Cause Analysis of Packet Loss in Underutilized Enterprise Network Links

2005.12.21
Thesis Defense

Deepali Agrawal
deepali@postech.ac.kr

Distributed Processing & Network Management Lab.
Department of Computer Science & Engineering
POSTECH

Contents

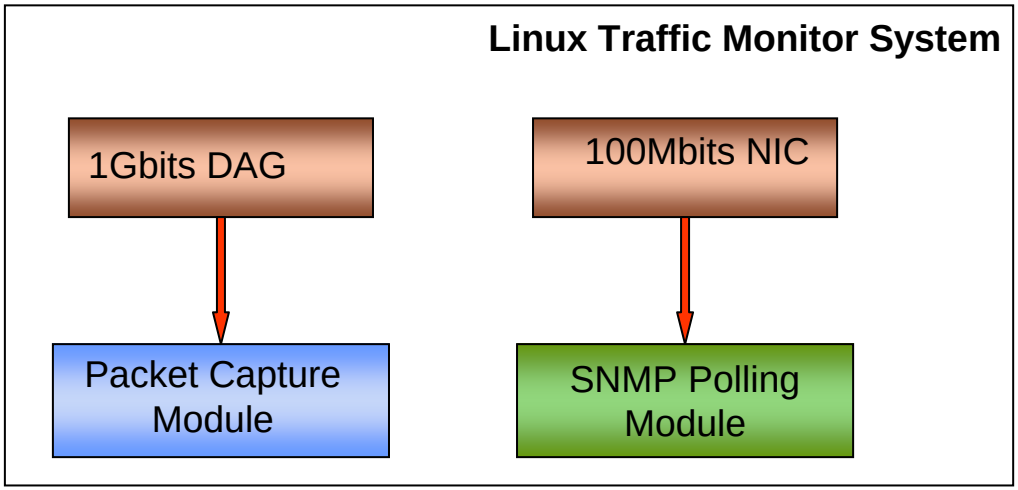
Introduction

- ISPs Employ Overprovisioning
  - Increasing number of users and applications
- Performance Problems
  - Packet loss, delay and jitter
  - Network applications: VoIP, multimedia, games and P2P
- Goal
  - Study traffic and packet loss characteristics
  - Determine the root cause of packet loss phenomenon
- Approach
  - Developed a root cause analysis method
  - Developed set of tools to execute the methodology

Related Work

- Most of the studies focus on packet delay analysis
  - Packet loss and delay are closely related
- Network Performance Monitoring at Small Time Scales
  - Papagiannaki *et. al.* (IMC 2003)
  - Attributed high delays to congestion in the routers
- Origins of Microcongestion in an Access Router
  - Papagiannaki *et. al.* (PAM 2004)
  - Identified and discussed causes of microcongestion: link bandwidth, multiplexing and traffic burstiness
- Detection and Analysis of Packet Loss on Underutilized Enterprise Networks
  - Chung et al. (E2EMON 2005)
  - Indicated that only bursty packets affect the packet loss

Traffic Monitoring and Loss Detection



Module Name	Description
SNMP Polling Module	This module polls Cisco standard MIB II and private MIB variables
Packet Capture Module	This module captures packet trace using DAG API

SNMP Polling

- Monitor traffic and switch status
  - By polling standard MIB II variables at 1 second granularity

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

Packet Loss Detection Using SNMP

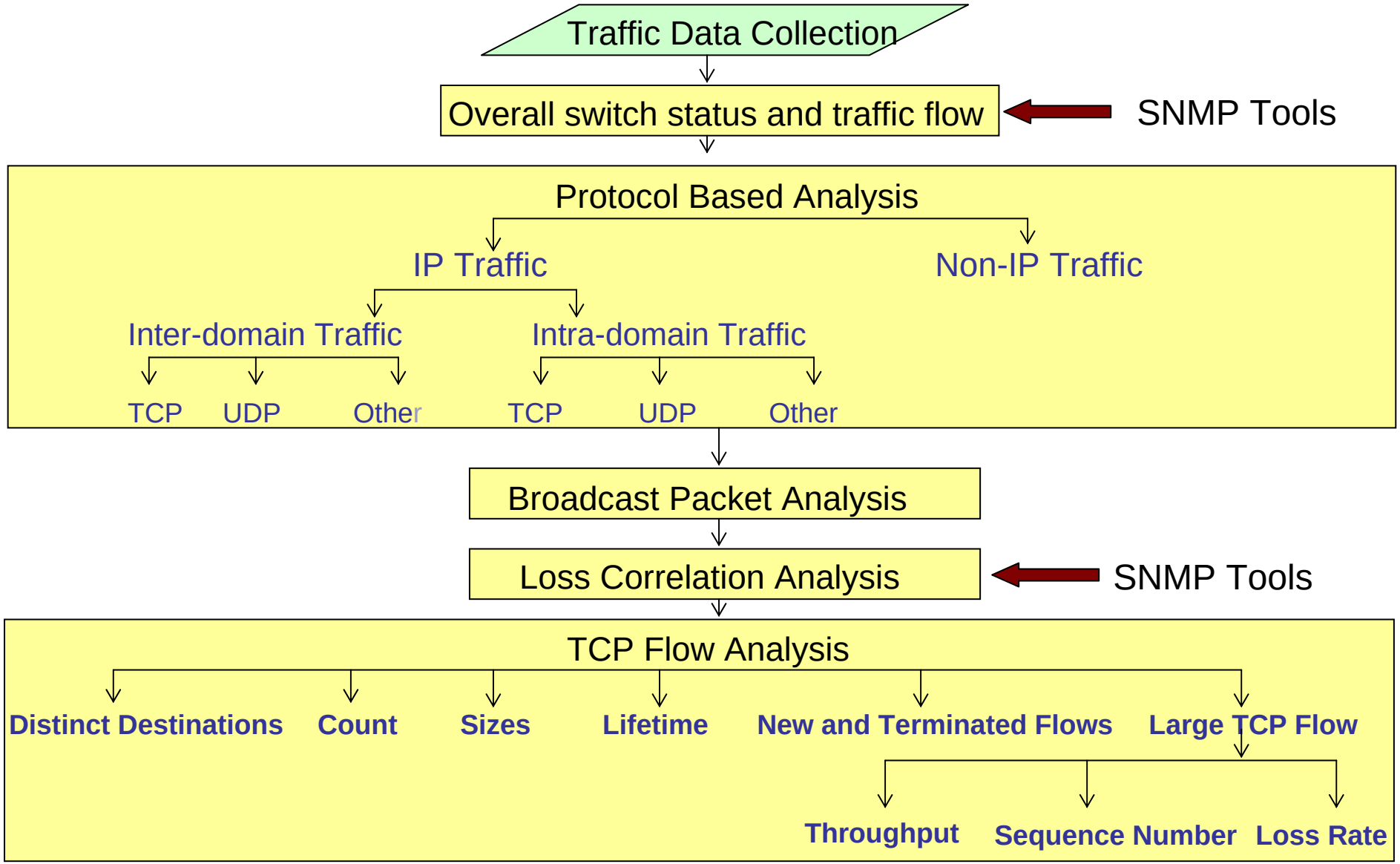
- Packet loss information
  - Using Cisco enterprise MIB variables
- Each interface owns input queue and output queue
- Packet Loss = Input Queue Drops + Output Queue Drops

Object	**OID**	**Description**
cpuLoad	1.3.6.1.4.1.9.2.1.56	CPU Utilization (5 sec avg.)
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

Packet Capture Using Network TAP

- SNMP
  - Inaccuracies due to high response loss rate
  - Time granularity not satisfactory enough
    - Need finer time analysis for cause detection
- Optical TAP
  - Packet trace capture using DAG card
  - Guaranteed lossless performance in gigabit link
  - High precision time stamps
- Packet Capture Module
  - Implemented using C API of DAG
  - Provides highest performance

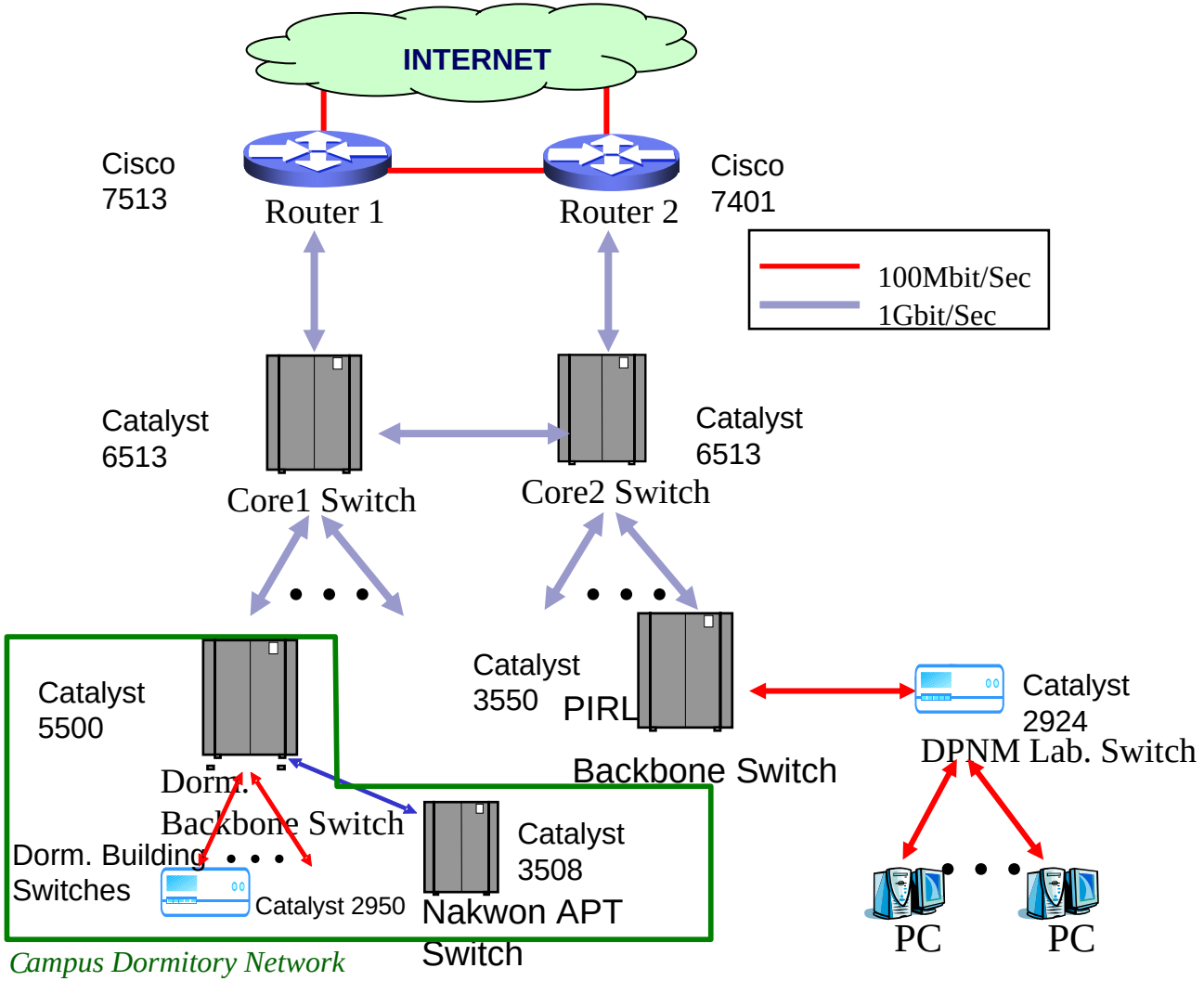
Cause Analysis Method



Traffic Data Collection

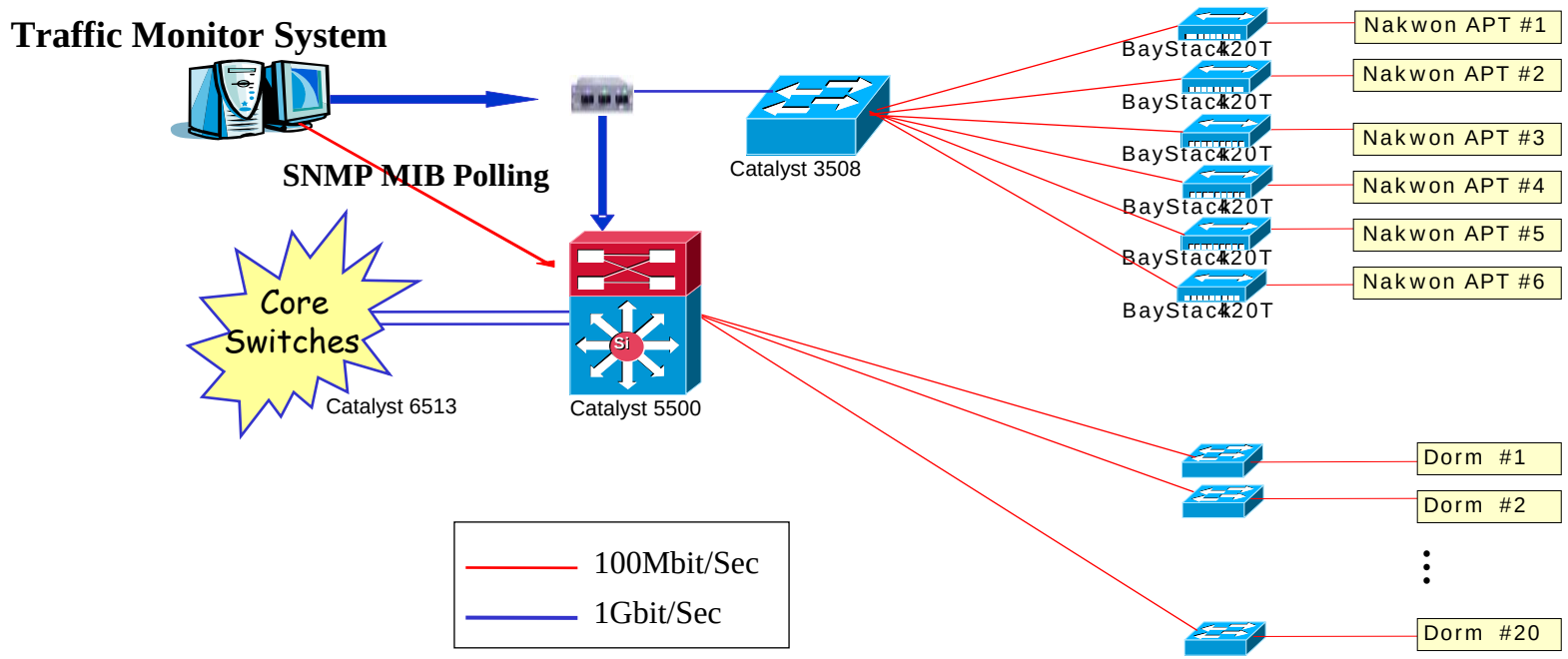
- POSTECH campus network
  - Composed of two IP routers, two core backbone switches, dozes of gigabit switches and hundreds of 100mbps switches
- Monitored Link
  - Always underutilized
  - Convey traffic composed of many internet application
- Link located in campus dormitory network

Traffic Data Collection



POSTECH Dormitory Network Overview

- Monitored link connecting Nakwon Apt to dormitory backbone switch
- Data collection over 4 months, interleaved with analysis



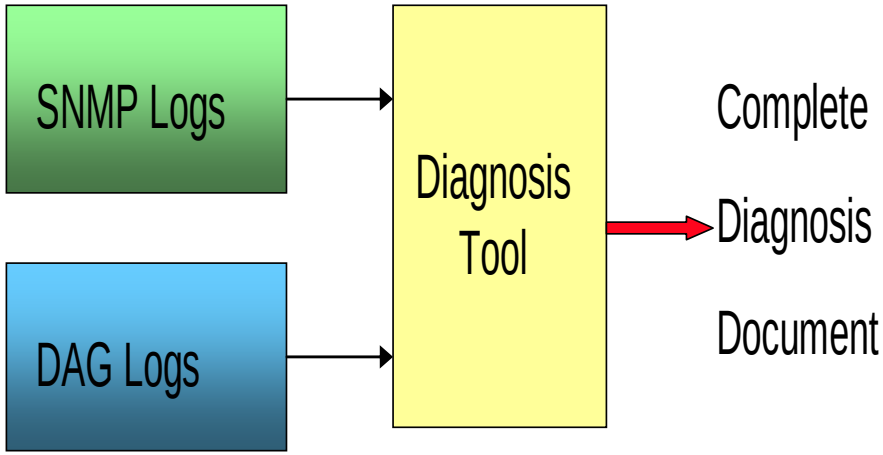
Analysis Tools
SNMP Logs Processing Tools

Tool Name (Perl Script)	**Input**	**Output**	**Function**
Interface Count	SNMP Log file	Text file	Count of interfaces those experience losses simultaneously
Interface Index	SNMP Log file	Text file	Index of interfaces those experience losses simultaneously
Response Loss Rate	SNMP Log file	Text file	Time in Unix seconds when the SNMP response is not received
Average	SNMP Log file	Text file	Averaged values for specified seconds
Total	SNMP Log file	Text file	Total count across all ports

Analysis Tools
DAG Logs Processing Tools

Tool Name (C programs)	Input	Function
Utilization measure	DAG Logs	Inter domain and intra domain bit counts (at 1s, 1ms and 1us scale)
Protocol Analysis	DAG Logs	Inter & intra domain Bit Counts : TCP, UDP and Other (1s, 1ms & 1us)
Flow generator	Binary and ascii flow file	Generate 4 (src/dst IP, src/dst port) tuple based TCP flows
Flow count	Binary Flow file	Inter/intra domain flow counts per second
Flow lifetime and size	Binary Flow file	Inter/intra domain flow lifetime and sizes
New and Exit Flow	Binary Flow file	New and terminated flow counts and sum of their sizes per second
Distinct destination	Binary Flow file	Count of distinct destinations to which each source IP connects
Top_n_flow	Binary Flow file	flows of size in the specified range
Data Rate	Binary Flow file & DAG logs	pps and BPS of the selected flow (at 1s, 1ms and 1us scales)
Run length and loss rate	Binary Flow file & DAG logs	run-length magnitudes and interval between two run-lengths in microsecond
Broadcast packets	DAG logs	Count of IP level broadcast packets (at 1s, 1ms and 1us scales)
Non-IP packets	DAG logs	Count of non-IP packets and ARP packets (at 1s, 1ms and 1us scales)

Analysis Tools

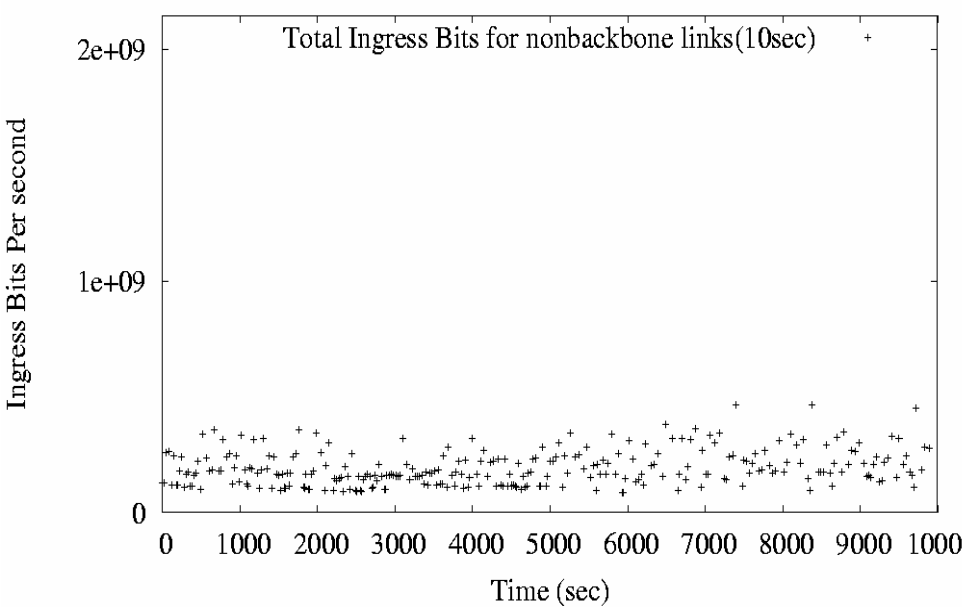


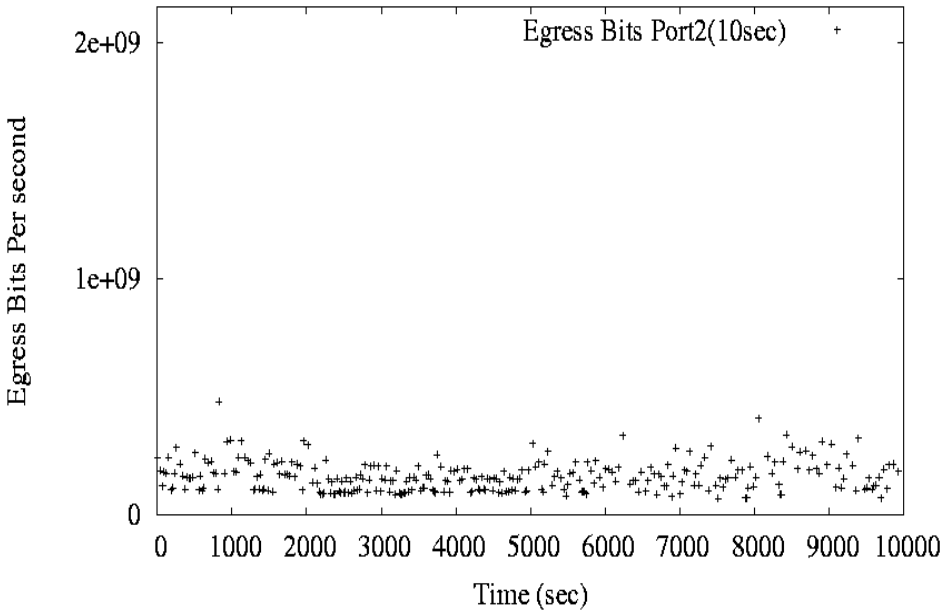
- Generating complete diagnosis document
  - Diagnosis Script: Process data to get useful information
  - Gnuplot Script: Generate plots
  - Latex script: Arrange plots in document

Dorm Backbone Switch
Underutilized Links

Interface Number	Mean Ingress Bits (Mbps)	Standard Deviation (Mbps)	Max (Mbps)	Avg. Utilization (AVG/BW) %	Max Utilization (Max/BW)%
1	0	0	0	0	0
2 (Backbone Link)	265	399.4	829.61	26.5	82.9
3	25.85	38.2	87.10	12.9	43.5
4	12.49	18.3	33.24	6.2	16.6
5	65.86	94.2	196.07	32.9	98
6	30.60	44.5	96.46	15.3	48.2
7	54.07	10.1	37.77	27.0	18.8
8	18.84	29.9	58.31	9.4	29.1
9	4.13	13.0	48.51	2.0	24.2
10	11.69	16.7	28.58	5.8	14.2
11(Nakwon Link)	17.44	27.4	61.82	1.7	6.1

Dorm Backbone Switch
Backbone VS Non-backbone Traffic

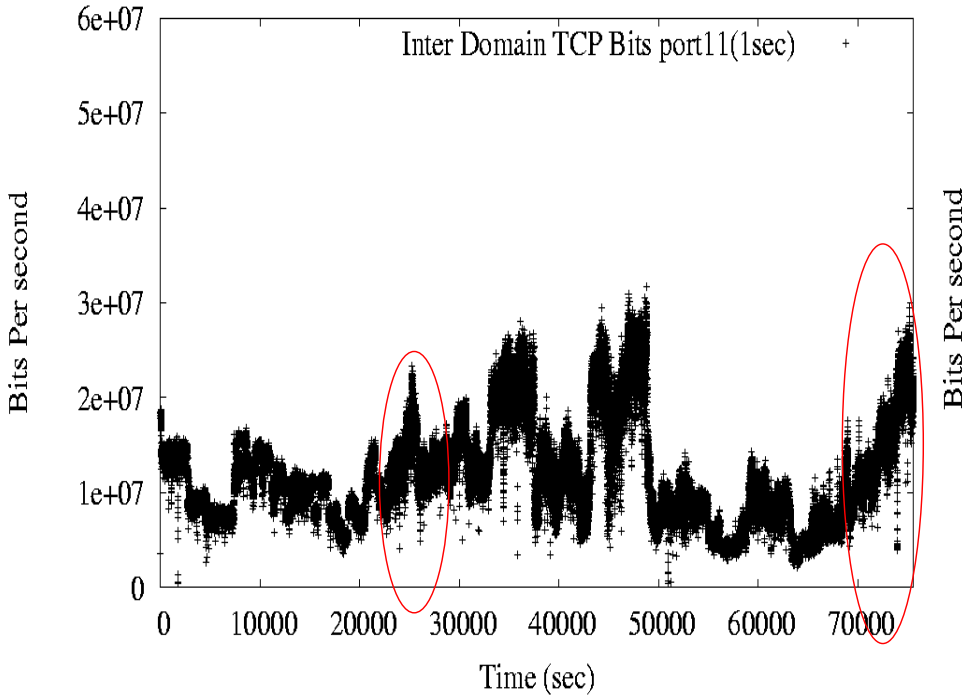


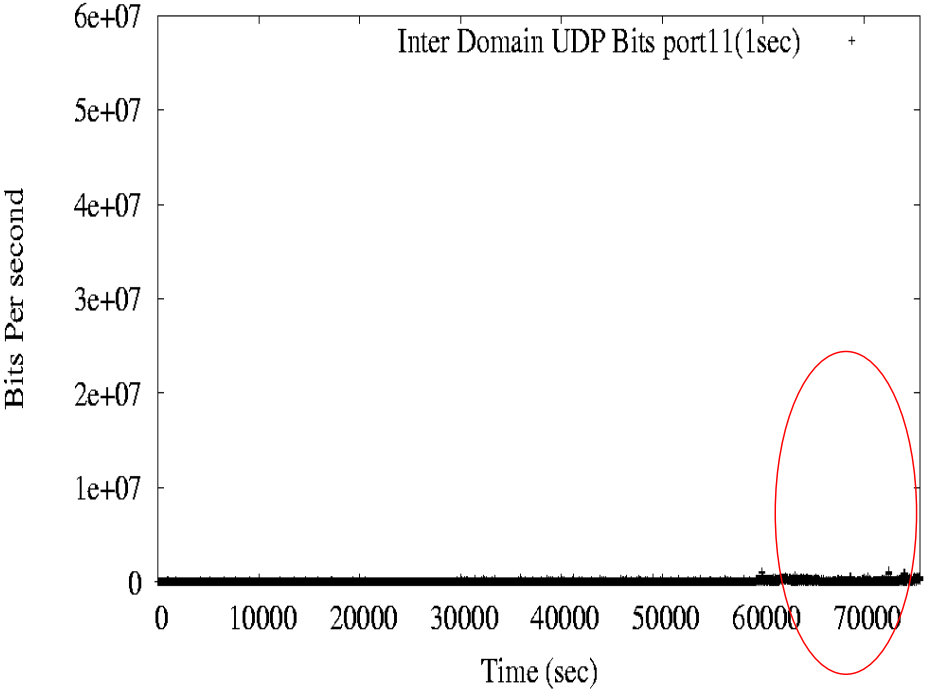


- Switch have single backbone link
- Total ingress traffic across all non-backbone link is equivalent to backbone egress traffic

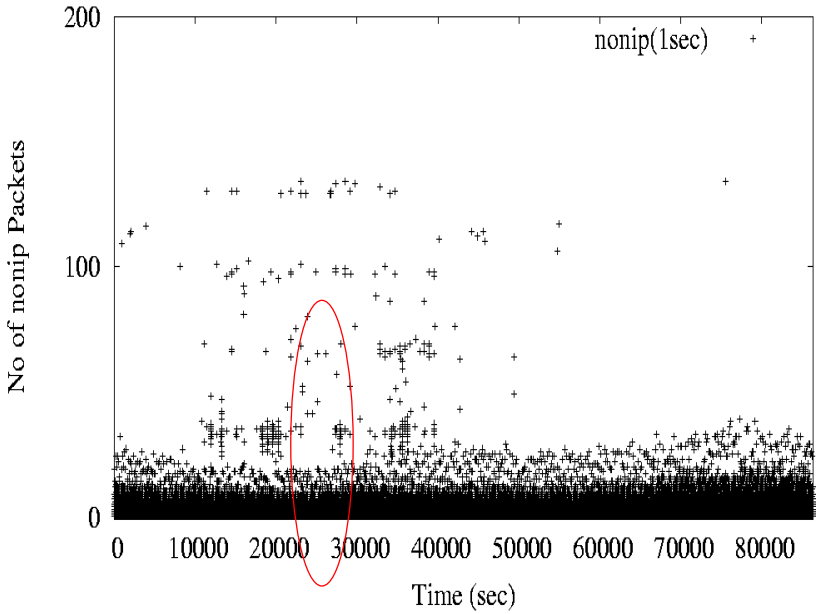
Protocol Based Analysis
IP Traffic

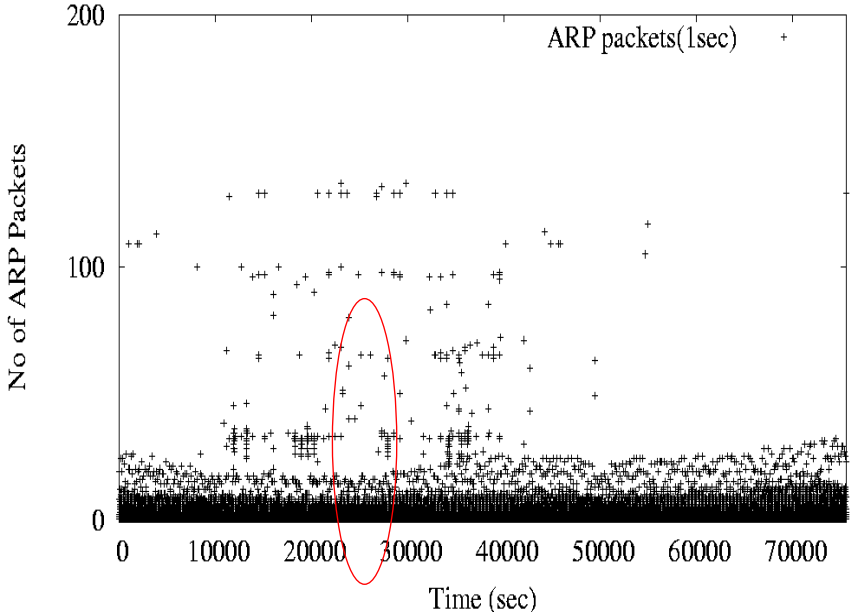
Nak-won link Traffic	TCP	UDP	Other
Intra Domain	2.8%	0.02%	0.003%
Inter Domain	96.7%	0.39%	0.01%



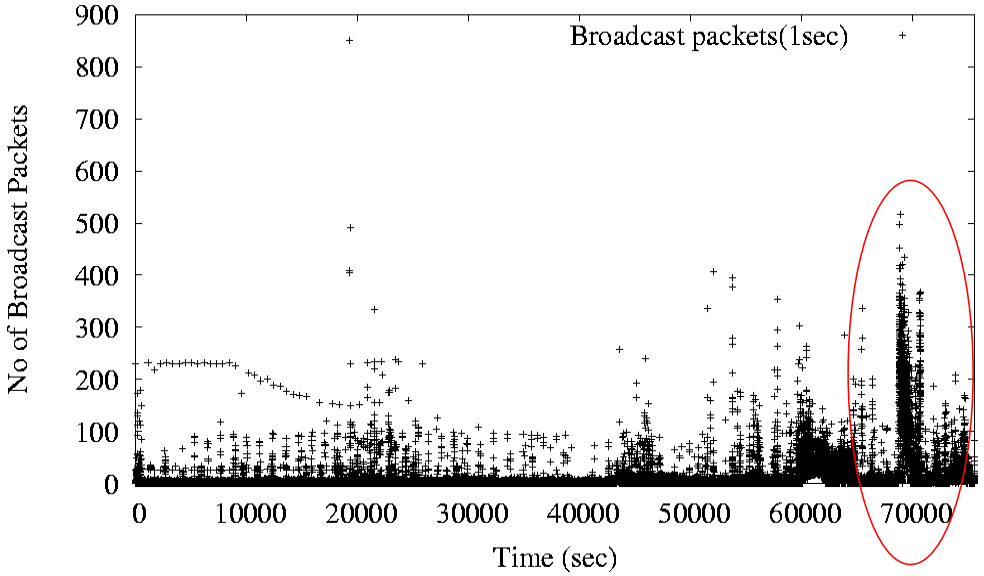


Protocol Based Analysis
Non-IP Traffic





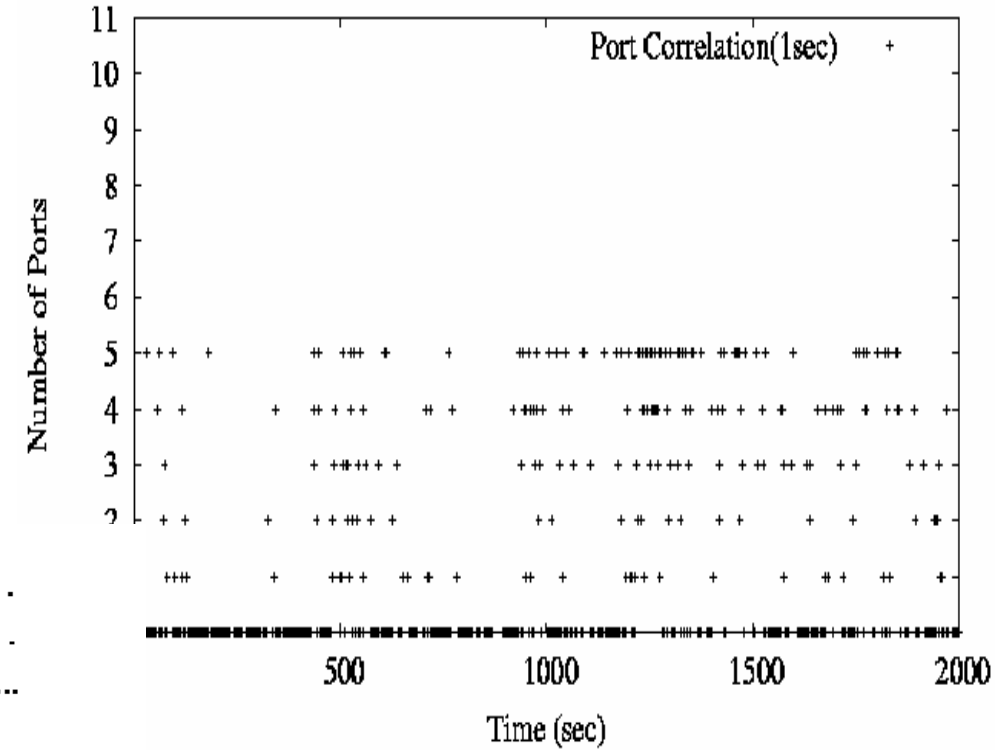
Broadcast Packet Analysis

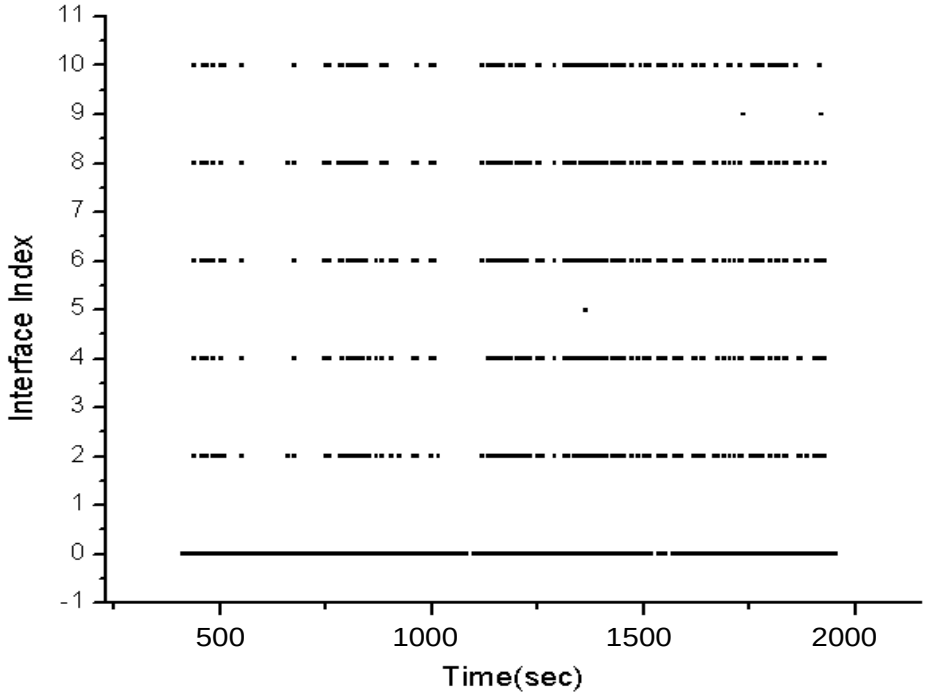


- IP level broadcast packets
- Tie up system resources
- Broadcast packets and packet loss correlation coefficient: -0.009

Loss Correlation

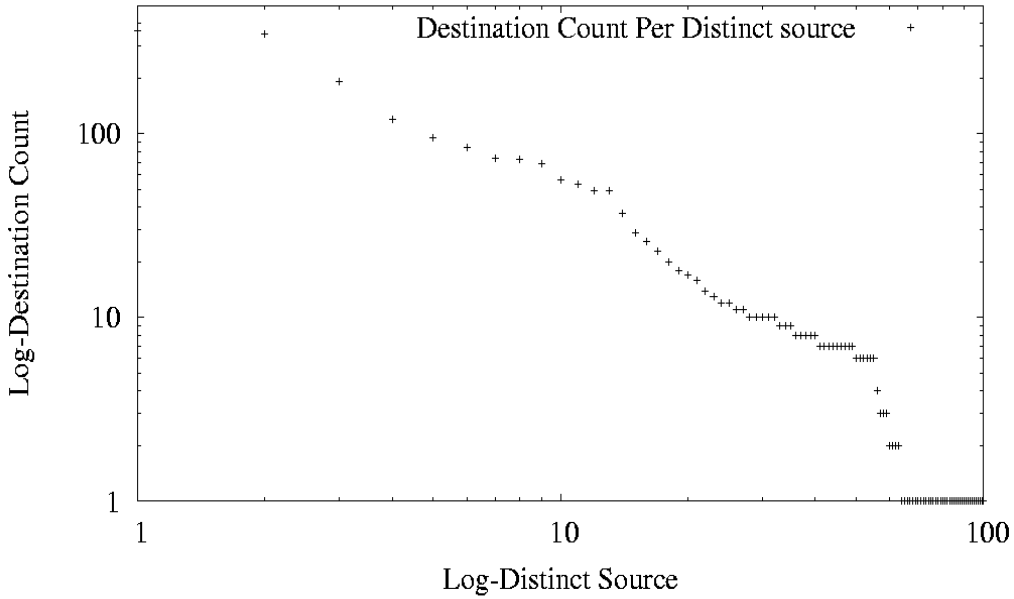
- Packet Loss
  - 1sec scale
  - Over 30mins





Losses are highly correlated

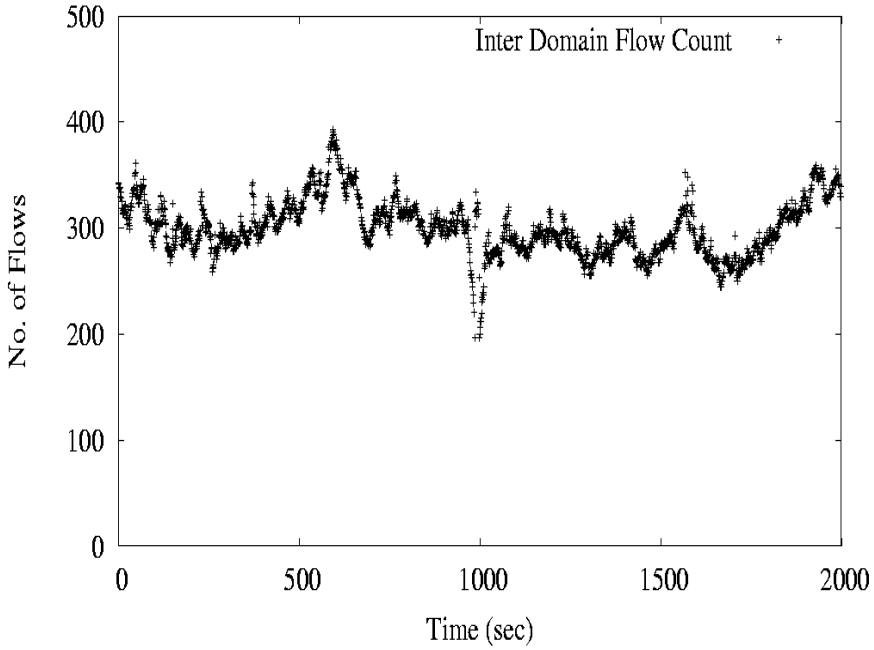
Flow Analysis - Distinct Destinations

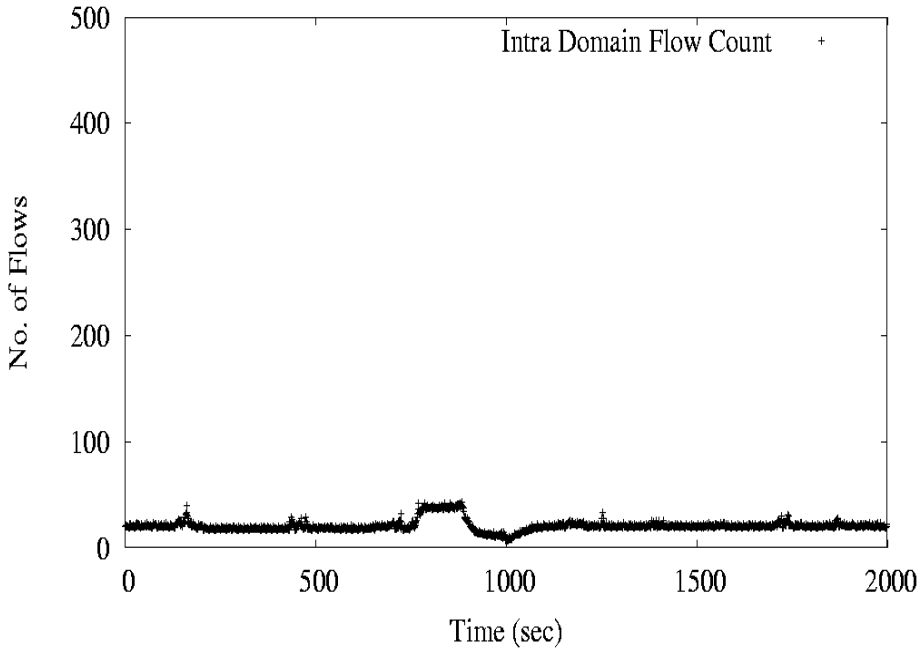


- 4 Tuple-based TCP Flow (Src/Dst IP Address, Src/Dst Port)
- Max number of distinct destinations
  - Loss period: 492
  - No loss period: 460
- Number of distinct sources are 63
- No IP spoofing

Flow Analysis - Flow Count

- More number of flows during loss period

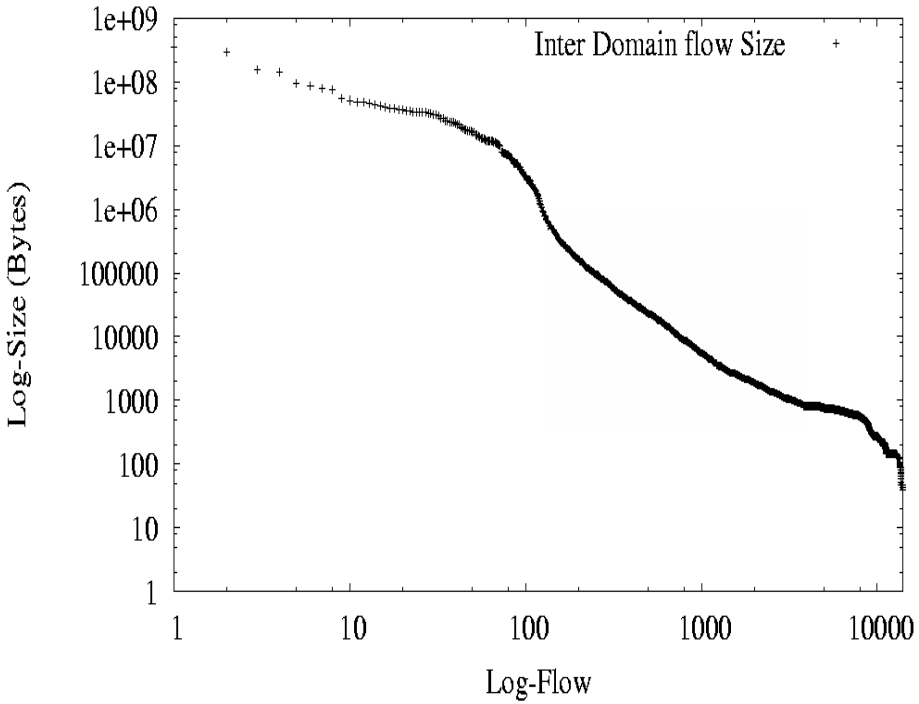


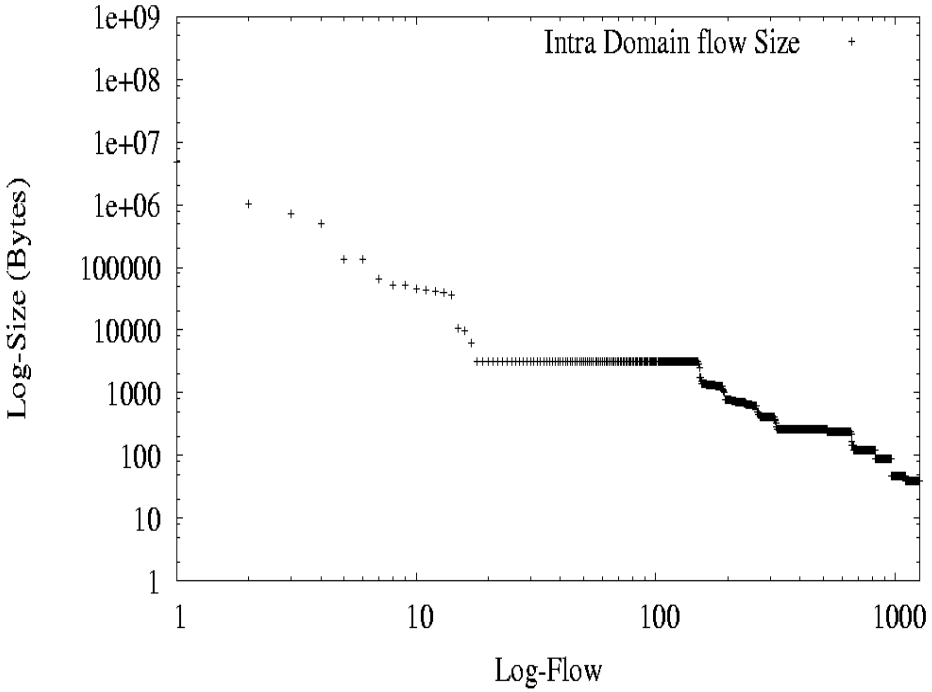


Packet Loss	Mean	Max	Min	Standard deviation
Heavy	300.11	393	197	26.277
Rare	240.490	316	111	26.669

Flow Analysis – Flow Size

- Pr [x = a] ~= c x^ {-alpha}

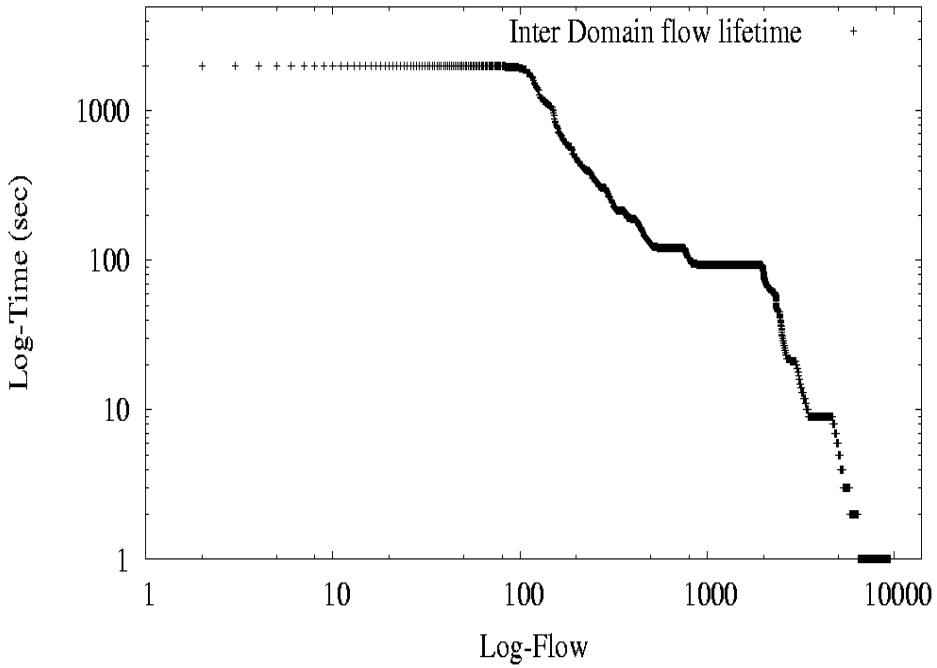


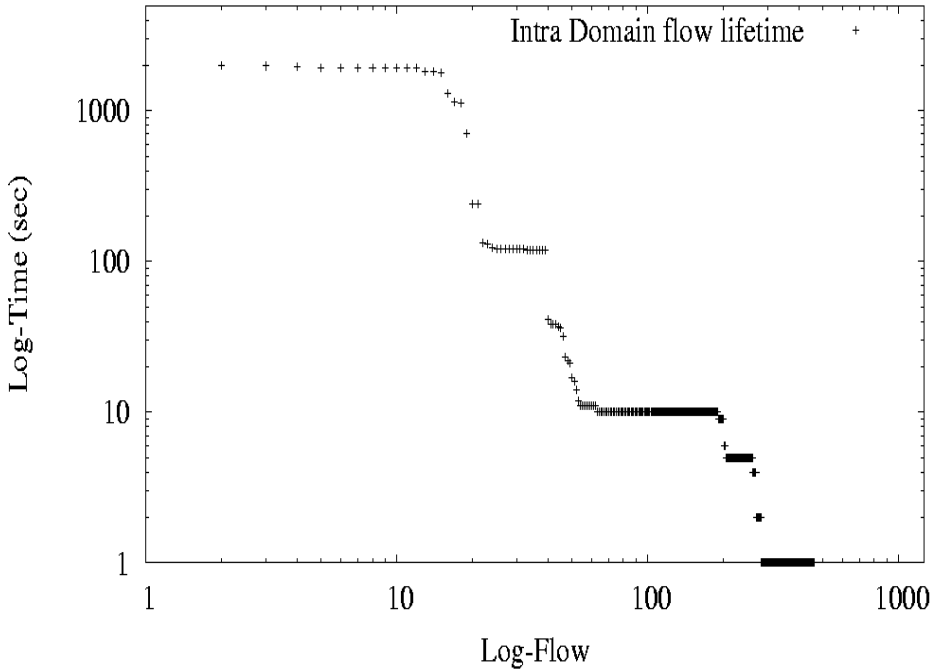


Packet Loss	Mean	Min (Bytes)	Max	Standard deviation
Heavy	0.24	40	436.61	6.06
Rare	0.233	40	241.228	4.583

Flow Analysis – Flow Lifetime

- Flows are longer during loss period

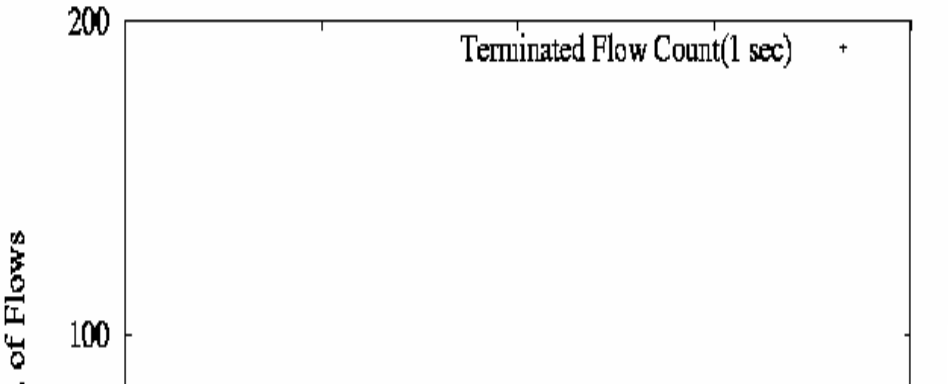


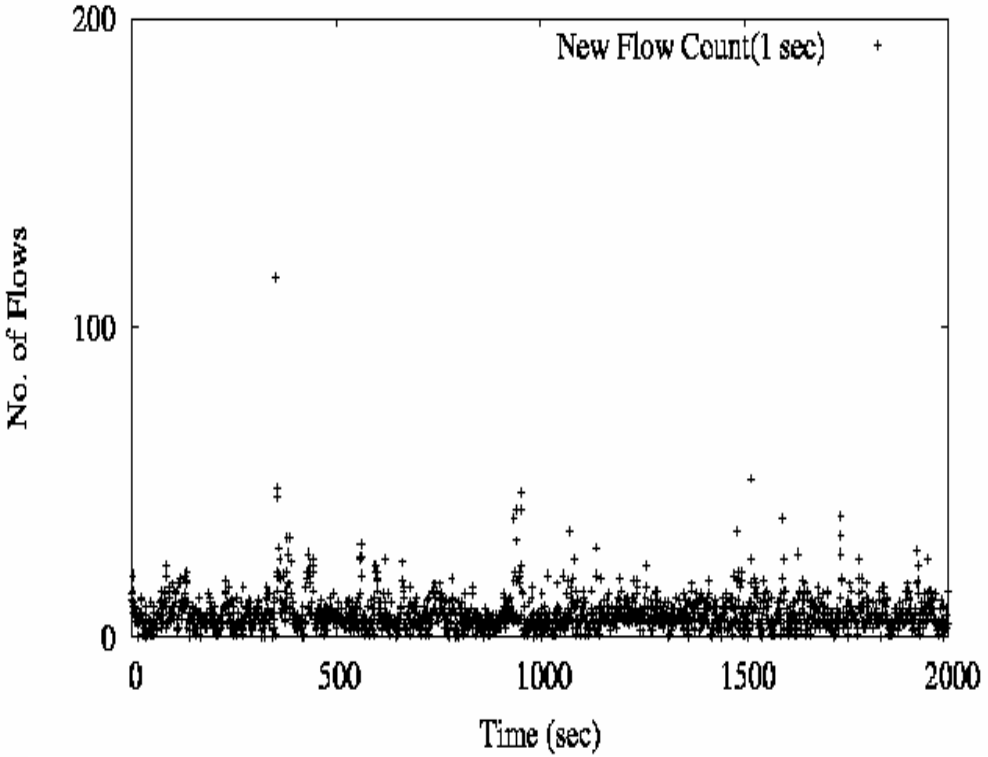


Loss	Mean	Max	Min	Standard deviation
Heavy	42.25034	2000	0	196.6926
Rare	36.51392	2000	0	177.6445

Flow Analysis – New &Terminated Flows

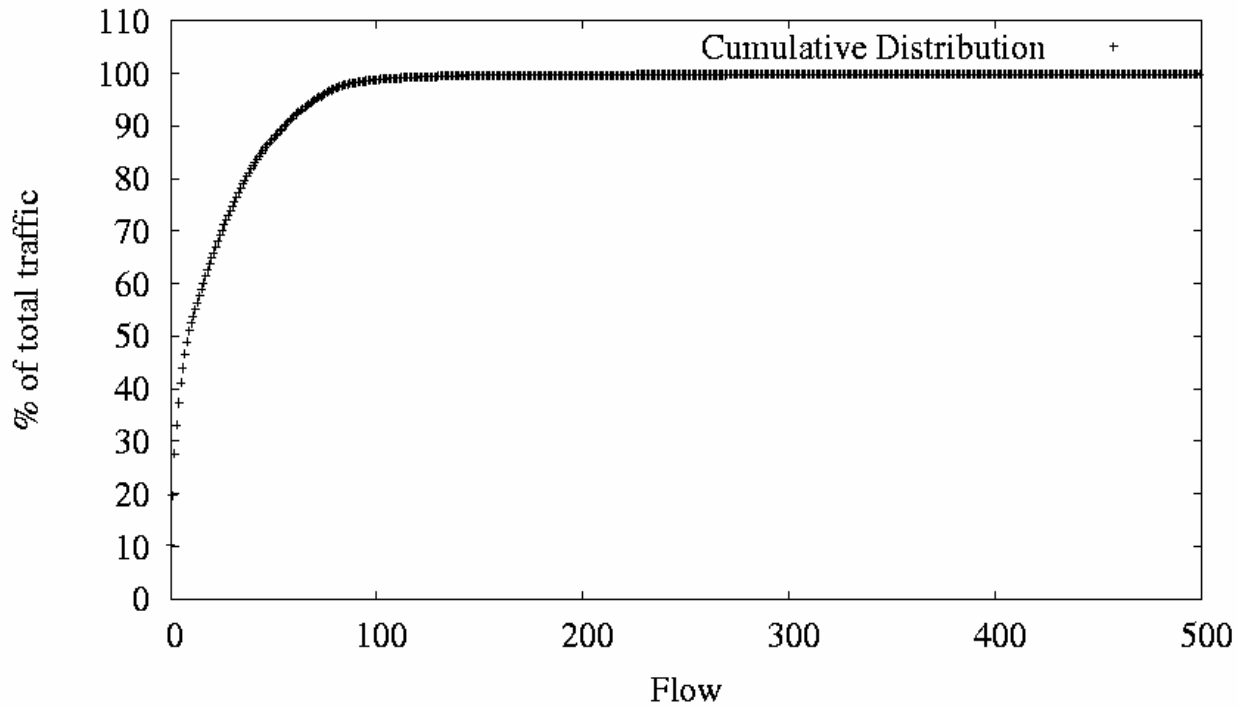
Number of flows initiated and terminated every second are comparable





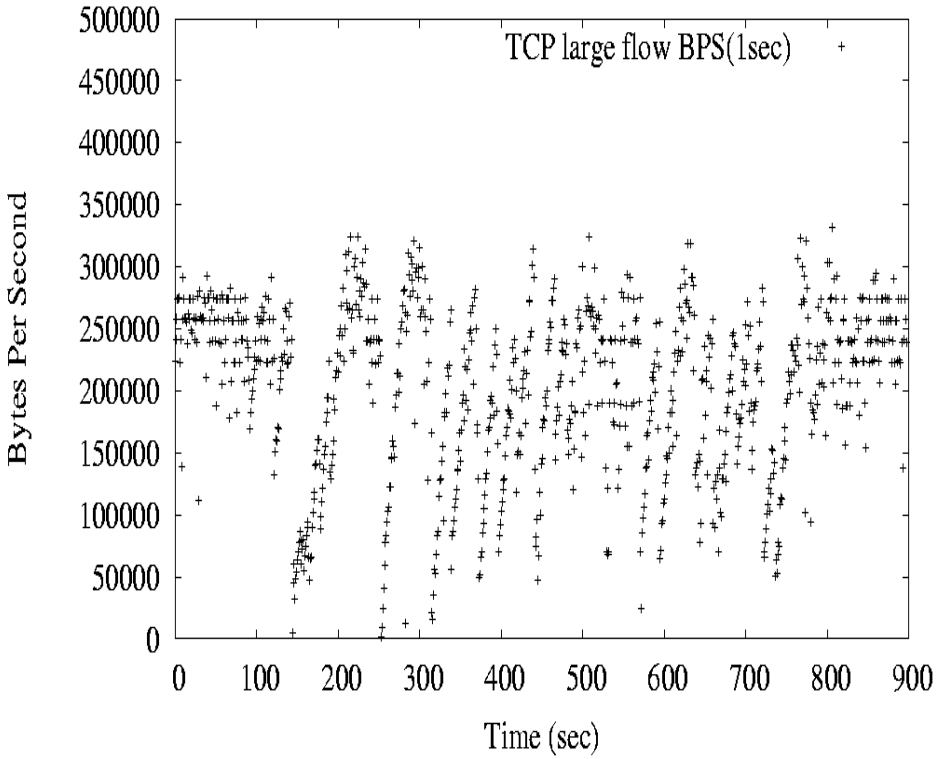
	Mean	Max	Min	Standard deviation
Loss - New Flow	7.660	116	0	6.039
Loss- Terminated Flow	7.660	73	0	5.624
New flow	7.081	83	0	5.753
Terminated Flow	7.081	63	0	5.733

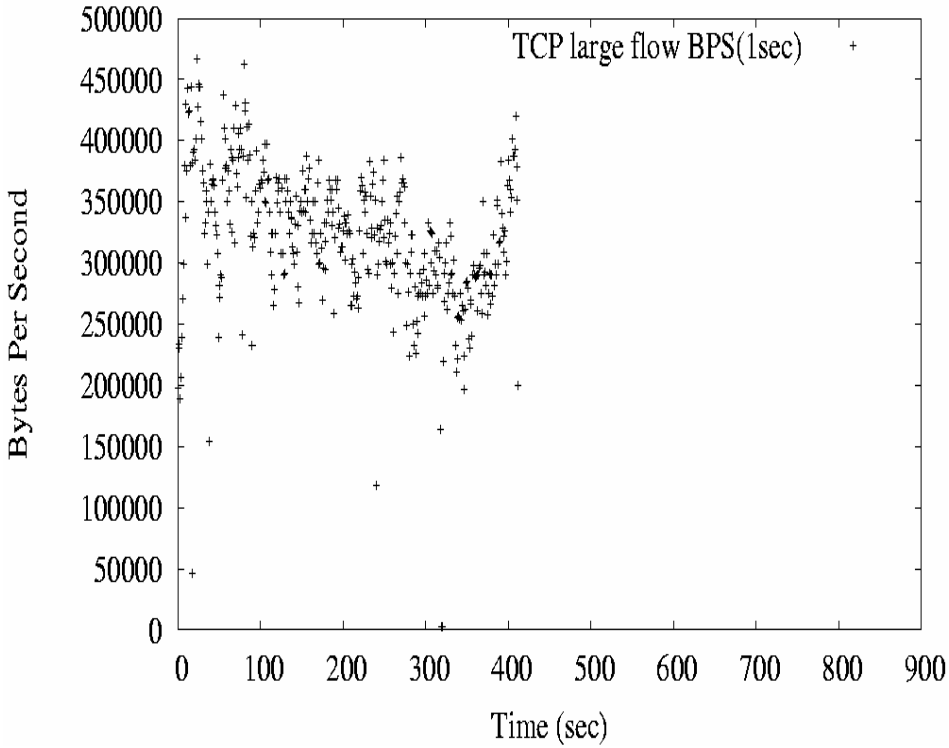
Flow Analysis - Large TCP Flows



- Sum of top 50 flows size: 83% of total traffic

Flow Analysis - Large TCP Flows
Throughput

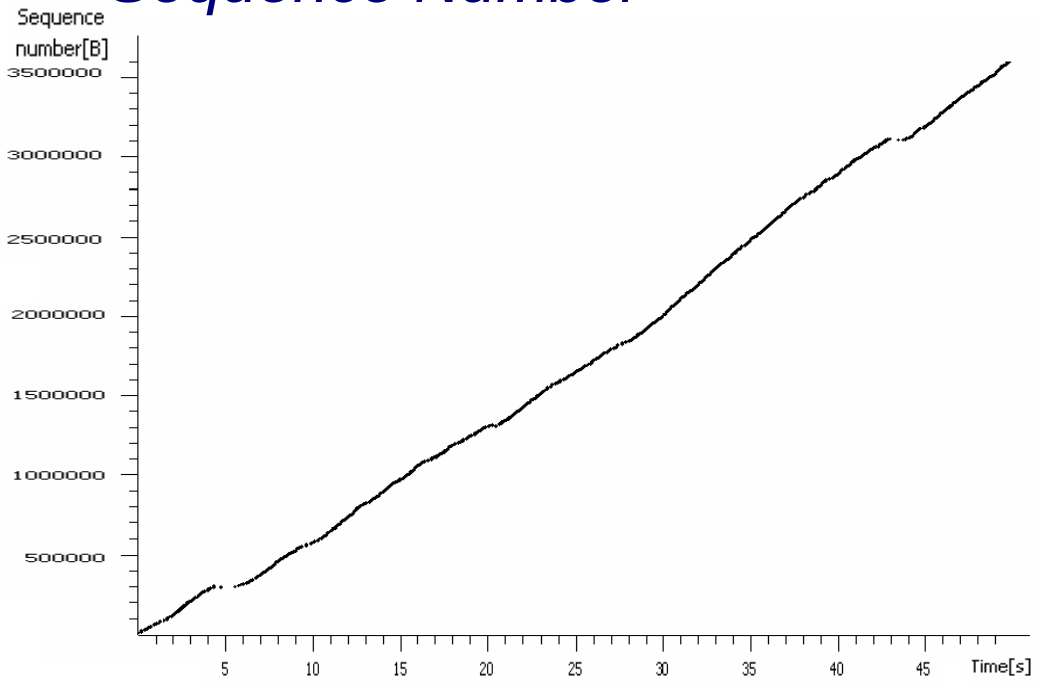


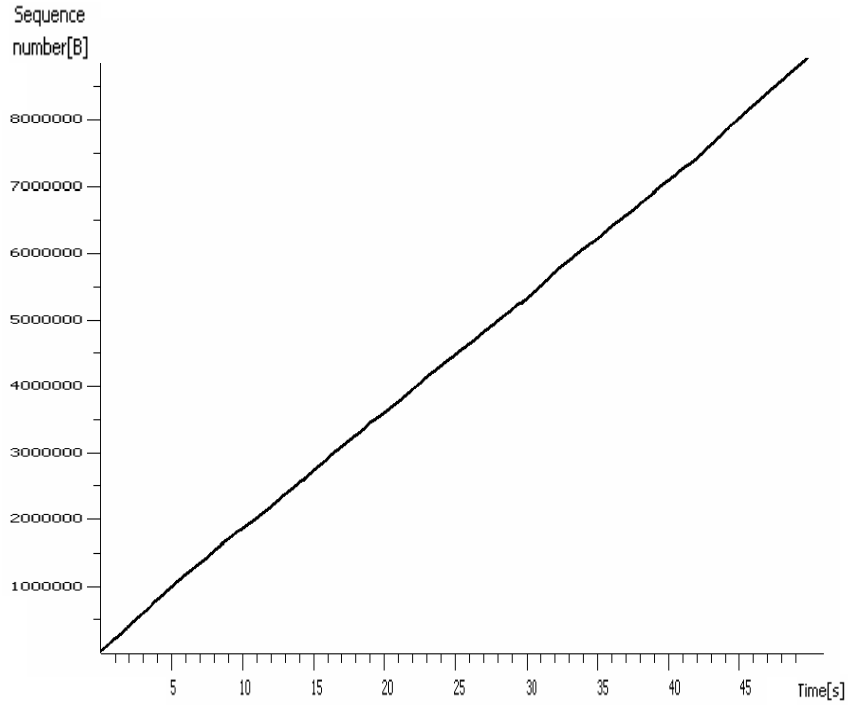


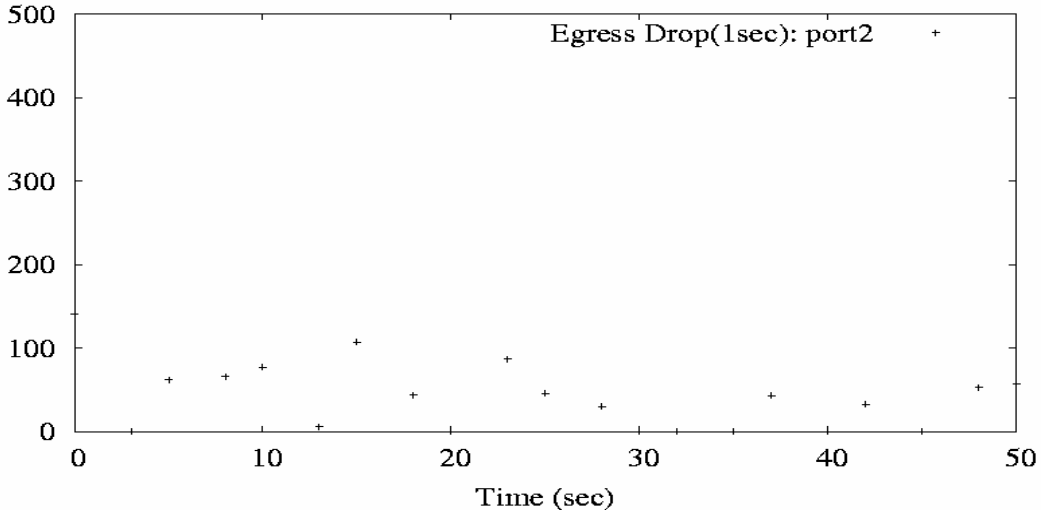
- Flow sizes: 179Mbytes and 140Mbytes

Flow Analysis - *Large TCP Flows*

Sequence Number







- SNMP Loss Rate: 40 packets/second
- Flow Loss Rate: 37 packets/second

Conclusion

- Study traffic and packet Loss characteristics
  - To determine root cause
- Cause Analysis
  - Collected data from a underutilized link (2%)
  - Defined a complete methodology
  - Developed tools to execute methodology
  - Analyzed data using our tools
- Results
  - TCP protocol is present in highest percentage
  - No malicious or spurious traffic is present in our link
  - Broadcast packets do not affect packet loss
  - Losses are strongly correlated
  - Number of flows are higher during loss period
  - TCP large flows are suspected as one of the possible reasons
    - Complicated to verify due to SNMP inaccuracies
- Contribution
  - Developed a cause analysis method
  - Developed set of tools to execute the analysis

Future Work

- Detail study of TCP characterization by monitoring and analyzing both ingress/egress directions and backbone link traffic
- Collecting data sets from various networks including IPv6
- Studying packet loss characteristics at core switch or router
- Checking if losses occur only on the links that convey large TCP flows
- If large TCP flows are responsible for losses
  - Need to determine remedy to avoid these losses

Questions?