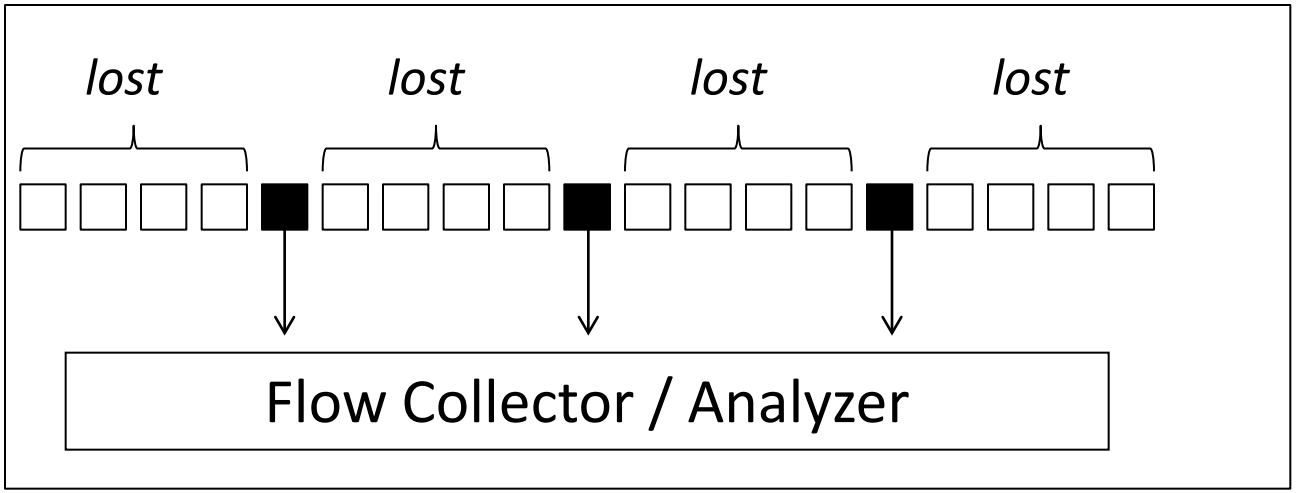
ex) X = 10



- Not necessary to see all the packets
  - Analyze traffic in a short time with a little load
  - Merit for large scale network
- Many ISPs set X more than 1000

Problem of Sampling

Cannot Analyze un-sampled packets

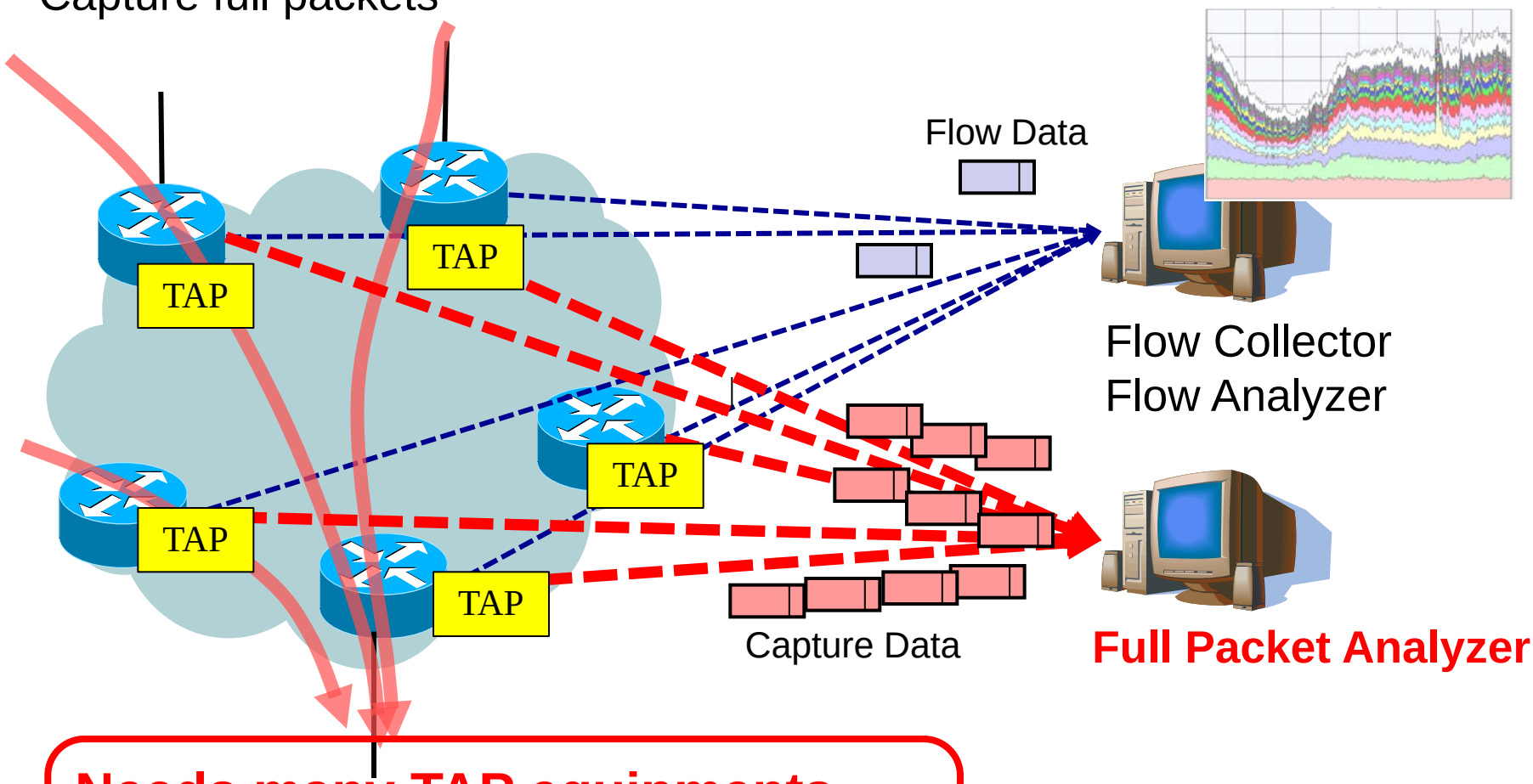


Sometimes, un-sampled packets might be important,,, (small amount)
Ex)
-For detail analysis of attack packets
-For IPv6 traffic analysis
(current IPv6 traffic is much smaller than IPv4 traffic)

© NTT Communications

Tapping

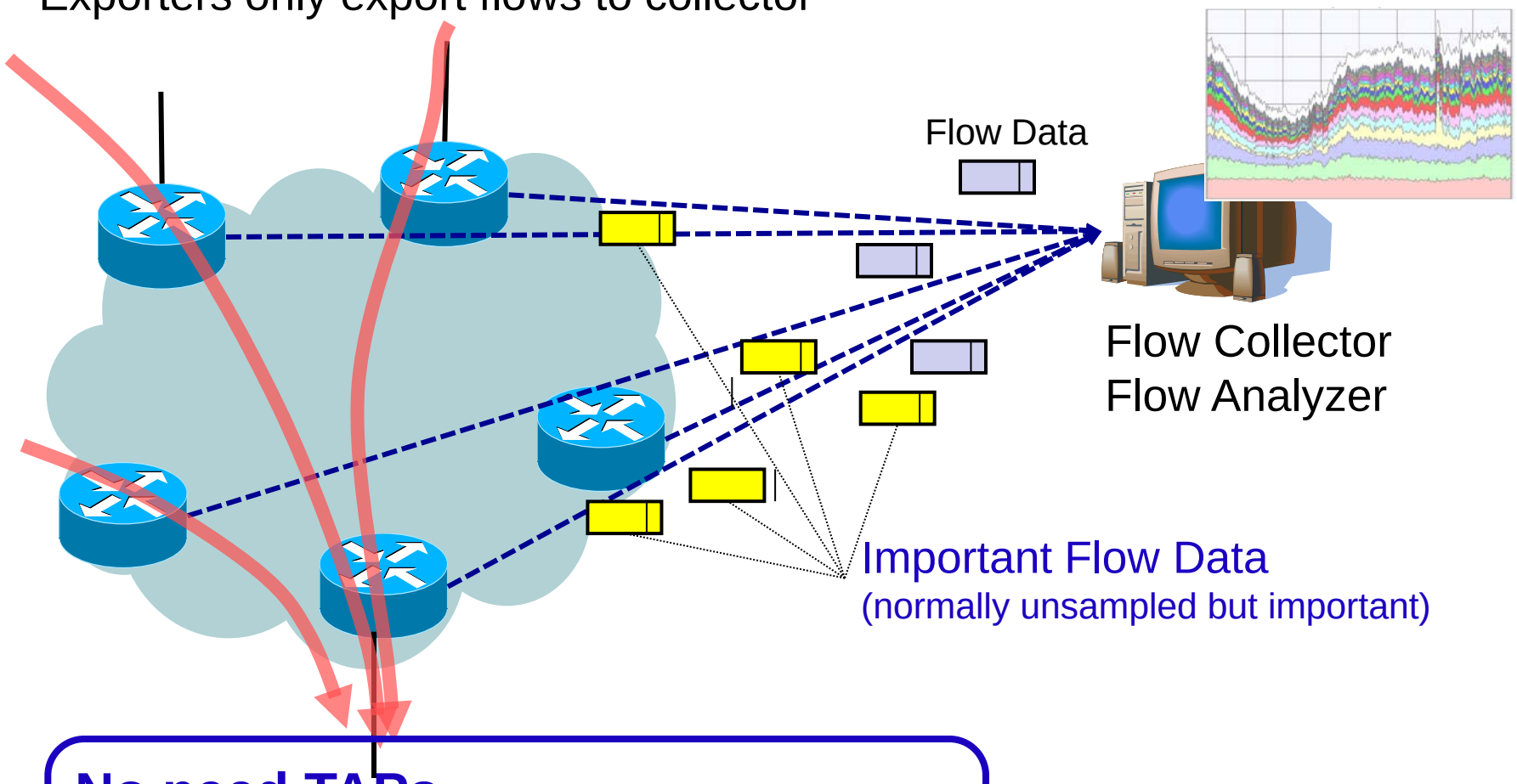
Capture full packets



Needs many TAP equipments
Needs another analyzer
Needs to analyze full packets

If possible,,,

Exporters only export flows to collector

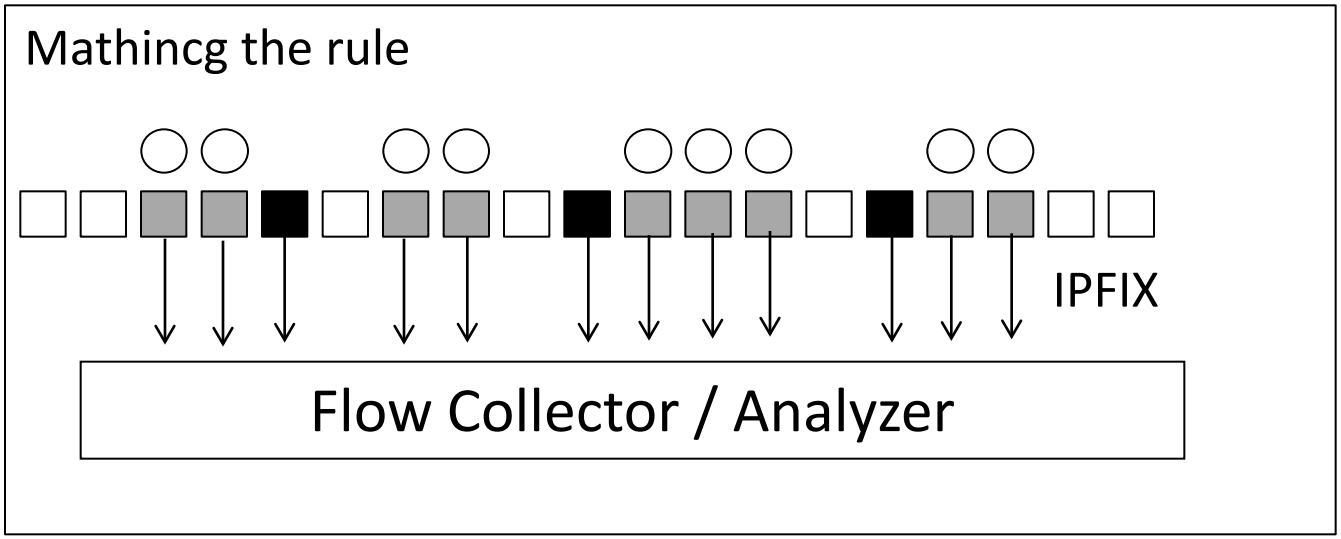


No need TAPs
No need other analyzer
No need to analyze full packets

© NTT Communications

PSAMP may be the solution

Export flow with packets matching the specified rule (ACL).



■ Normal sampling

■ Rule-based sampling (PSAMP)

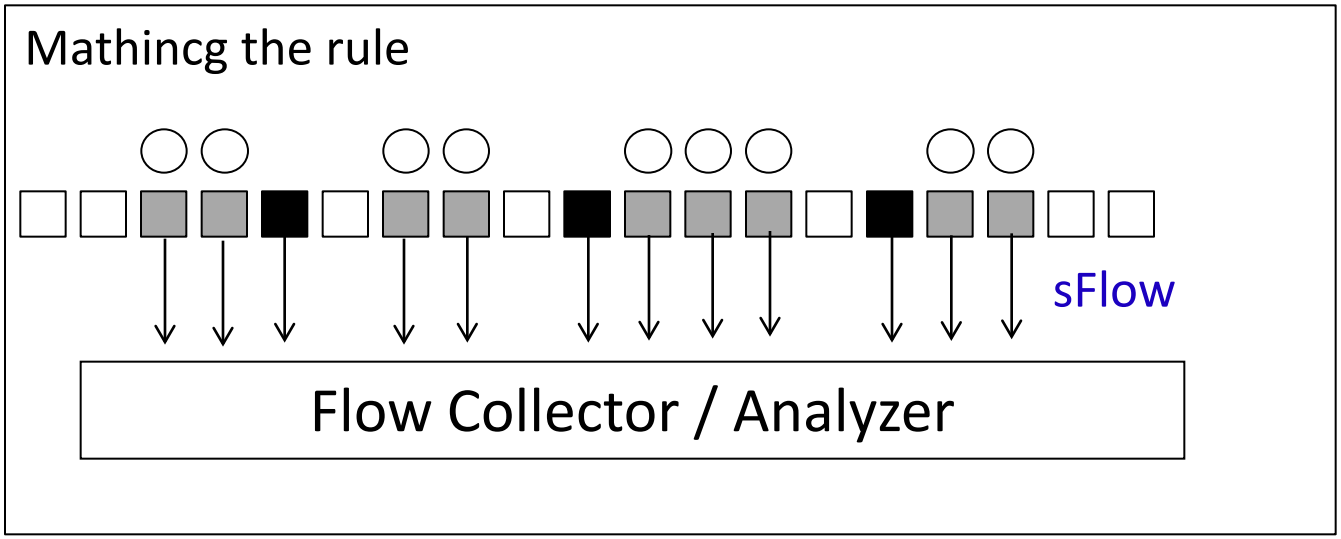
What is implemented:

- Flexible Netflow
- ACL-based sFlow

© NTT Communications

ACL-based sFlow

Export flow with packets matching the specified rule (ACL).



Normal sampling

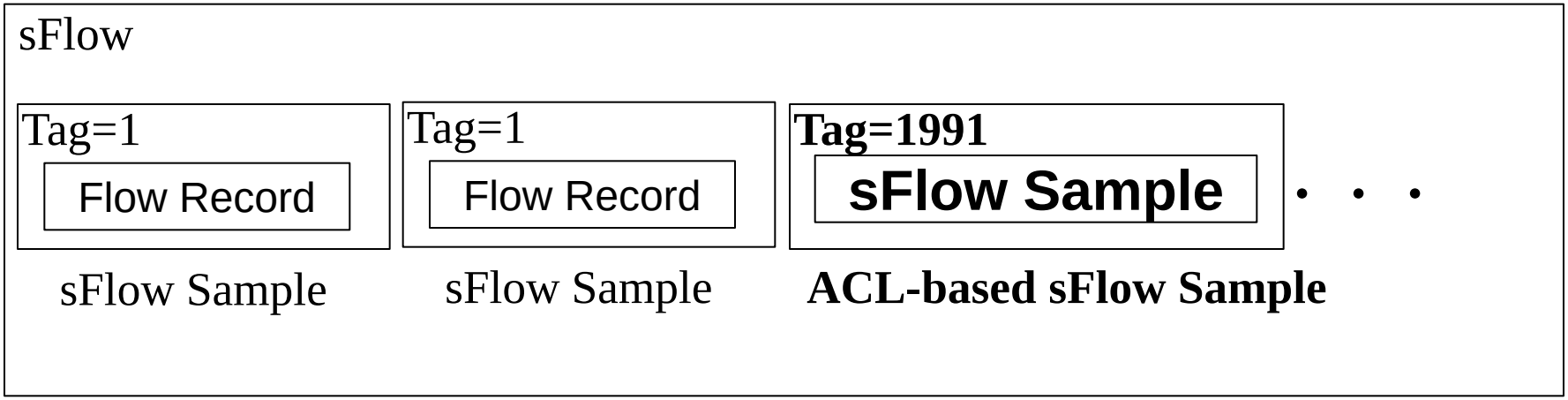
ACL-based sampline (sampling rate=1)

ACL-based sFlow is implemented on some switches.

© NTT Communications

ACL-based sFlow Cont…

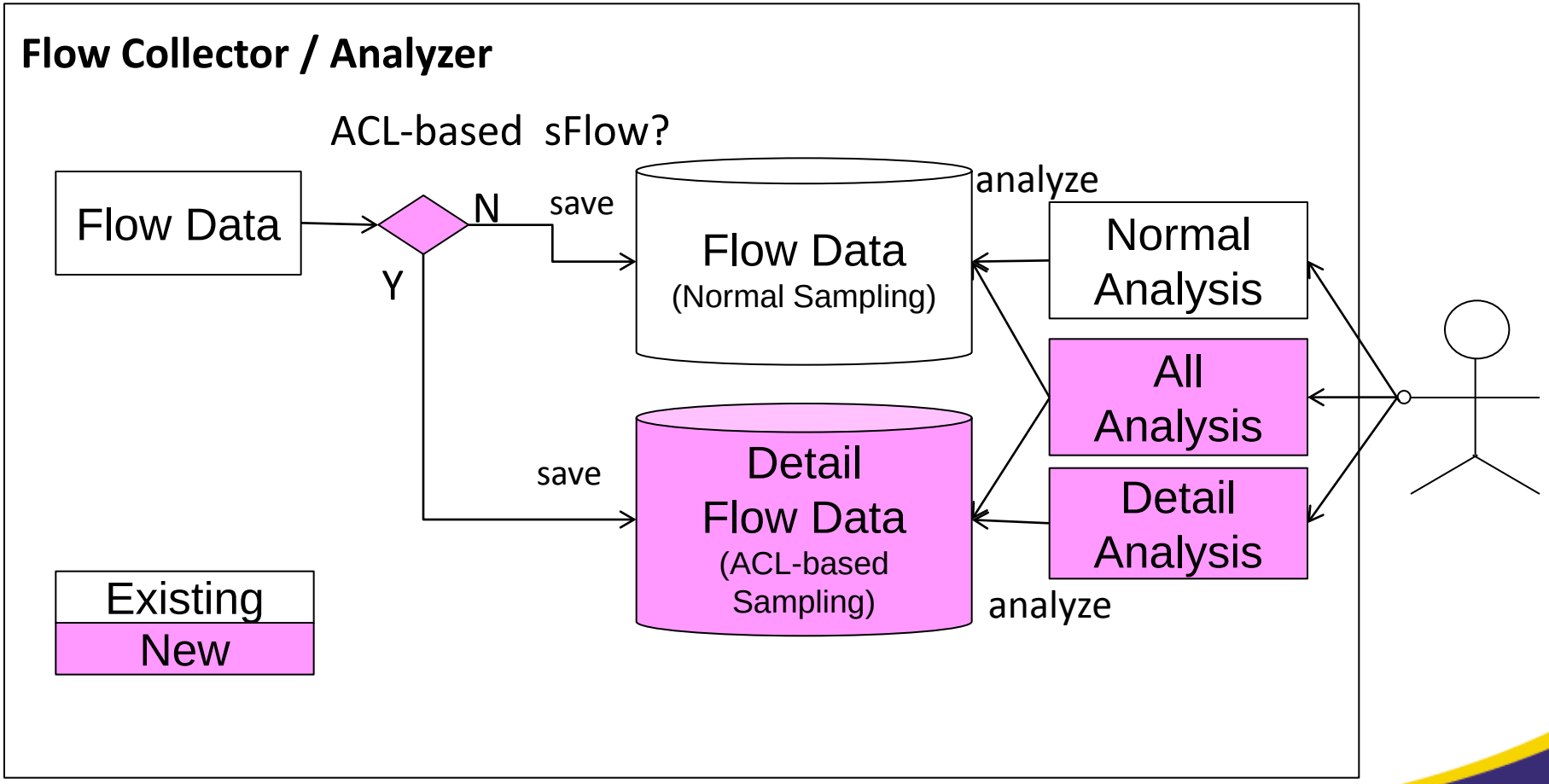
- sFlow sample is encapsulated in Tag=1991
- can be mixed with normal sFlow sample



© NTT Communications

Our implementation of Flow Collector / Analyzer

In addition to normal analysis (existing implementation), we implimented detailed analysis function.



© NTT Communications

[Evaluation1] Detection of Network Scan

- Network Scan
  - Port Number is randomized, difficult to detect scan from sampling flow

[Expeiment]

	daddr	dport	saddr	sport	proto	pps
T1(Web)	100.0.0.1	80	rand.	rand.	tcp	100k
T2(Scan)	100.0.0.1	rand.	rand.	rand.	rand.	100

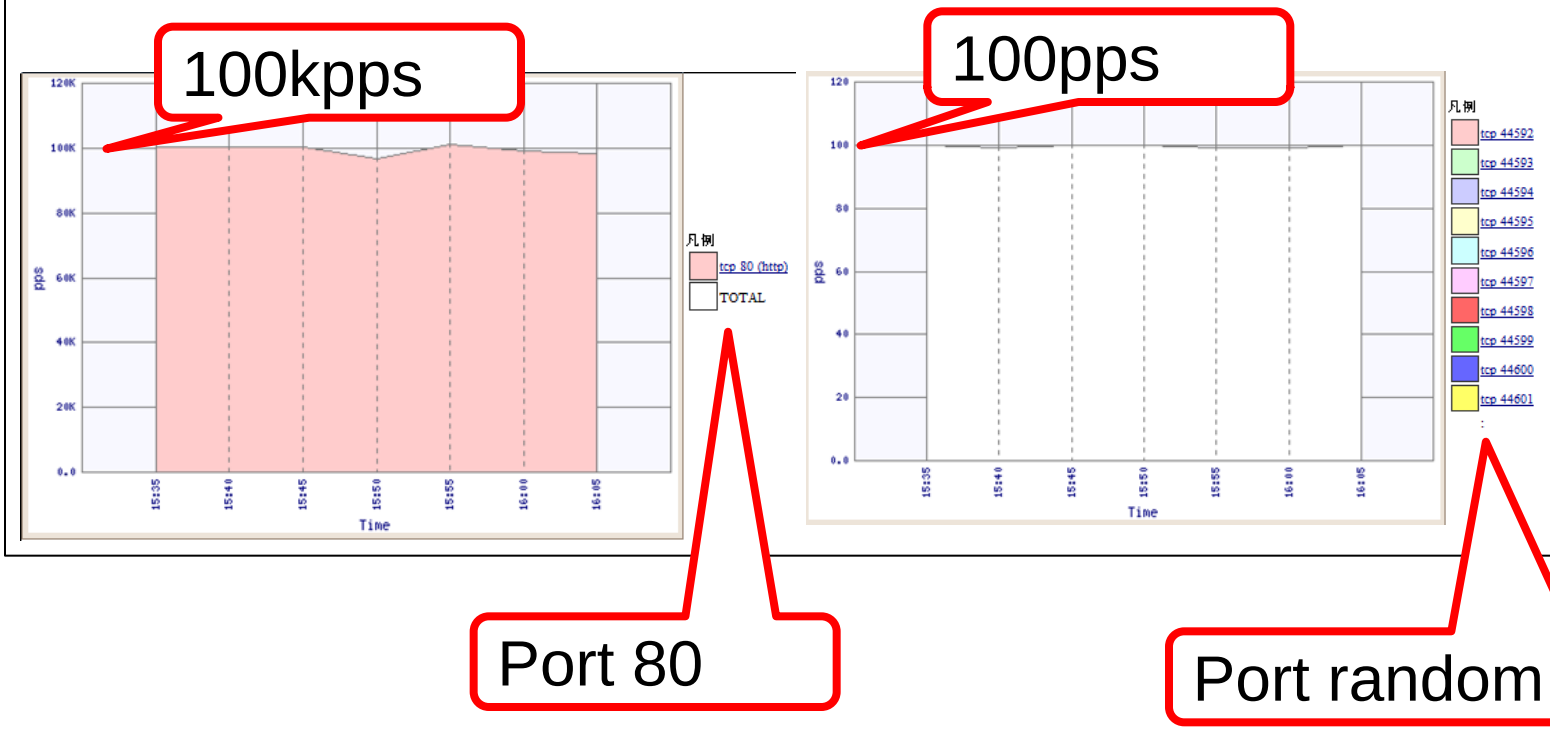
Device	Brocade NetIron MLX8
Sampling Rate	10000
Flow	sFlow v5
	ACL-based sFlow
ACL	not dst port 80

[Evaluation1] Detection of Network Scan cont.

- Successful in visualizing 100 pps network scan of 100kpps normal traffic

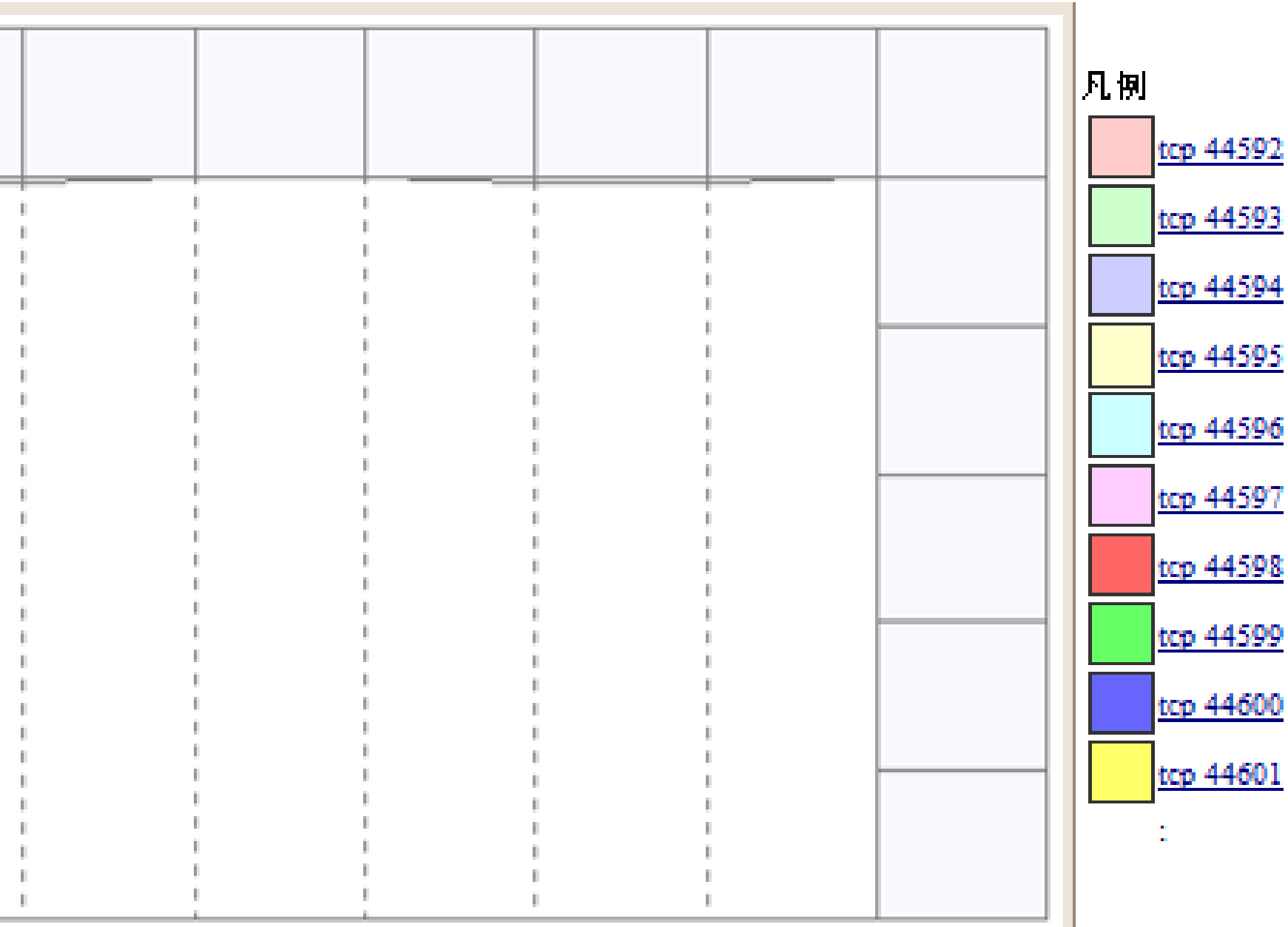
- Existing System
No scan packet is seen.

- New System
Scan is visualized.



© NTT Communications

Zoomed,,,


凡例
tcp 44592
tcp 44593
tcp 44594
tcp 44595
tcp 44596
tcp 44597
tcp 44598
tcp 44599
tcp 44600
tcp 44601

[Evaluation2] IPv6 traffic in dual-stack network

- IPv6 traffic
  - Currently IPv4 >> IPv6
  - The volume of IPv6 traffic is much smaller than IPv4 traffic
    - IPv6 Traffic might not be out of sampling
    - Might not analyze Ipv6 traffic in dual-stack network
- Experiment
  - Experiment in real dual-stack network
  - ACL=“ipv6”

© NTT Communications

NTT Communications

[Evaluation2] The result

- Show the result on site.

© NTT Communications

Demonstration

- On site

© NTT Communications

Thank You!!

© NTT Communications