IPTV Traffic "Qcast": ~~IP Multicast Traffic~~ Monitoring System with IPFIX/PSAMP

Shingo Kashima and Atsushi Kobayashi

NTT Information Sharing Platform Laboratories

Outline

- **Introduction**
  - Motivation
  - IP Multicast Streaming Traffic
- **Issues in Existing Multicast Monitoring**
- **Requirements**
  - Requirements
  - Difficult Requirements for Current NetFlow
  - Why IPFIX/PSAMP?
- **Our System: Qcast**
  - System Overview
  - System Architecture
  - System Evaluation
- **Conclusion**

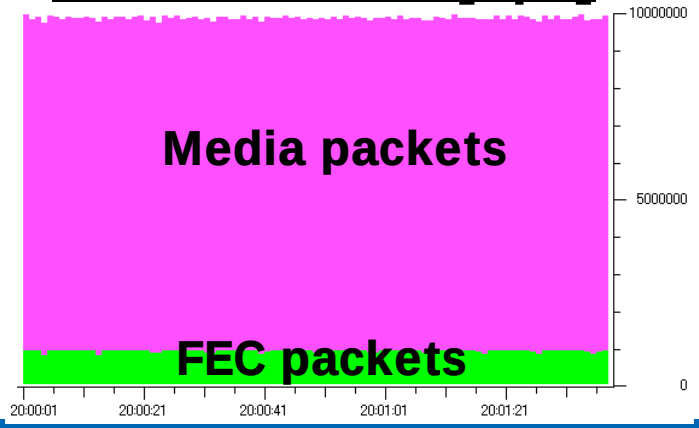
Motivation

- **Multicast service has started in several provider networks.**
  - Large number of broadband users leads to heavy demand for IP multicast streaming services, such as IPTV.
- **Existing multicast tools work, but not well enough to monitor streaming services in large-scale networks.**
  - Multicast ping, trace route, and multicast MIB.
- **Easy troubleshooting tools are required.**
  - IPFIX/PSAMP seems helpful.

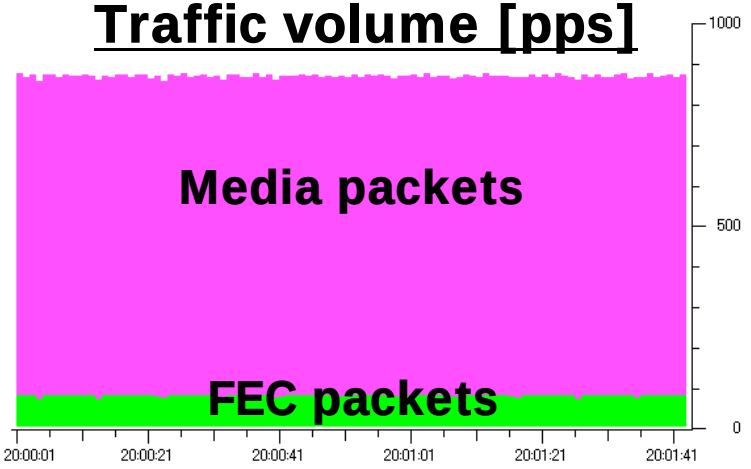
IP Multicast Streaming Traffic

- **Traffic volume of an IPTV channel: 10 Mbps, 0.9 kpps.**
  - Packet size: from 1300 to 1400 bytes.
- **IP multicast stream traffic includes two kinds of packets.**
  - Media packets and FEC packets.
- **IP multicast stream traffic includes RTP headers.**
  - Packet loss can be easily detected by keeping track of RTP seq. number.
- **More than 50 channels pass through an ISP network.**

Traffic volume [bps]



Traffic volume [pps]



Issues in Existing Multicast Monitoring

- **Multicast ping and trace route**
  - Detect fault point and check continuity by using test packets.
  - Do not observe real packets.

  → Inadequate for detecting service quality deterioration and confirming service quality.

- **Mirroring + packet capture**
  - Last resort for confirming service quality.
  - But requires great care and is not suitable for always-on monitoring.

Requirements

- **Requirement #1: Detect service quality deterioration and confirm service quality.**
  - Detect packet loss, disorder, and duplicates within 1 minute while there is continuous packet loss at 1/1000.
  - Monitor packet delay variation.
- **Requirement #2: Perform always-on monitoring of traffic volume and service quality of each IPTV-channel and each customer.**
  - Always monitor per {S,G}.
  - Always monitor per VLAN in access network.
- **Requirement #3: Localize failure point.**
  - Localize failure point not only in a service suspension but also when service quality deterioration occurs.
- **Requirement #4: Use at low cost as soon as possible.**
  - Necessary because multicast streaming service has already started.

Difficult Requirements for Current NetFlow

- **Requirement #1: For the current NetFlow exporter implementation, it is impractical to detect service quality deterioration and monitor service quality.**
  - Flow records in NetFlow cannot include packet loss, disorder, and duplicates.
  - In general, many operators use random sampling to introduce NetFlow.

- **IPFIX/PSAMP seems helpful in meeting this requirement.**

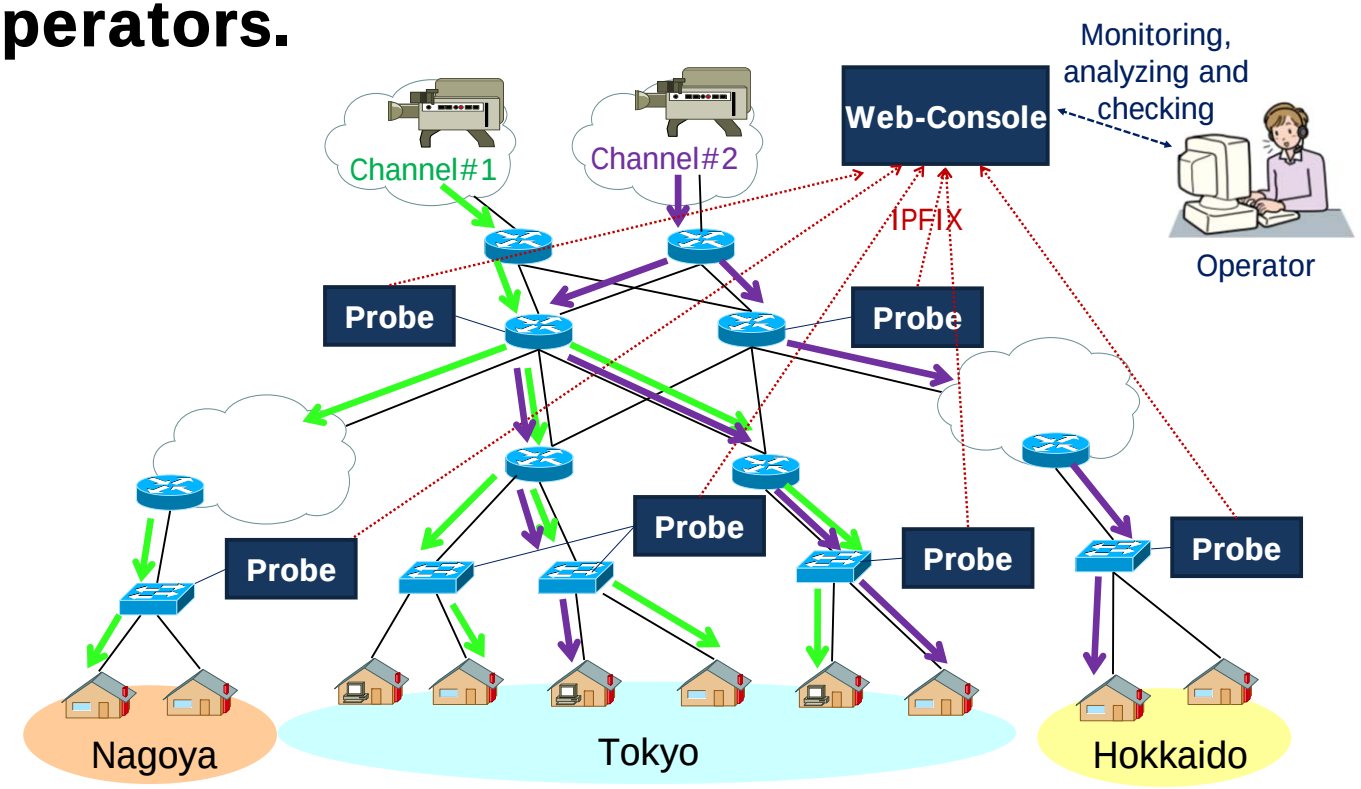
Why IPFIX/PSAMP?

- **PSAMP (RFC 5475)**
  - "Property Match Filtering" can focus the monitoring on IPTV traffic by selecting on the basis of packet header value.
  - "Systematic Time-based Sampling" can detect packet loss and packet interval time by selecting continuous packets.

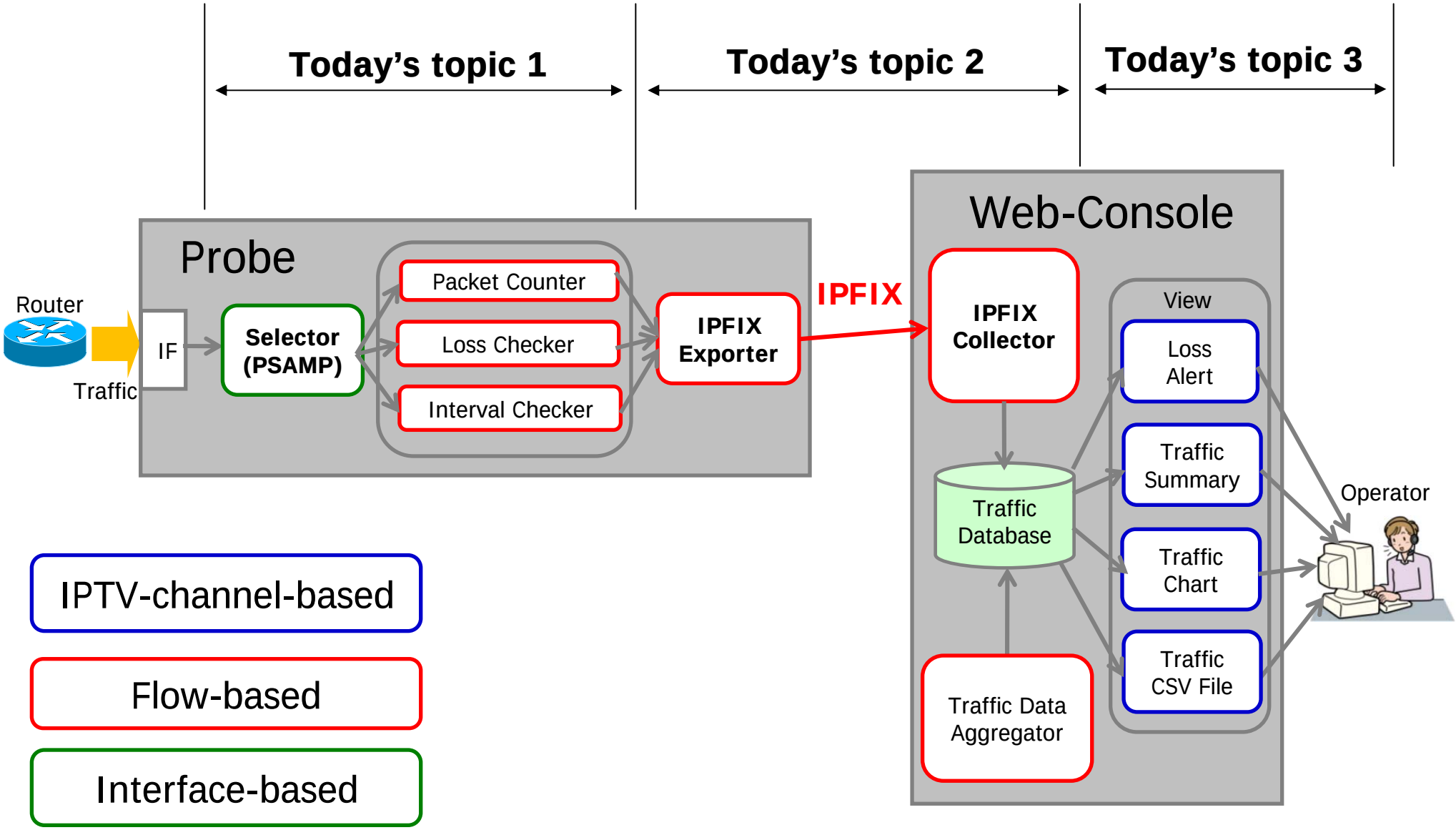
- **IPFIX (RFC 5153)**
  - "Enterprise-specific Information Elements" can export not only UDP/IP header information but also application header information.

Our System: Qcast Overview

- **Probe: Captures traffic from mirror port, monitors IPTV traffic with PSAMP, and exports with IPFIX.**
  - Runs on a general-purpose personal computer.
- **Web-Console: Collects IPFIX information and shows it to operators.**

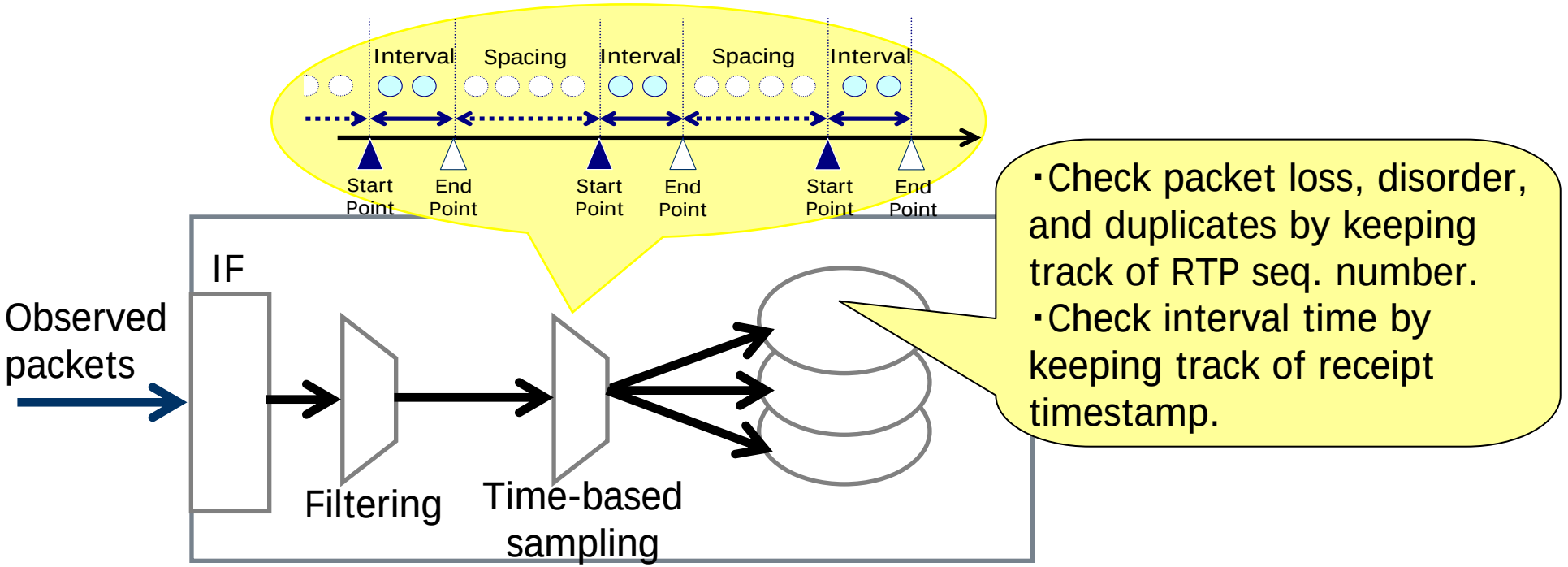


Qcast Architecture



Topic 1: Packet Loss and Interval Time

- **Combination of PSAMP techniques in Probe**
  - Observe packets at input interface.
  - Select multicast packet by “Property Match Filtering”.
    - Example: “Destination IPv6 Address == FF38::/16”
  - Extract them using “Systematic Time-based Sampling”.
    - All input packets during the interval period are selected.



Topic 2: Exporting Traffic Data

- **IPv6 template**
  - Flow key information
    - Includes VLAN ID
  - Traffic volume information
  - Packet loss information
  - Interval time information
    - Uses “Enterprise-specific Information Elements”

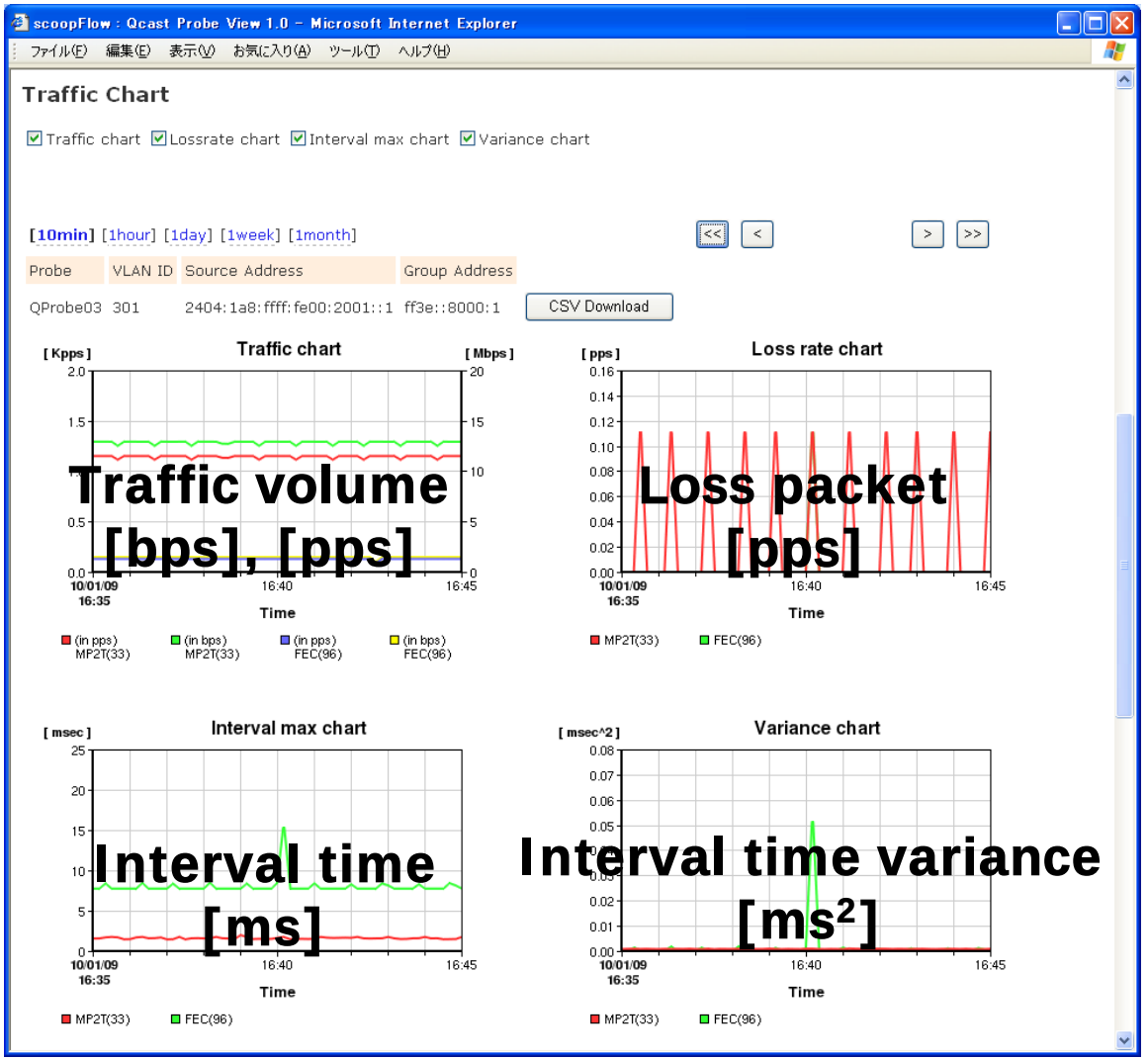
	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
0	Set ID (0x0002)	Length
4	Template ID (0x0103)	Field Count = 18 (0x0012)
8	octetDeltaCount (0x0001)	Field Length (0x0004)
12	packetDeltaCount (0x0002)	Field Length (0x0004)
16	srcTransportPort (0x0007)	Field Length (0x0002)
20	dstTransportPort (0x000B)	Field Length (0x0002)
24	srcIPv6Address (0x001B)	Field Length (0x0010)
28	dstIPv6Address (0x001C)	Field Length (0x0010)
32	droppedPacketDeltaCount (0x0085)	Field Length (0x0004)
36	flowStartMilliseconds (0x0098)	Field Length (0x0004)
40	flowEndMilliseconds (0x0099)	Field Length (0x0004)
44	vlanId (0x003A)	Field Length (0x0002)
48	protocolIdentifier (0x0004)	Field Length (0x0001)
52	ipVersion (0x003C)	Field Length (0x0001)
56	rtpIntervalAvgTime (0x8001)	Field Length (0x0004)
60	ENTERPRISE NUMBER (0x000000D2)	
64	rtpInternalMaxTime (0x8002)	Field Length (0x0004)
68	ENTERPRISE NUMBER (0x000000D2)	
72	rtpIntervalMinTime (0x8003)	Field Length (0x0004)
76	ENTERPRISE NUMBER (0x000000D2)	
80	rtpIntervalVariance (0x8004)	Field Length (0x0004)
84	ENTERPRISE NUMBER (0x000000D2)	
88	rtpPayloadType (0x8005)	Field Length (0x0002)
92	ENTERPRISE NUMBER (0x000000D2)	

- **Option template**

	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
0	Set ID (0x0003)	Length
4	Template ID (0x0106)	Field Count (0x0003)
8	Scope Field Count (0x0001)	exporterIPv4Address (0x0082)
12	Scope 1 Length (0x0004)	samplingTimeInterval (0x0133)
16	Field Length (0x0004)	samplingTimeSpace (0x012E)
20	Field Length (0x0004)	flowActiveTimeout (0x0024)
24	Field Length (0x0002)	

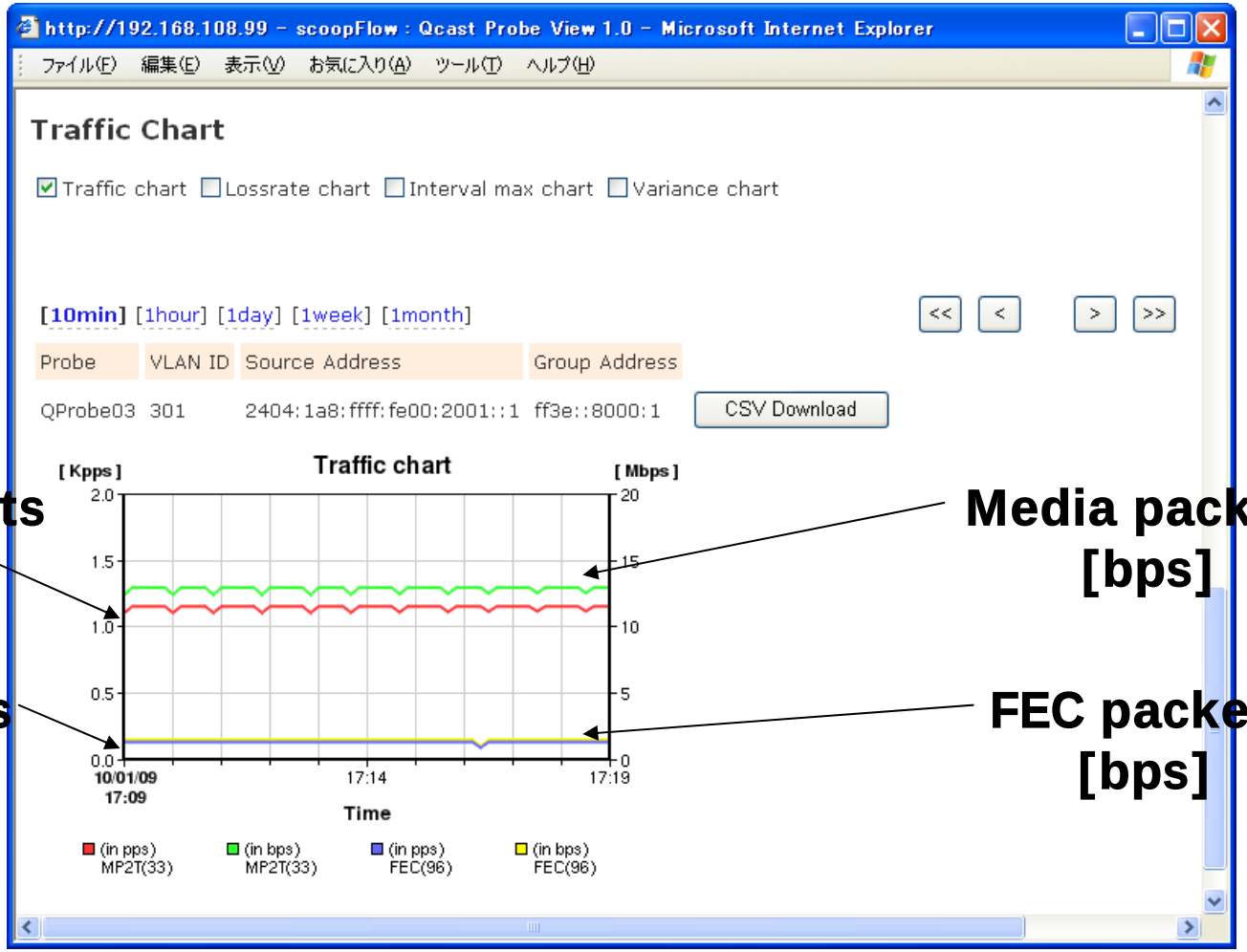
Topic 3: View [1/6]

- **Shows four kinds of traffic information**



Topic 3: View [2/6]

- **Shows a traffic chart separated by RTP payload type.**
  - {Media packets, FEC packets}



Media packets [pps]

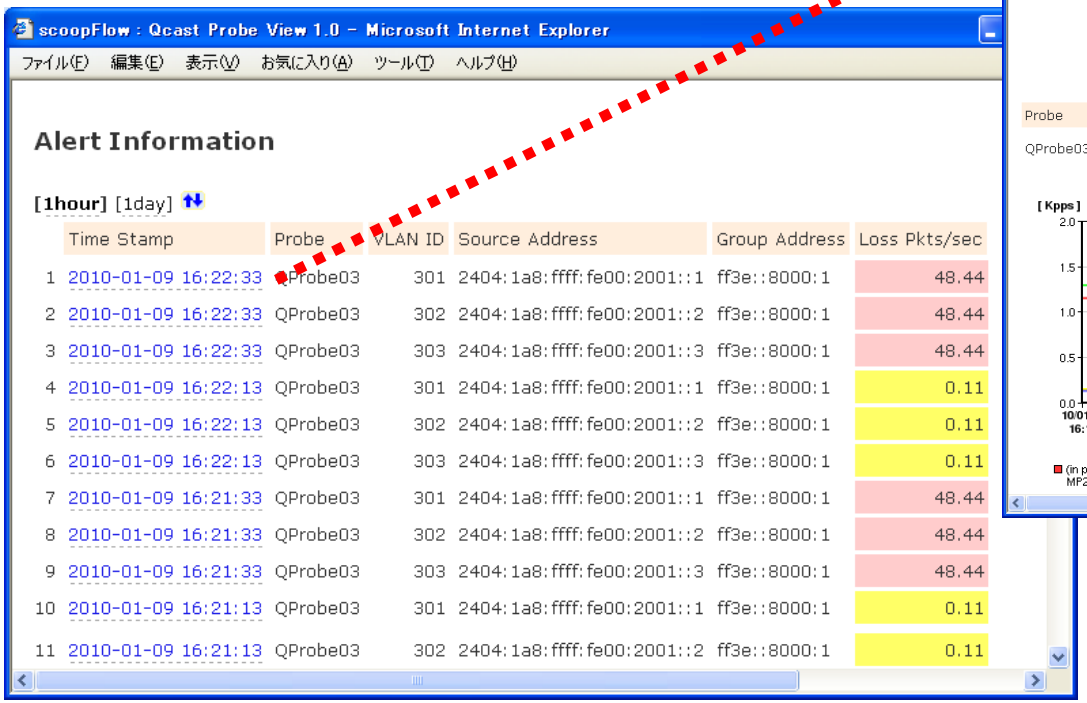
FEC packets [pps]

Media packets [bps]

FEC packets [bps]

Topic 3: View [3/6]

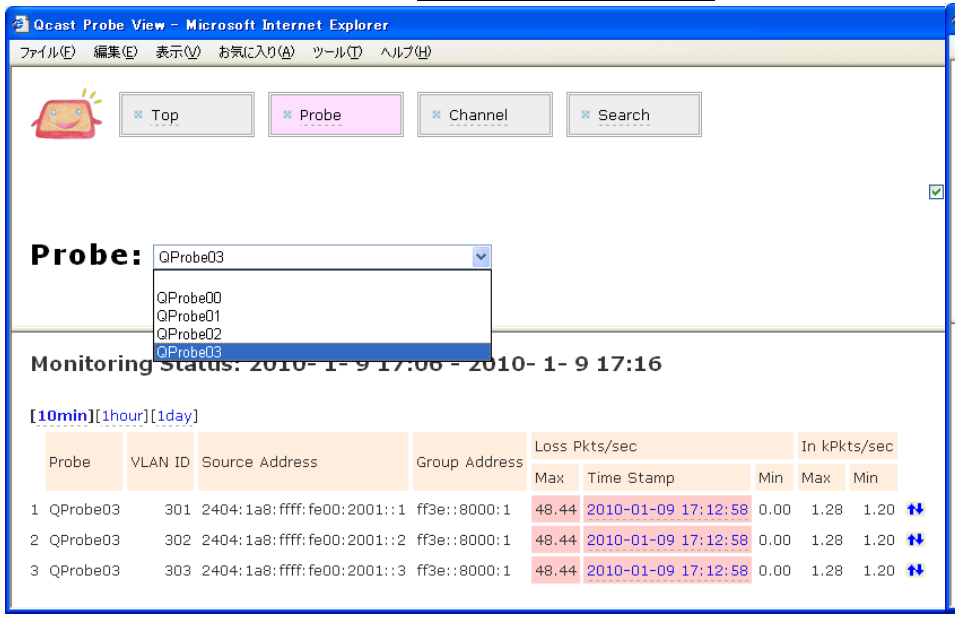
- **Shows packet loss alert**
  - Two-level alert
    - Red: dangerous level
    - Yellow: warning level
  - Link to traffic chart



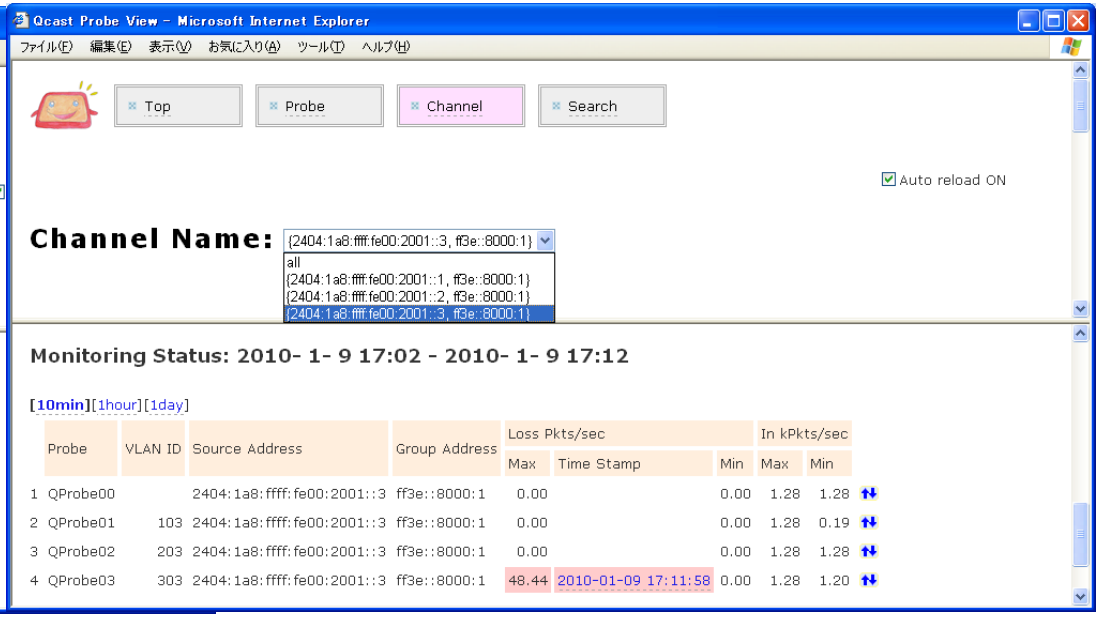
Topic 3: View [4/6]

- **Probe view**
  - When you select a probe from the Probe pull-down menu, the specified interface information is shown.
- **Channel view**
  - When you select {S,G} from the Channel Name pull-down menu, the specified IPTV-channel information is shown.

Probe view



Channel view



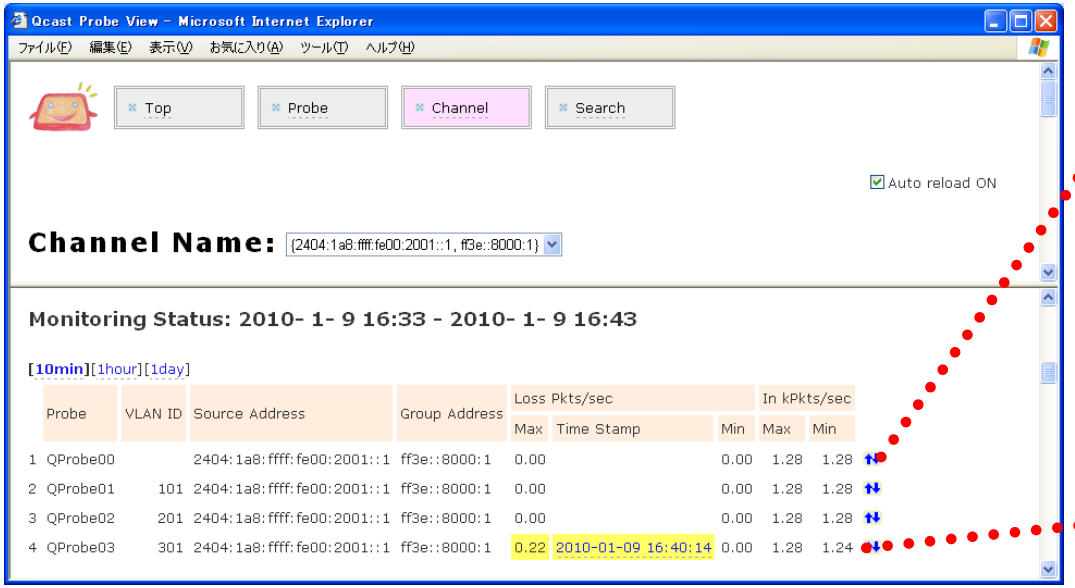
Topic 3: View [5/6]

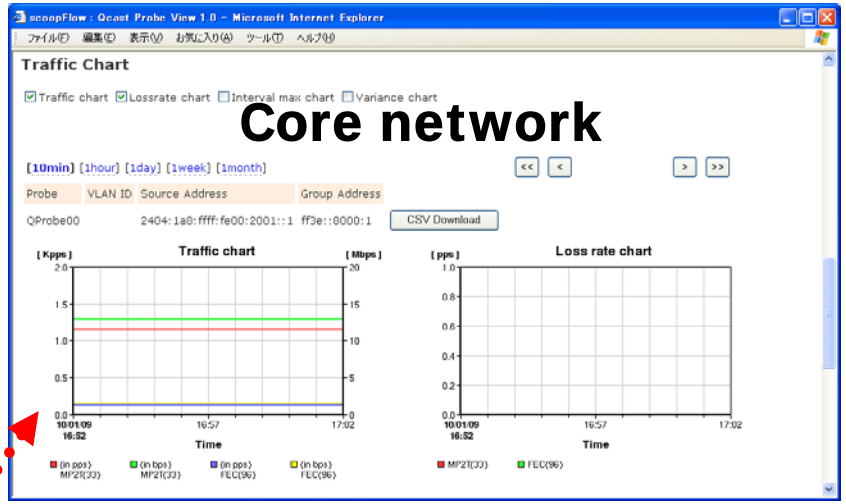
- **Probe view**
  - Also shows traffic volume chart built up from all channels.
  - Useful for capacity planning.

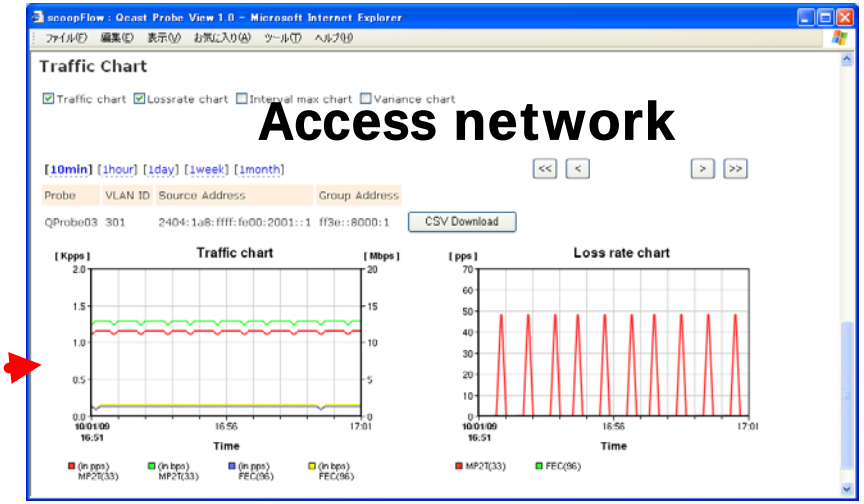
{2404:1a8:ffff:fe00:2001::3, ff3e::8000:1}
{2404:1a8:ffff:fe00:2001::2, ff3e::8000:1}
{2404:1a8:ffff:fe00:2001::1, ff3e::8000:1}

Topic 3: View [6/6]

- **Channel view**
  - Also localizes fault point by comparing traffic charts of multiple probes.

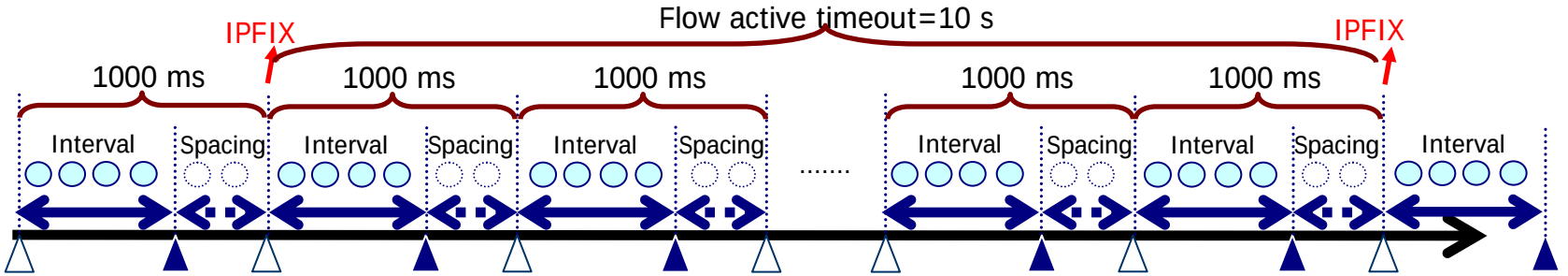






Evaluation of Probe

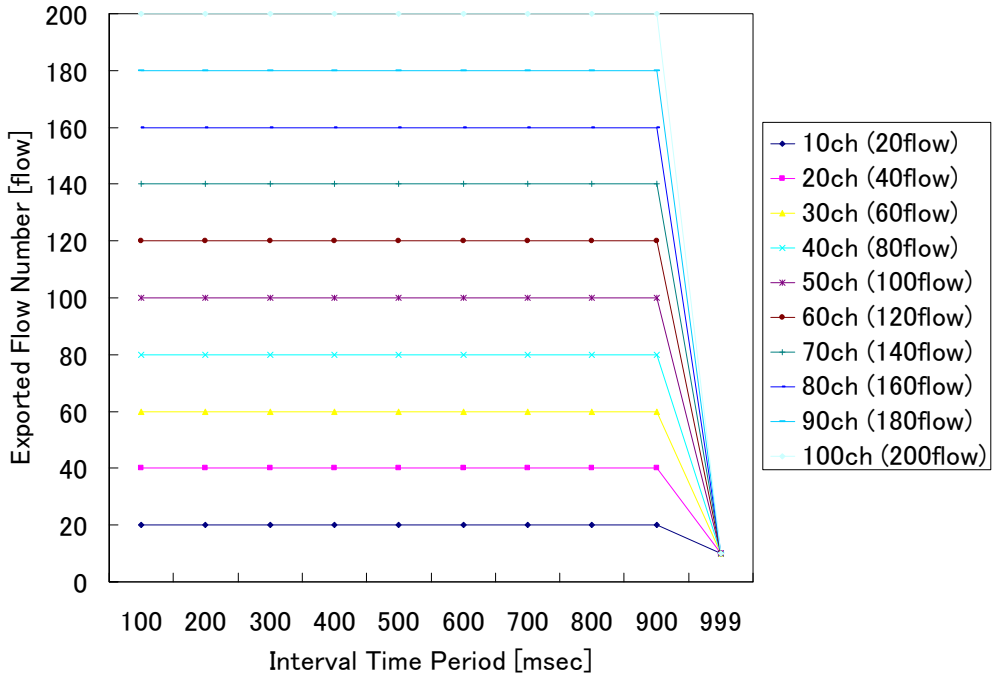
- **Experimental assumptions:**
  - Packets of 20—100 IPTV channels pass through a probe.
    - Traffic volume of an IPTV channel: 10 Mbps, 0.9 kpps.
    - IPTV channel includes two kinds of packets (Media, FEC).
  - We evaluated the probe by varying the sampling interval period.
    - Sum of the sampling and spacing interval period was kept at a fixed value of 1000 ms.
    - Flow active timeout had a fixed value of 10 s.

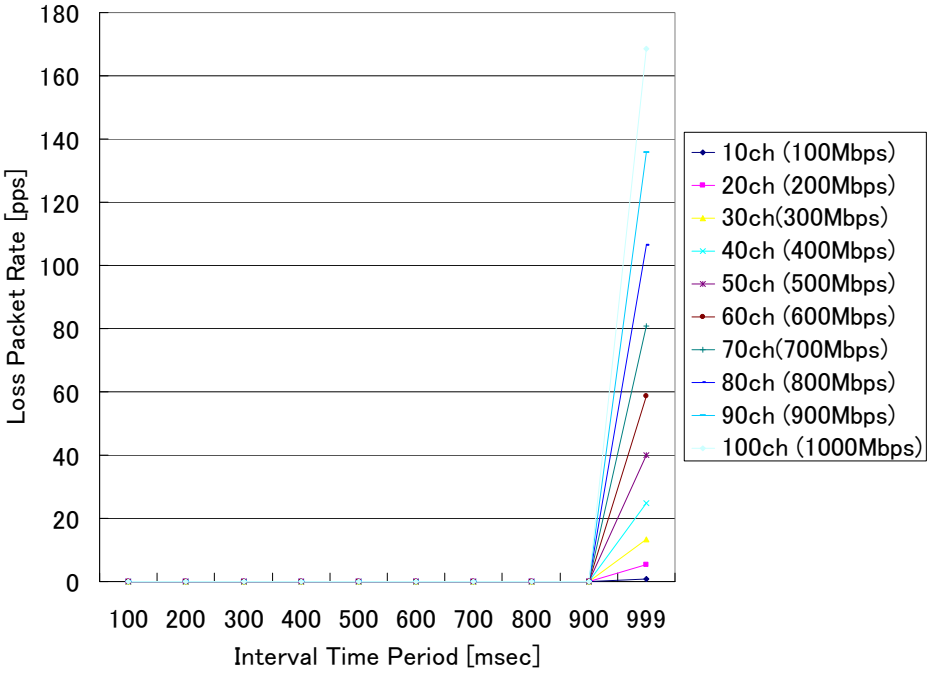


- **Experimental environment:**
  - CPU: Core 2 Duo 2.0GHz, Memory: 3.5 GB, Interface: Intel 1GbE NIC, OS: CentOS 5.3

Experimental Results for Probe

- **Exported flow number and packet loss rate obtained by changing the interval period from 100 to 999 ms.**
- **Performance had no limitation for interval period from 100 to 900 ms.**

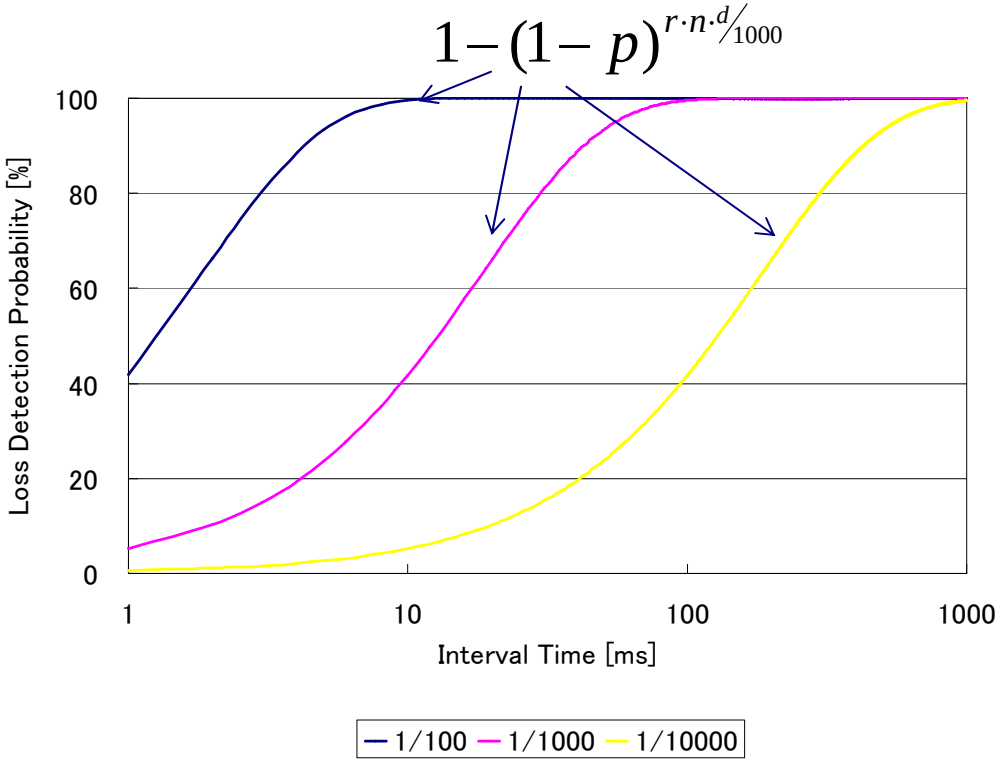




Packet Loss Detection Probability

- **We evaluated the detection probability for packet loss within the given monitoring interval (*n*) by changing packet loss rate (*p*) and sampling interval time (*d*).**
  - On the condition that *n* is 1 min and packet rate (*r*) is 0.9 kpps, the experimental results are shown.

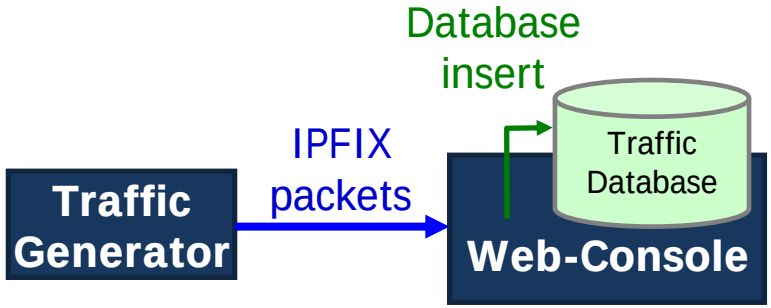
- **Detection probability is almost 100% if the sampling interval period is 900 ms and packet loss is 1/1000 for over 1 min.**



Evaluation of Web-Console

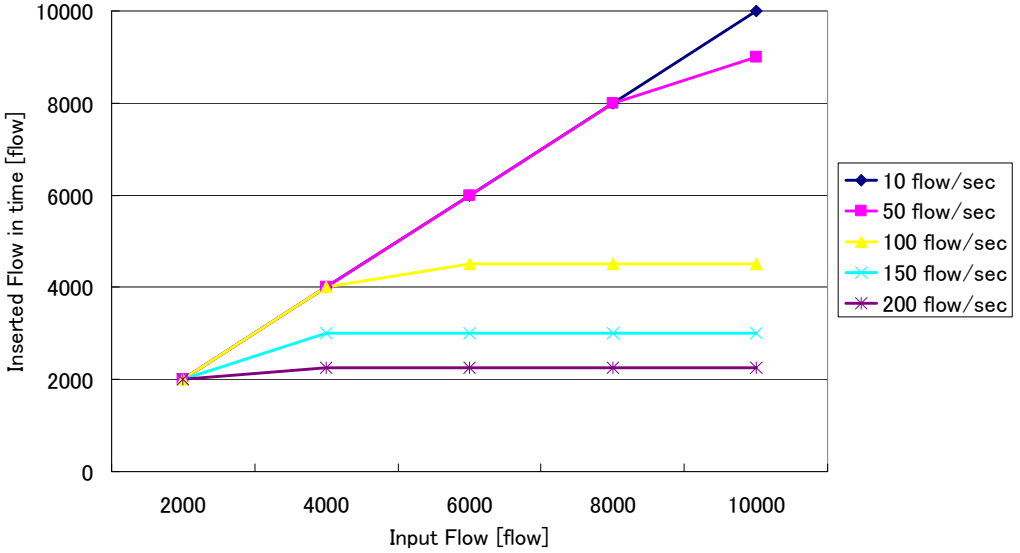
- **Experimental assumptions:**
  - IPFIX packets were input to a Web-Console.
    - A IPFIX packet includes 10 flow records.
  - We evaluated the Web-Console by varying the flow rate and number of flow.
    - Flow rate: 10-200 flow/sec (1-20 pps)
    - No. of flow: 200-1000 flow (20-100 packets)

- **Experimental environment:**
  - CPU: Xeon 3.6Hz, Memory: 3.5 GB,
    OS: CentOS 5.3, DB: PostgresSQL 8.37



Experimental Results for Web-Console

- **We measure the number of inserted flow into traffic database in time by changing the following conditions:**
  - No. of input flow from 2,000 to 10,000
  - Input flow rate from 10 to 200 flow/sec.



- **The performance limit seems to be as follows:**
  - 50 flow/sec: 9,000 flow
  - 100 flow/sec: 4,500 flow
  - 150 flow/sec: 4,000 flow
  - 200 flow/sec: 2,200 flow
- **That is to say:**
  - When flow active timeout is 180 sec, 90 probe (9,000 flow) is supported.
  - When flow active timeout is 45 sec, 45 probe (4,500 flow) is supported.
  - When flow active timeout is 26 sec, 40 probe (4,000 flow) is supported.
  - When flow active timeout is 11 sec, 22 probe (2,200 flow) is supported.

Summary

- **We presented a new traffic monitoring method for IP multicast streaming services, such as IPTV, and the implemented system using IPFIX/PSAMP (Qcast).**

- **We showed the feasibility of the Qcast.**

NTT

Thank you very much.

Please come and see our demonstration.

This study was supported by the Ministry of Internal Affairs and Communications of Japan.