Analysis of Bursty Packet Loss Characteristics on Underutilized Links

DPNM Lab.

Seung-Hwa Chung

2004. 12. 21

mannam@postech.ac.kr

Content

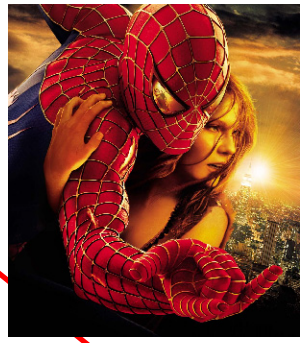
- Introduction
- Related Work
- Packet Loss Detection & Traffic Monitoring
- Traffic Data Collection
- Analyzing Packet Loss and IP Traffic
- Concluding Remarks & Future Work

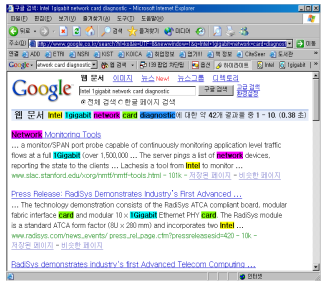
Introduction

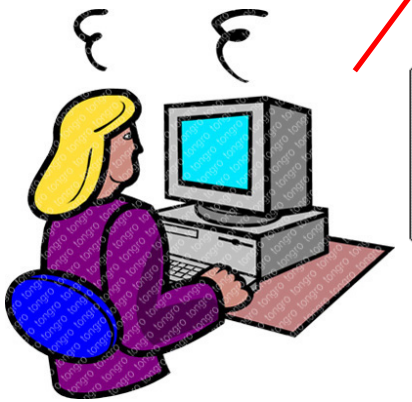
- Continuous increase in Internet apps & users
  - The number of networked applications and users are continuously increasing
  - ISPs & enterprises provide sufficient bandwidth according to increasing traffic requirements

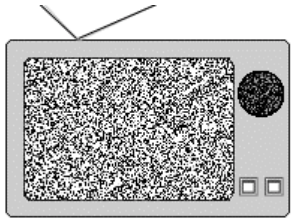
- Network-based applications
  - Service quality is not up to expectation even in underutilized links
    - VoIP, Video conferencing, Streaming media, etc
    - Due to sporadic but non-negligible losses

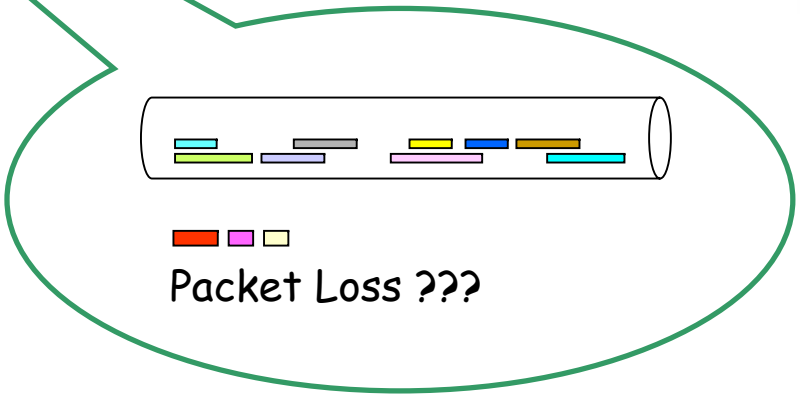
Problem











Goals

1. Prove Packet Loss exists on Underutilized Links
2. Analysis of Bursty Packet Loss Characteristics

- Knowing the characteristics of packet loss:
  - We expect this study can assist in designing new applications or router/switch structures that are prepared to handle unexpected packet loss

Related Work

- Not many researches in area of packet loss on underutilized link
  - People take no packet loss on underutilized link as a matter of course on underutilization links

- A characterization of congestion in the Sprint IP backbone network
  - Papagiannaki *et. al.* (IMC 2003)
  - They showed that there are micro congestions using SNMP at millisecond level

- The effect of early packet loss on web traffic
  - Hall *et. al.* (PAM Workshop 2003)
  - They showed a small number of packet loss can contribute to serious delays at second level

SNMP: Standard MIB variables (1/2)

- Traffic information using SNMP
  - by using standard MIB II variables

Object	OID	Description
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	The number of subnetwork-unicast packet delivered to a higher-layer protocol
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
ifInOctets	1.3.6.1.2.1.2.2.1.10	The total number of octets receive on the interface, including framing characters
ifOutOctets	1.3.6.1.2.1.2.2.1.16	The total number of octets transmitted out of the interface, including framing characters

SNMP: Standard MIB variables (2/2)

- Problems to Detect Packet Loss using Standard MIB
  - Some packets are destined to the router
  - Some packets are generated by the router
  - Some packets are broadcasted by the router

- MIB has the limitation of polling time interval
  - MIB counters not being updated immediately
    (First priority job of router is the packet routing)
  - Update at 5-10 Second Interval

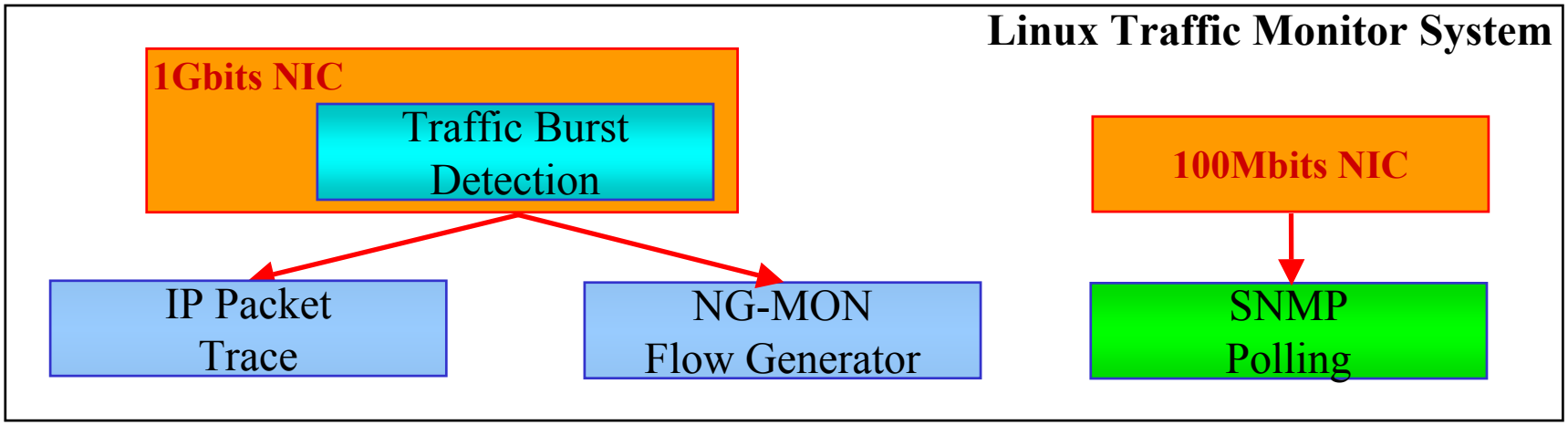
- SNMP
  - Problems on short time granularity and traffic information
- Mirroring Port
  - Router overload and affecting packet loss characteristics
- TAP can solve time interval problem
  - Capturing passing packets at real time
  - Not affecting Router Process
- Traffic Monitor System using TAP
  - Implemented with packet capture APIs
    - Libpcap and SOCKET_PACKET, etc.

- Detecting packet loss and cpuLoad
  - by using Cisco enterprise MIB variables

- Each interface owns its input queue and output queue

Object	OID	Description
locIfInputQueueDrops	1.3.6.1.4.1.9.2.2.1.1.26	The number of packets dropped because the input queue was full
locIfOutputQueueDrops	1.3.6.1.4.1.9.2.2.1.1.27	The number of packets dropped because the output queue was full
cpuLoad	1.3.6.1.4.1.9.2.1.56	CPU Utilization (5 sec avg.)

Traffic Monitoring



Module Name	Module Description
Traffic Burst Detection Module	This module detect traffic burst (number of packet, size of packet) at short time granularity.
SNMP Polling Module	This module polls Cisco private MIB and Standard MIB II values.
IP Packet Trace Module	This module capture all IP packets and save their header with time stamp.
NG-MON Flow Generator Module	This module generates packets into flows and used for detail flow analysis.

Packet Loss Detection & Traffic Monitoring Method

1. If there is a packet loss, we can obtain the packet loss occurred time through SNMP in accuracy of 10 seconds

2. At the same time, the traffic on the link is monitored by our traffic monitor system, we also collect traffic data in ten second intervals to verify packet loss in the data set

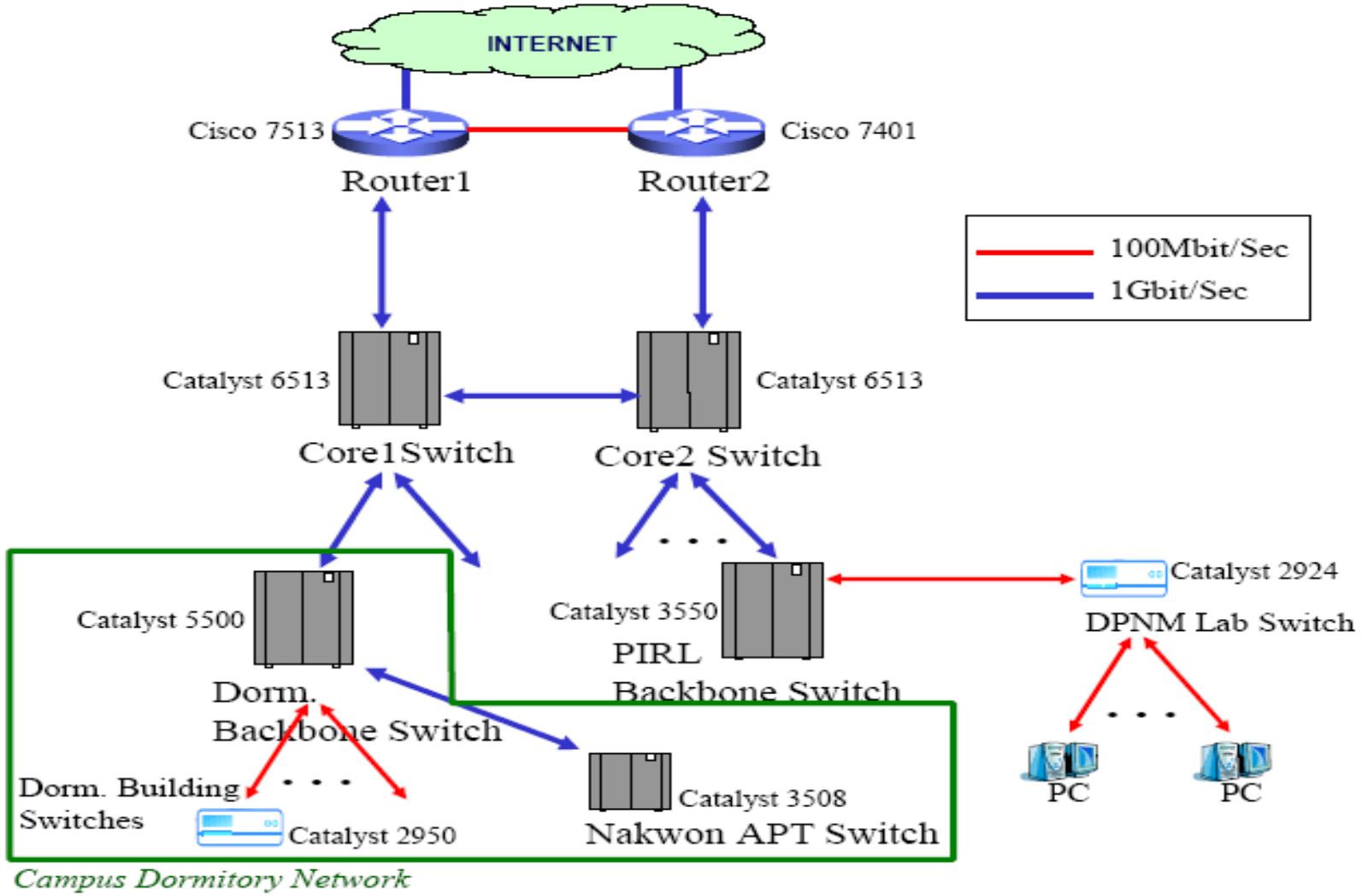
3. We analyze data sets obtained by the step above in offline, and show bursty packet loss characteristics on underutilized link

Traffic Data Collection

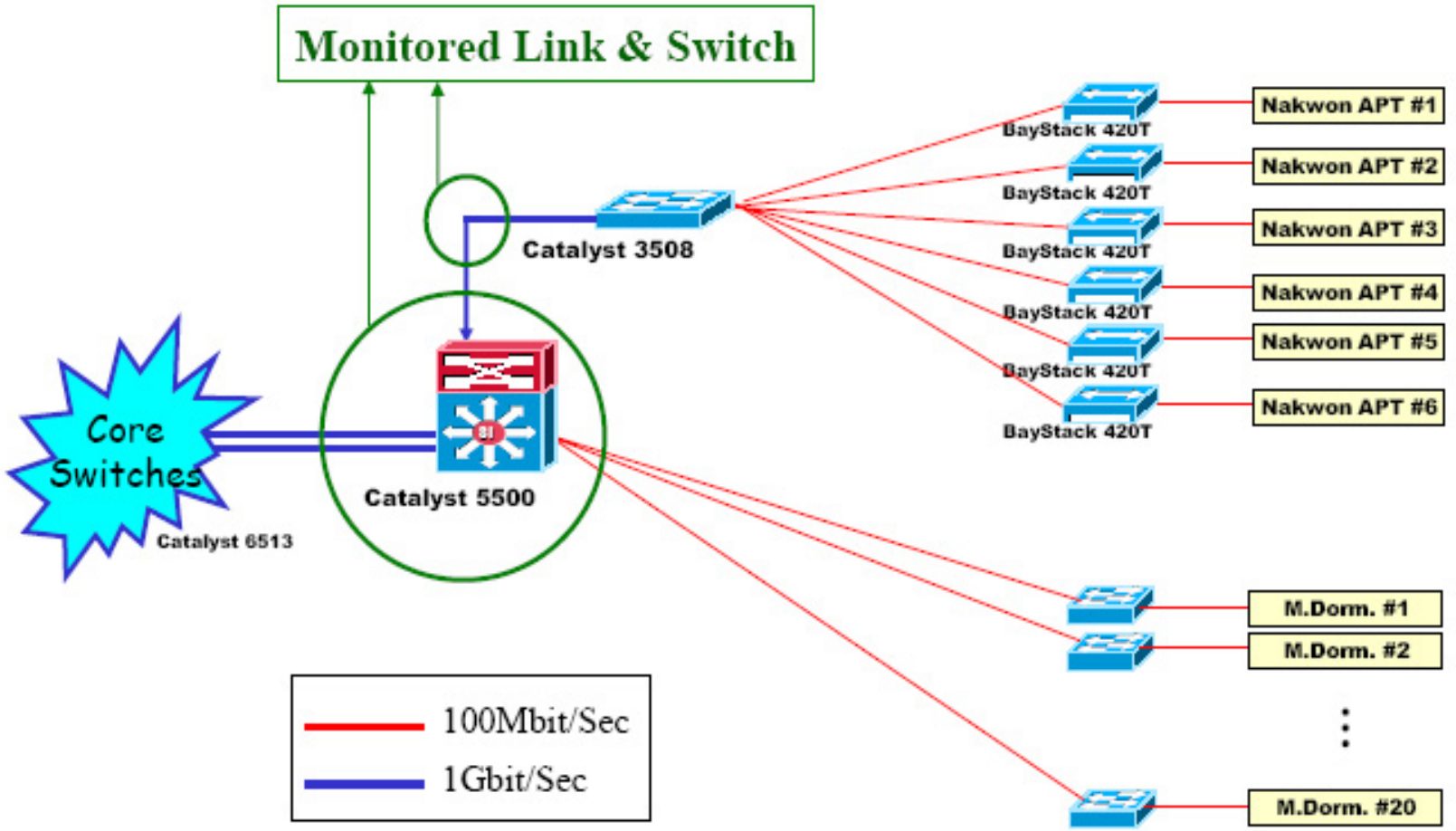
- POSTECH Campus Network
  - two Internet routers, two core backbone switches, two dozens of gigabit building backbone switches, and hundreds of 100 Mbps switches and hubs

- Link to Monitor
  - Continuously Underutilized Link
  - Traffic composed of many internet applications
  - Port on link has Cisco enterprise MIB

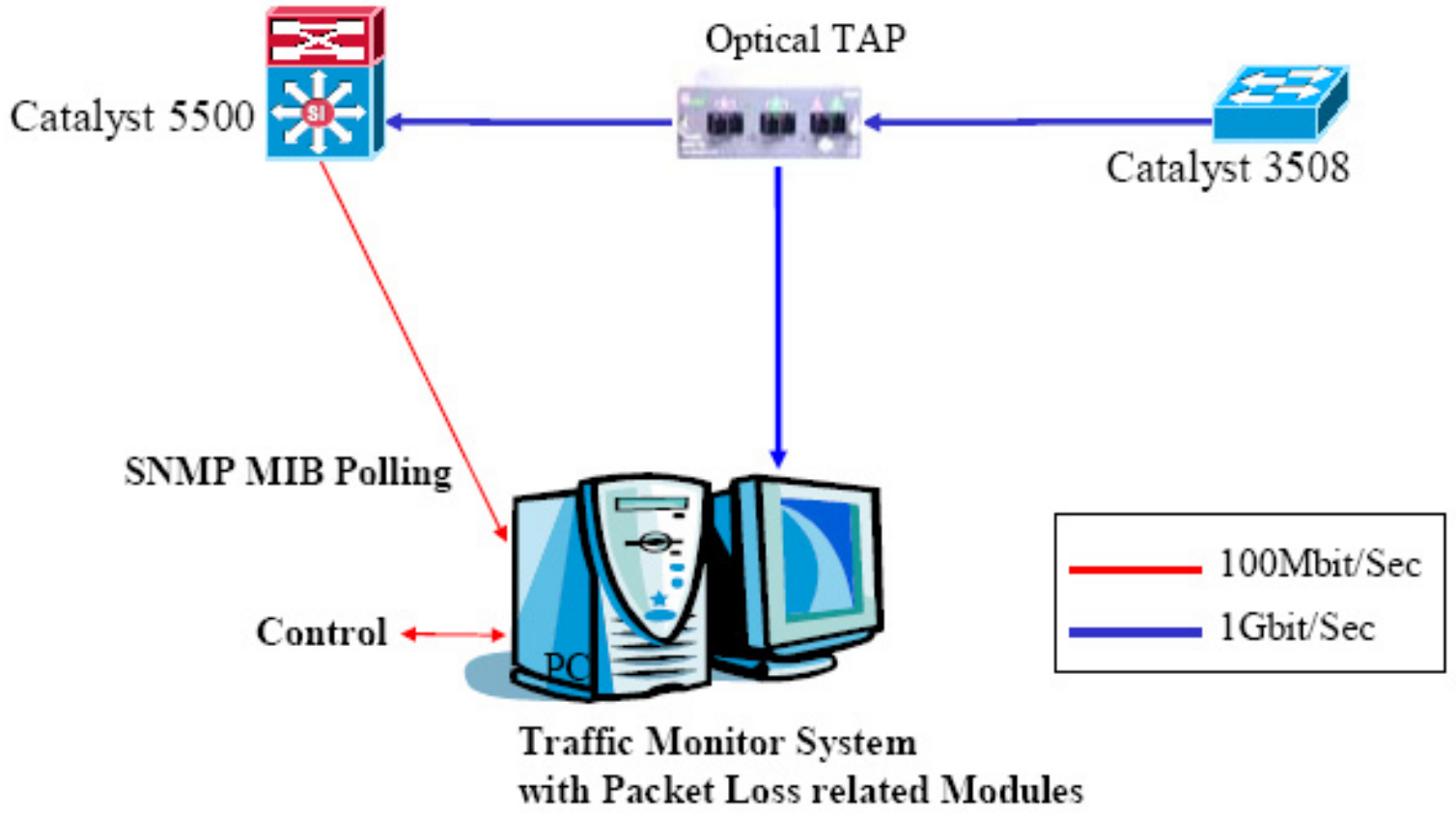
Traffic Data Collection
POSTECH Campus Network Overview



Traffic Data Collection
POSTECH Dormitory Network Overview



Traffic Data Collection
Experimental Environment Overview



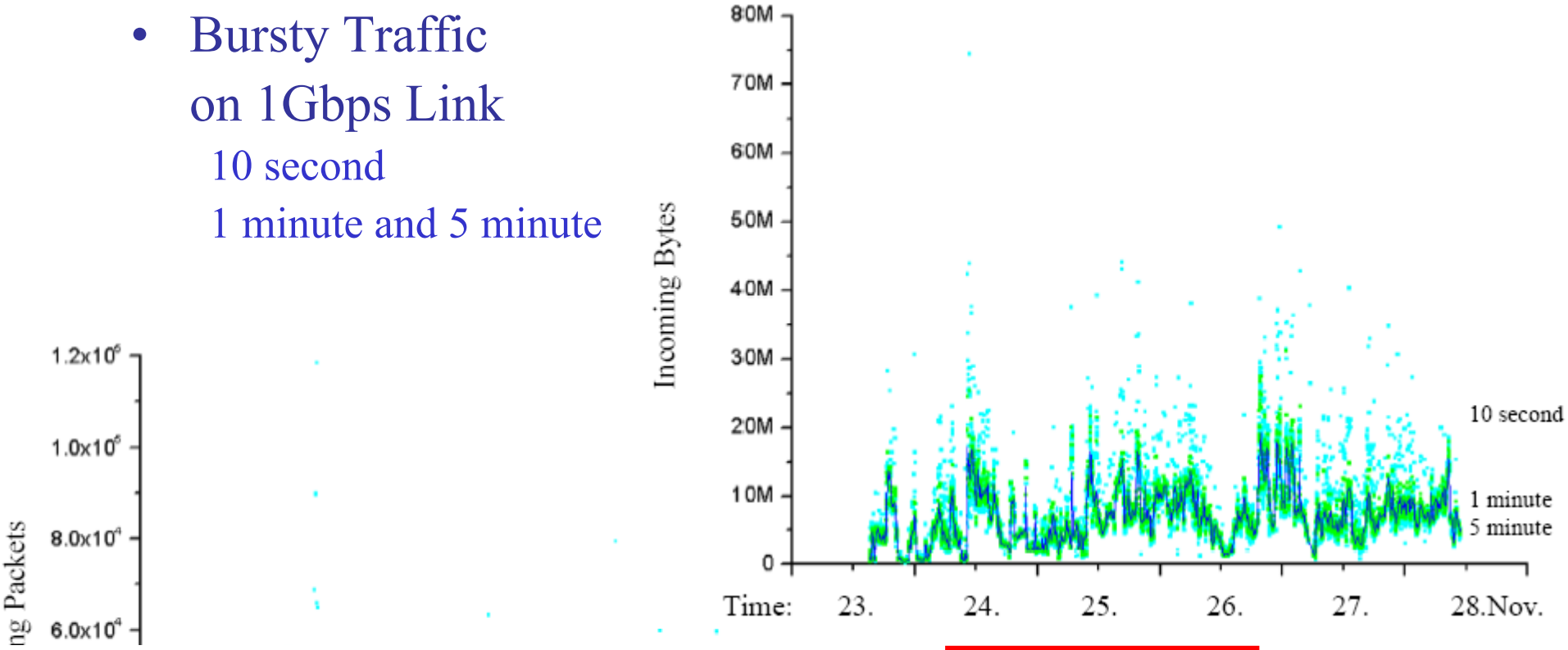
Analyzing Packet Loss and IP Traffic

- Data collected over one week
  - The upLink between Dormitory Backbone Switch and Sub-dormitory Switch (Nakwon APT)
  - from 2004.11.23 2:00pm to 2004.11.30 3:00pm

1. Bursty Traffic & Packet Loss
   - 10 second, 1 minute and 5 minute
2. Bursty Traffic in Small Time Scale
   - 10 millisecond and Real-time
3. Packet Size Distribution
   - Real-time
4. Flow Analysis
   - 10 millisecond, 1 second and 1 minute

Analyzing Packet Loss and IP Traffic

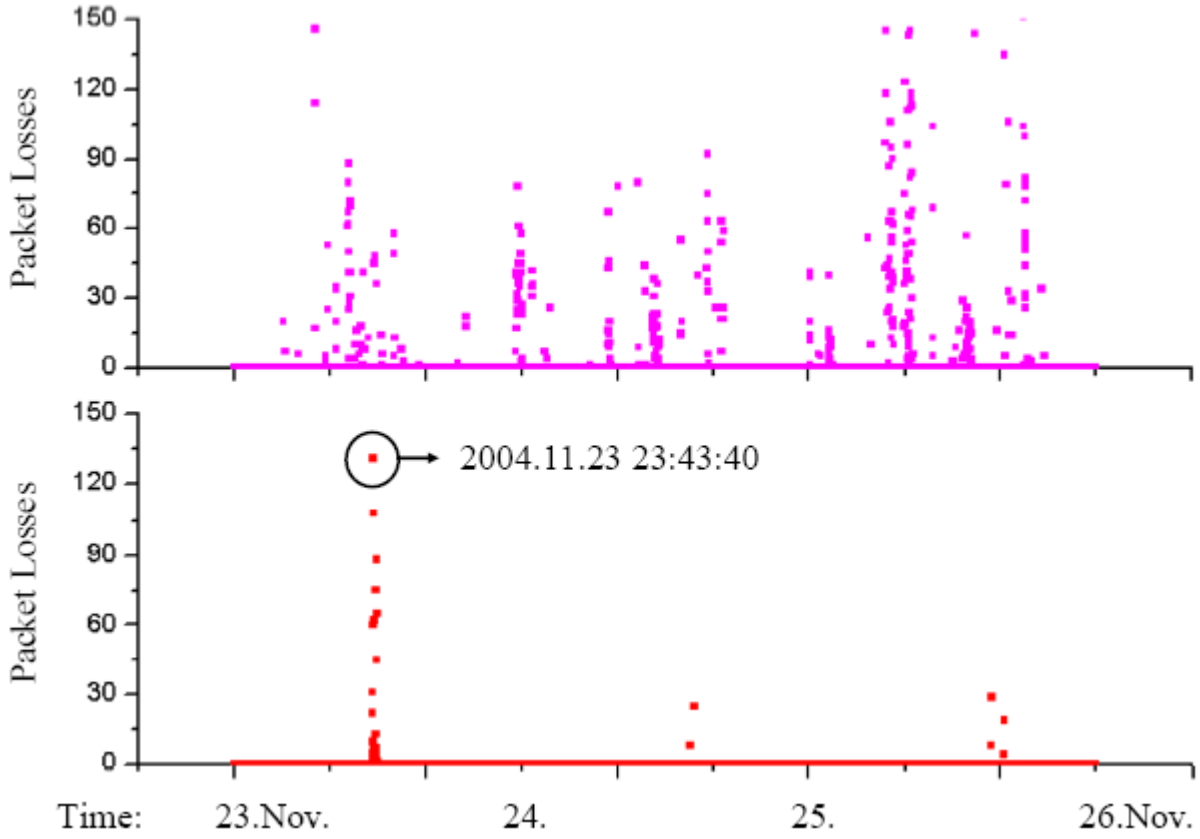
- Bursty Traffic on 1Gbps Link
  - 10 second
  - 1 minute and 5 minute



Time Interval	Min.	Max.	Mean	Standard Dev.	Standard Dev. divided by Avg.
10 second	112235	95294848	6424751	4578390	0.71
1 minute	160218	49847286	6416863	4257214	0.66
5 minute	285986	45501012	6438273	4144063	0.64

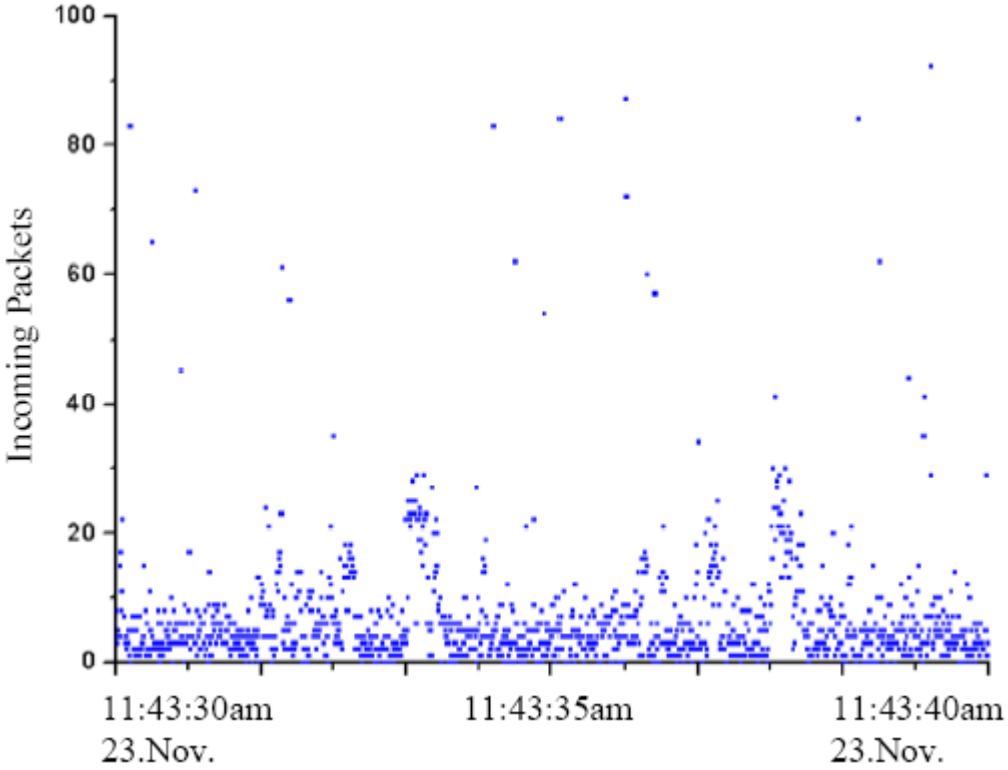
Analyzing Packet Loss and IP Traffic

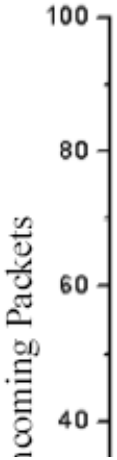
- Analysis of traffic data on the Packet Loss
  - Only our experimental port has the packet loss
  - Packet loss characteristics are not affected by traffic of other ports



Analyzing Packet Loss and IP Traffic

- Bursty Packets
  - 10 millisecond
  - Over 10 second

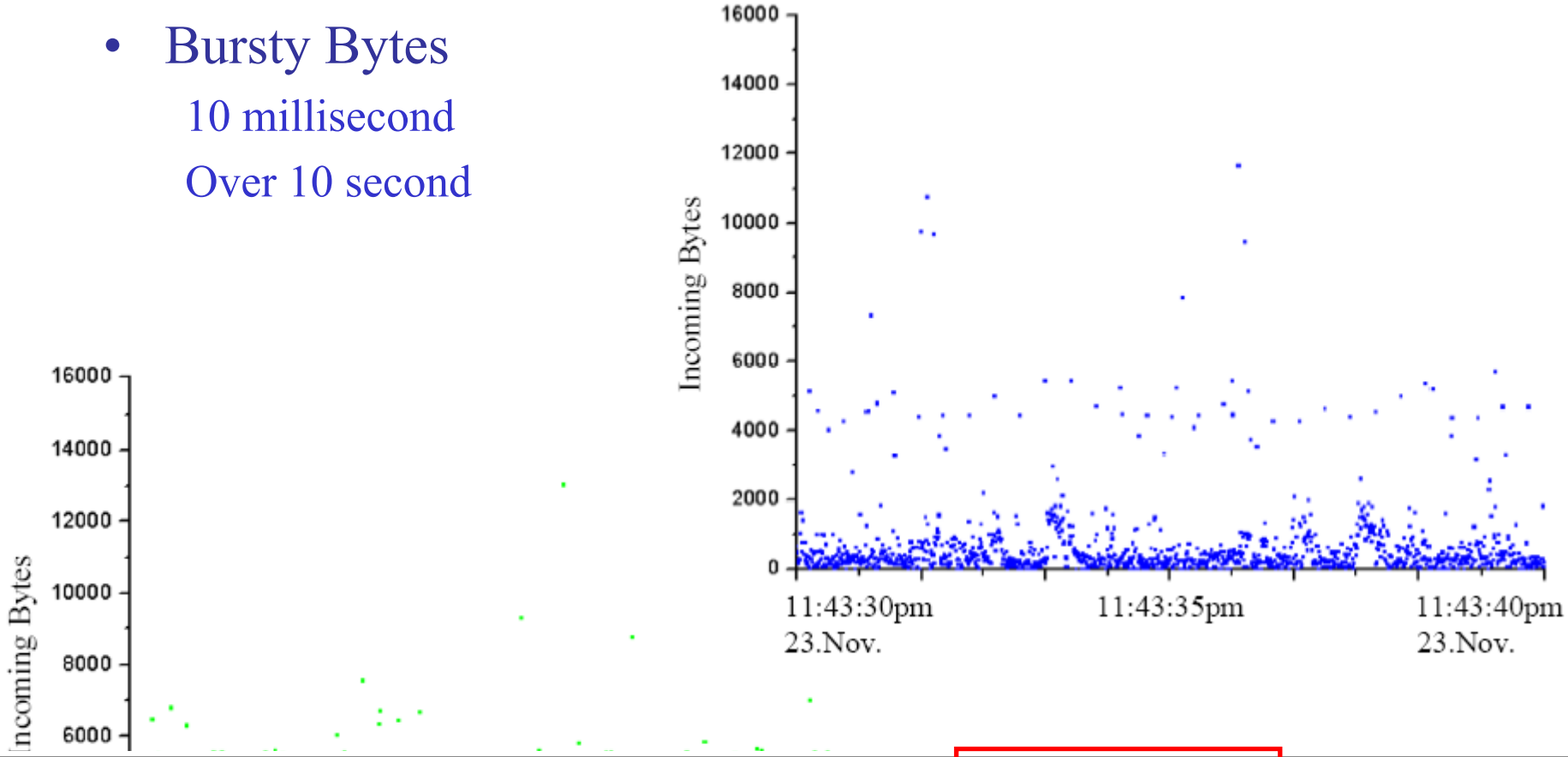




Packet Loss?	Min.	Max.	Mean	Standard Dev.	Standard Dev. divided by Avg.
No	1	32	11	4	0.36
Yes	0	196	8	15	1.87

Analyzing Packet Loss and IP Traffic

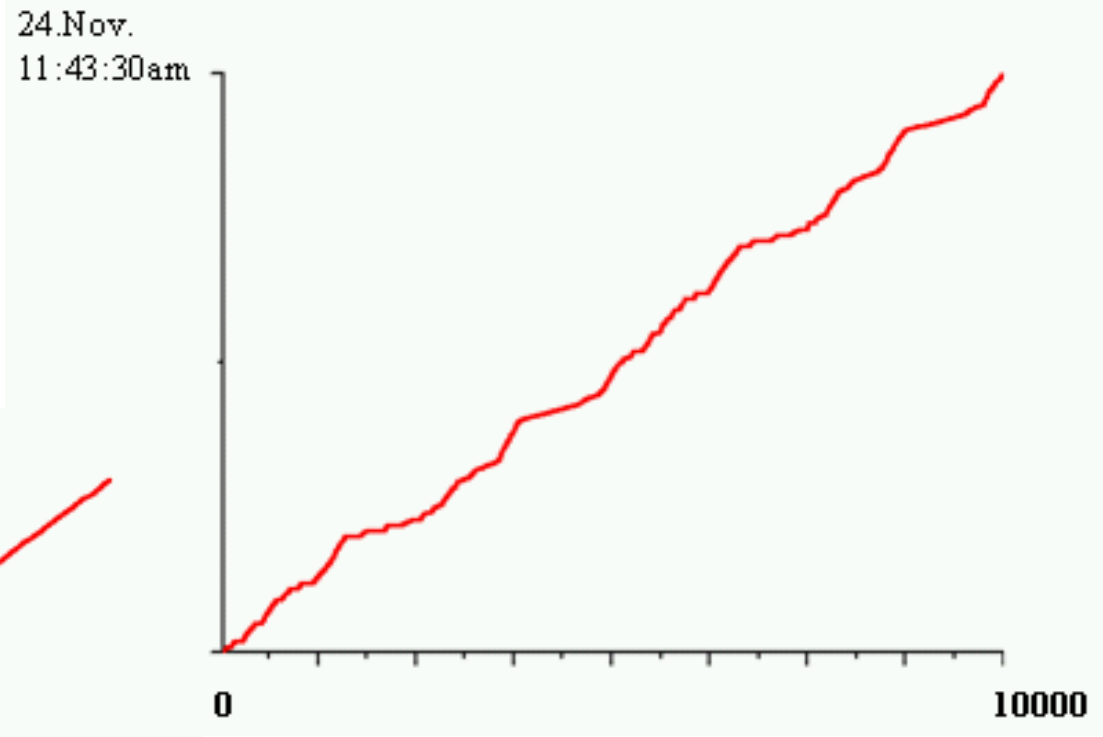
- Bursty Bytes
  - 10 millisecond
  - Over 10 second

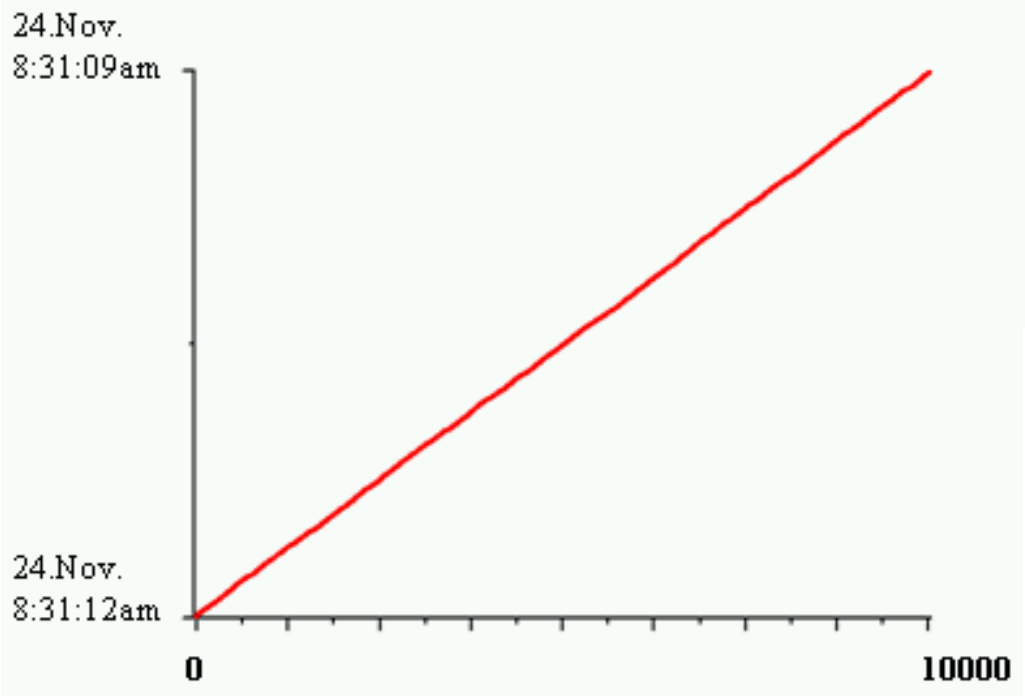


Packet Loss?	Min.	Max.	Mean	Standard Dev.	Standard Dev. divided by Avg.
No	60	13948	1730	1932	1.11
Yes	0	12212	680	1187	1.74

Analyzing Packet Loss and IP Traffic

- Interarrival Time
  - Real-time
  - Over 10 Seconds



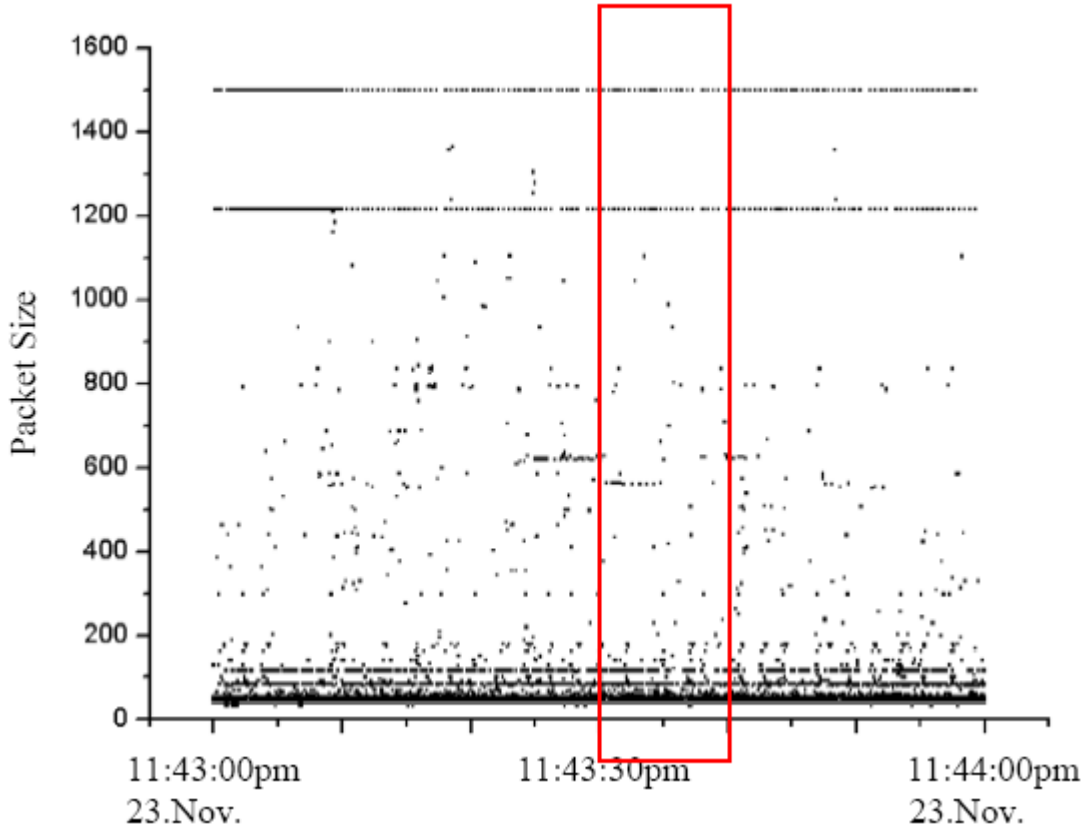


Bursty Packets

On the Packet Loss Time

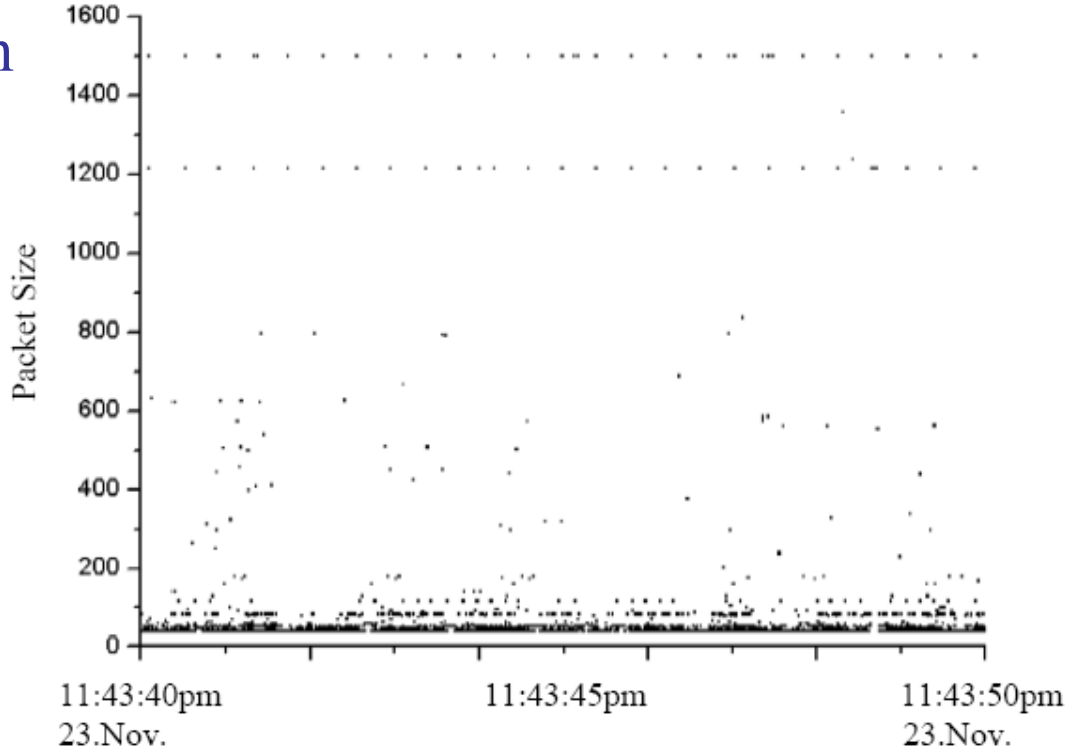
Analyzing Packet Loss and IP Traffic

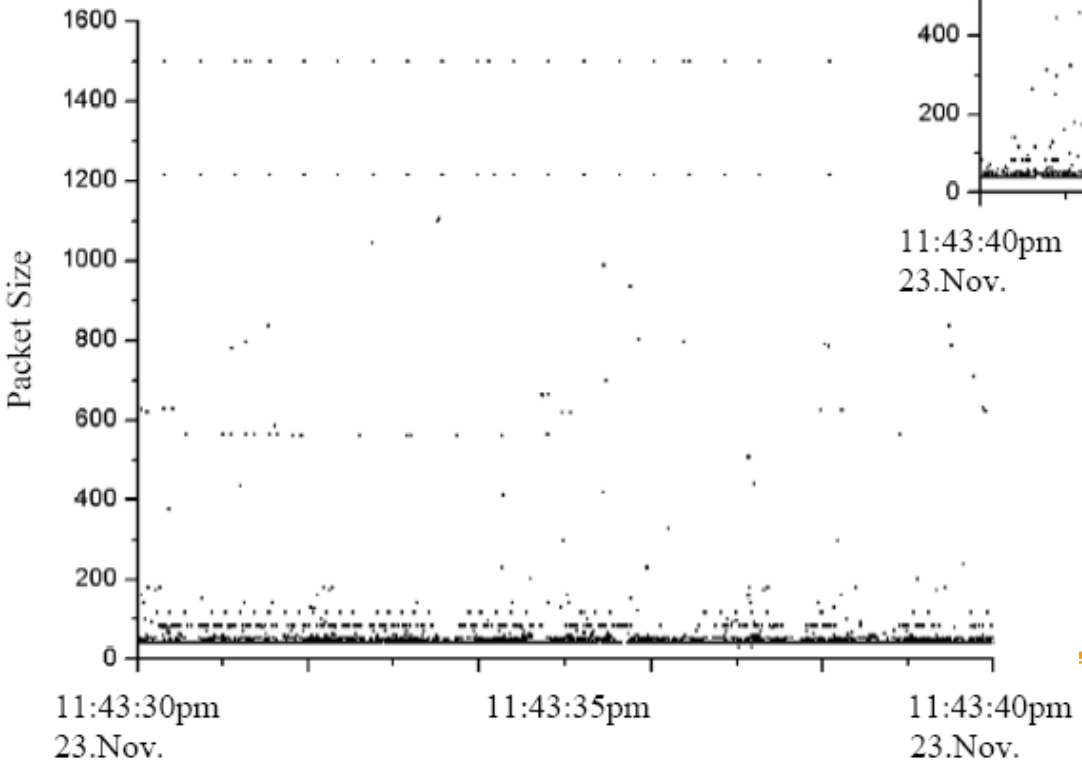
- Packet Size Distribution
  - Certain packet sizes are more popular than others
  - No special characteristics for the packet loss



Analyzing Packet Loss and IP Traffic

- Packet Size Distribution
  - Real-time
  - Over 10 Seconds

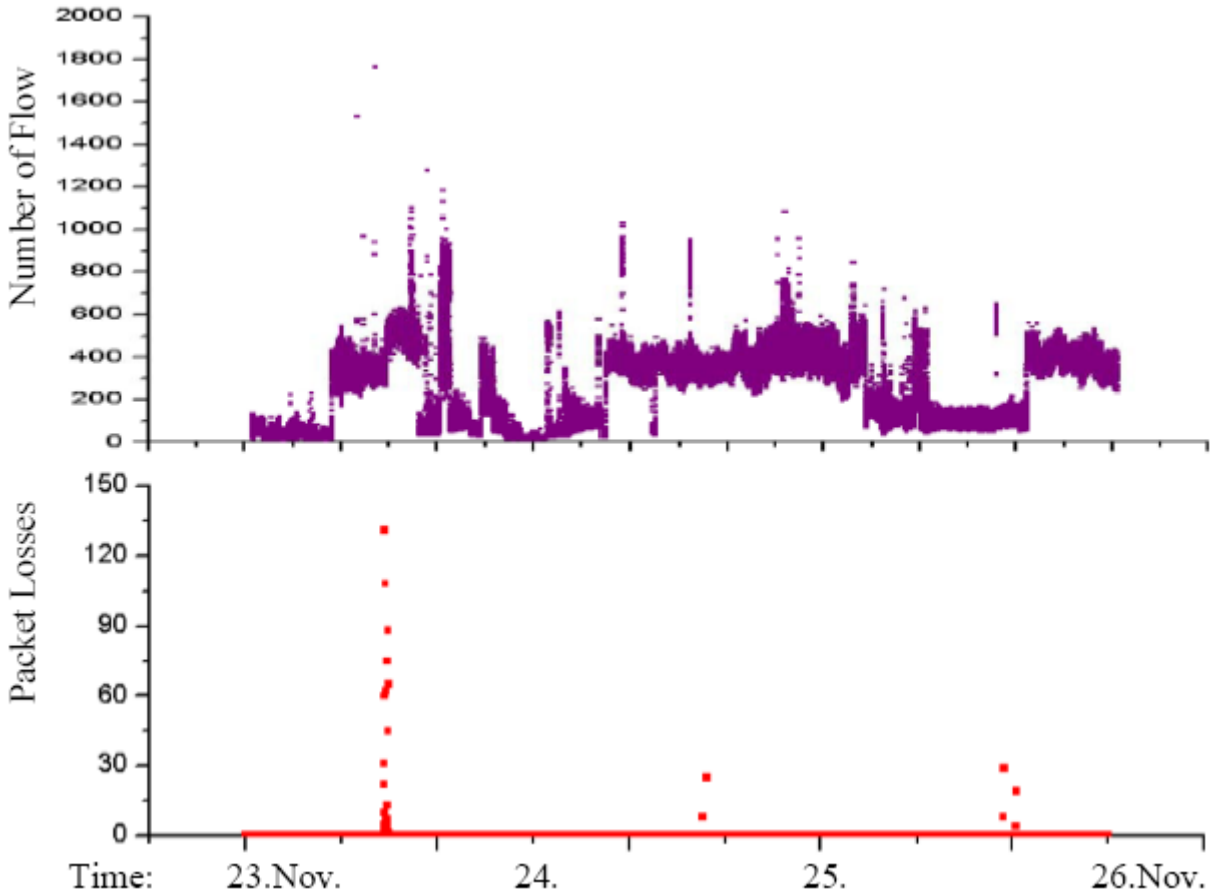




Do not affect
the Packet Loss

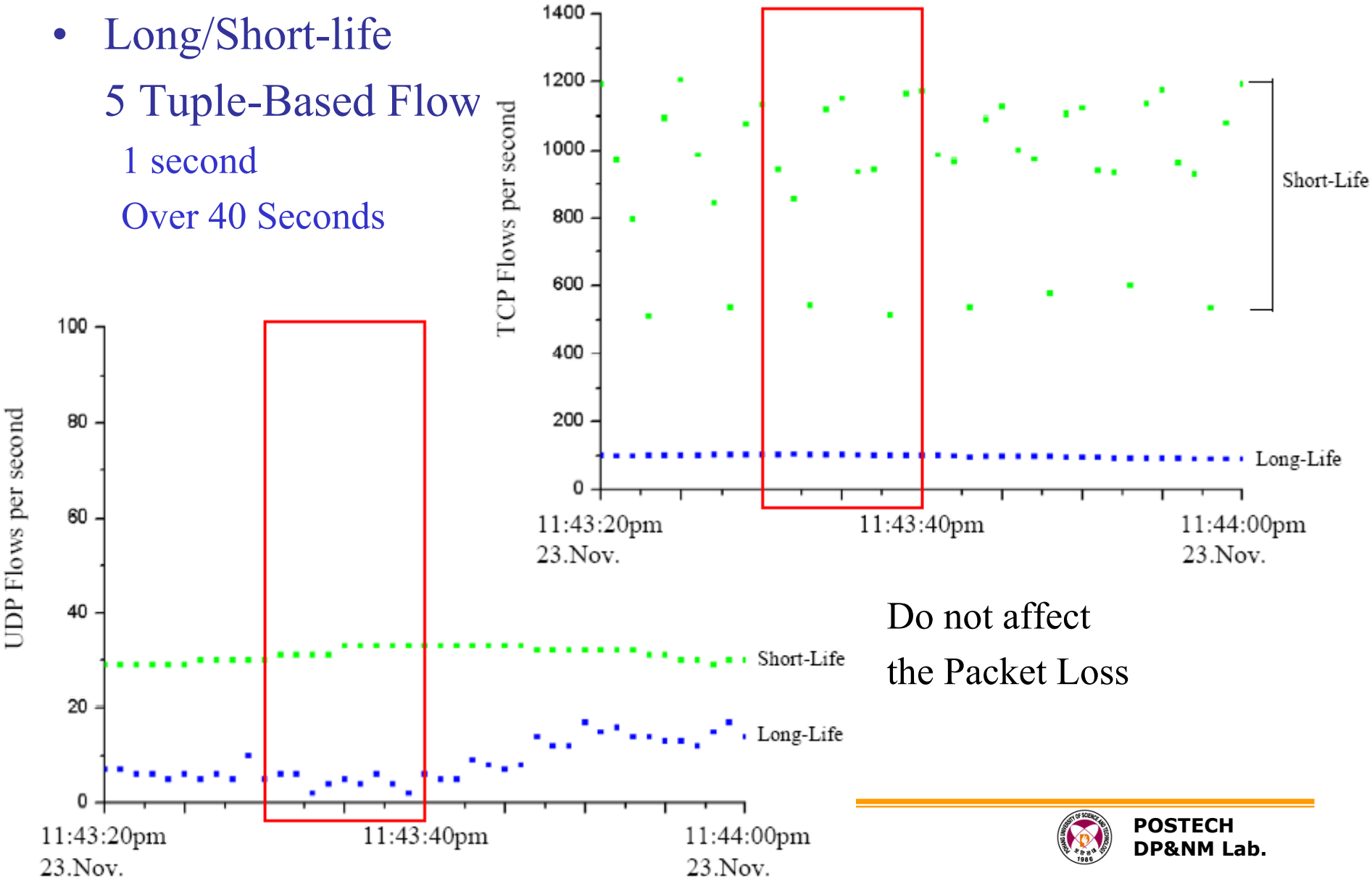
Analyzing Packet Loss and IP Traffic

- 5 Tuple-based Flow (Src/Dst IP Address, Src/Dst Port, Protocol)
  - 1 Second time granularity & No special characteristics



Analyzing Packet Loss and IP Traffic

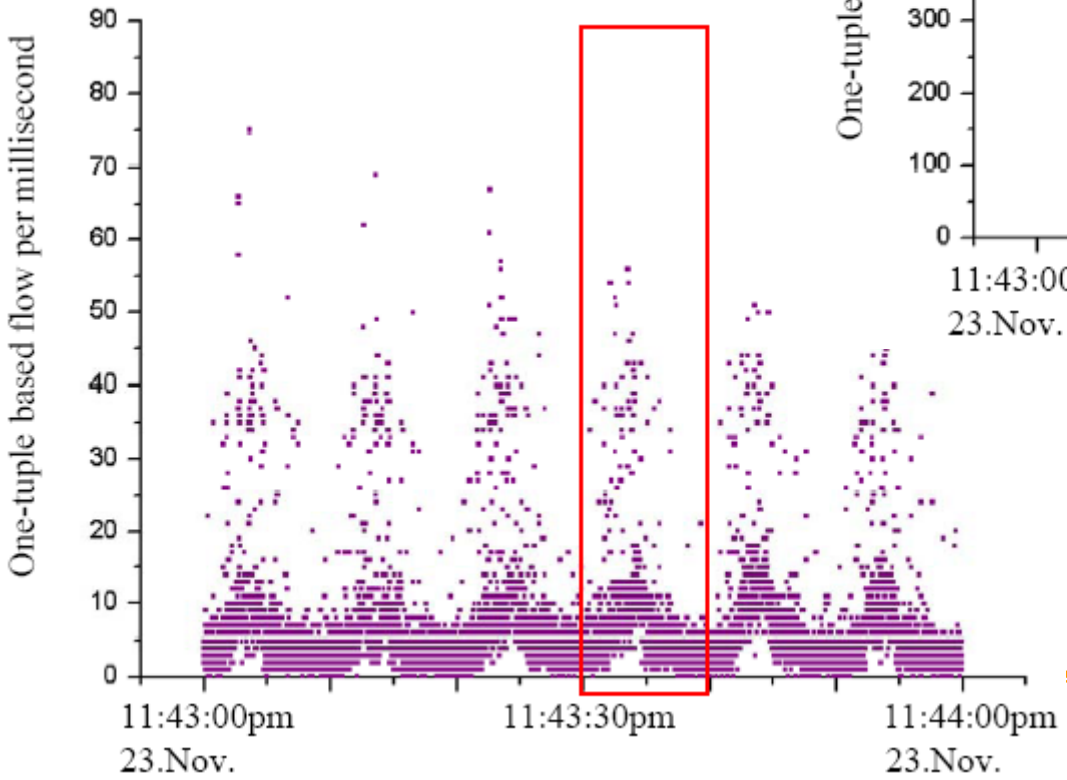
- Long/Short-life
  5 Tuple-Based Flow
  1 second
  Over 40 Seconds

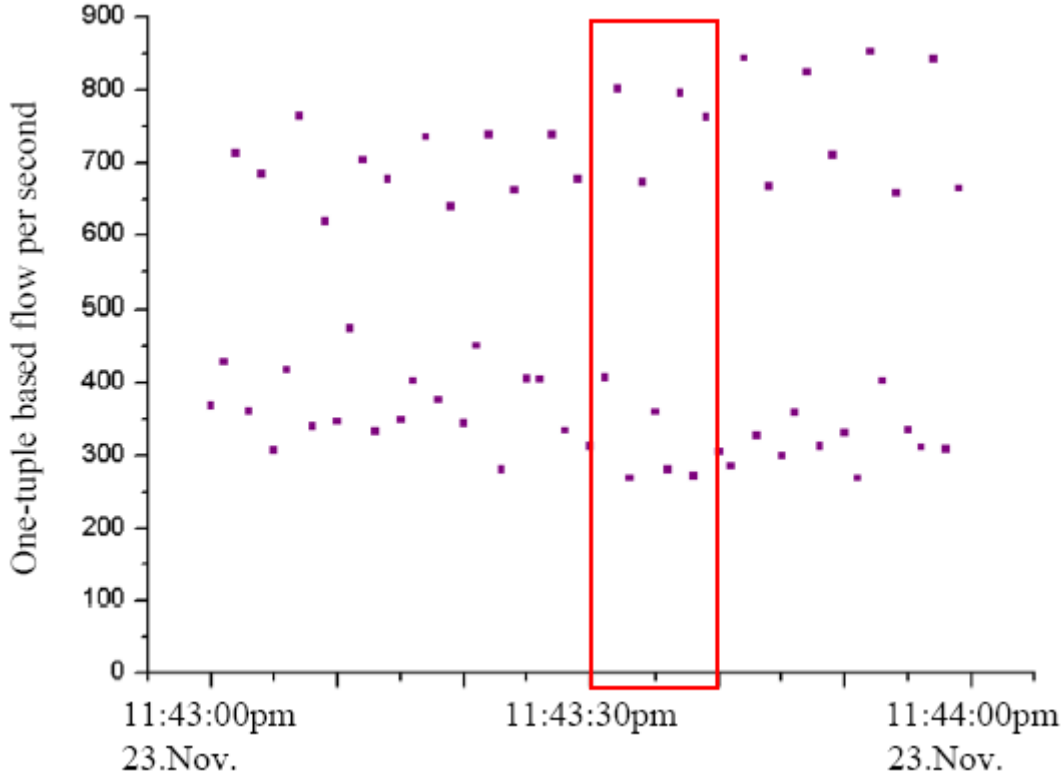


Do not affect
the Packet Loss

Analyzing Packet Loss and IP Traffic

- 1 Tuple-Based Flow (Destination IP Address)
  - 1 second, 10 millisecond
  - Over 1 minute





Do not affect
the Packet Loss

Concluding Remarks

- Collecting data from POSTECH dormitory network
  - Underutilized Link During Observation (5% Utilization)
  - Various Internet Application Traffic generated by many students

- Analysis of Packet Loss and IP Traffic
  - Packet Losses occur on Underutilized Links
  - The traffic bursts do occur at small time granularity
    - such as 10 seconds, 10 milliseconds
  - Bursty Packets are main reason for the packet loss
  - Bursty Bytes & Packet Size are not matter for the packet loss on underutilized link
  - Number of flows do not affect the packet loss

Future Work

- CPU & Packet Loss
  - CISCO enterprise MIB offers 5 second avg. value of CPU load
  - Detecting Bursty CPU load

- Detecting Packet Loss characteristics of Applications on First-Contact Hub
  - Web, FTP and P2P, etc

- The time granularity of 10 milliseconds can be still large for router/switch process
  - With the help of hardware (e.g. DAG Card) we try to monitor the packet loss characteristics in microsecond unite

Questions?