Analyzer

sehee@postech.ac.kr

DPNM, POSTECH

-

-

-

-

-

INTERNET → Router → mirroring → Hub → Probe → Analyzer → Presenter

Binary Log File

NAS
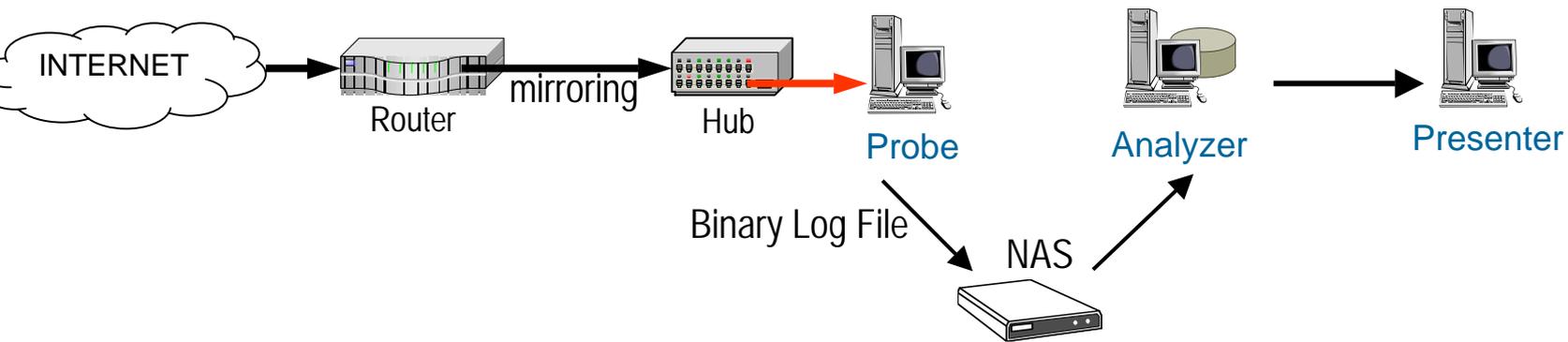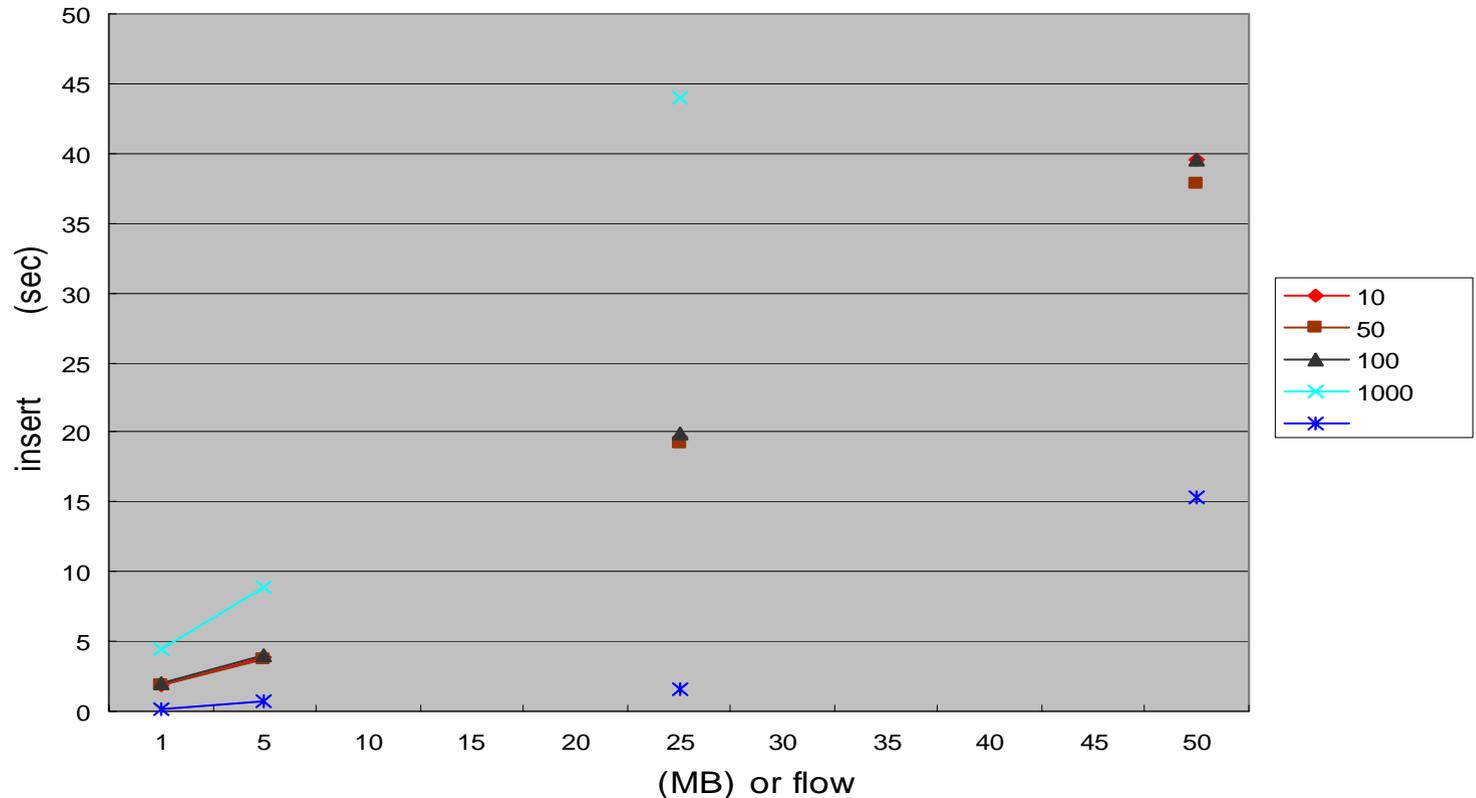
- **Simple Analyzer**
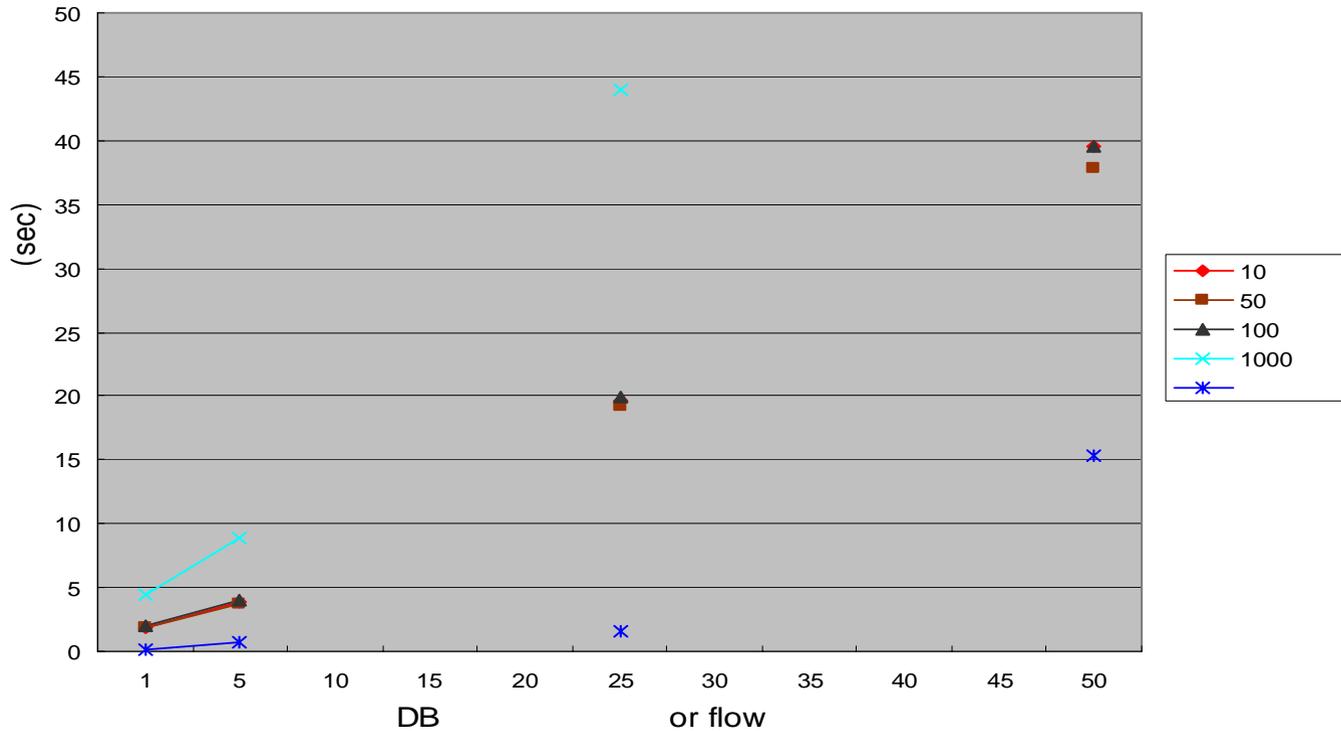 - 1
  - Hashing Flow
    DB insert
    - ✓ 100 Mbps 1 :
      30Mbytes ( )
  - insert
  - Presenter

Insert time of Simple Analyzer

- insert & query

  exponential increase graph (   )

Query response time

- DB insert

    →   DB insert

-

    → pre-analysis (separated tables), cache scheme

- capture all, store all

- (30MB)+
  (MB) +
  (MB) +   (MB)
  →

  → Top N Scheme, Time sliding window

- Analyzer read operation Flow Store write operation

flow messages

Flow Store #1

Flow Store #2

Flow Store #3

Write operations

Read operations

Database
Query / Response

Traffic Analyzer

t 1   t 2   t 3

Postech
DP&NM Lab
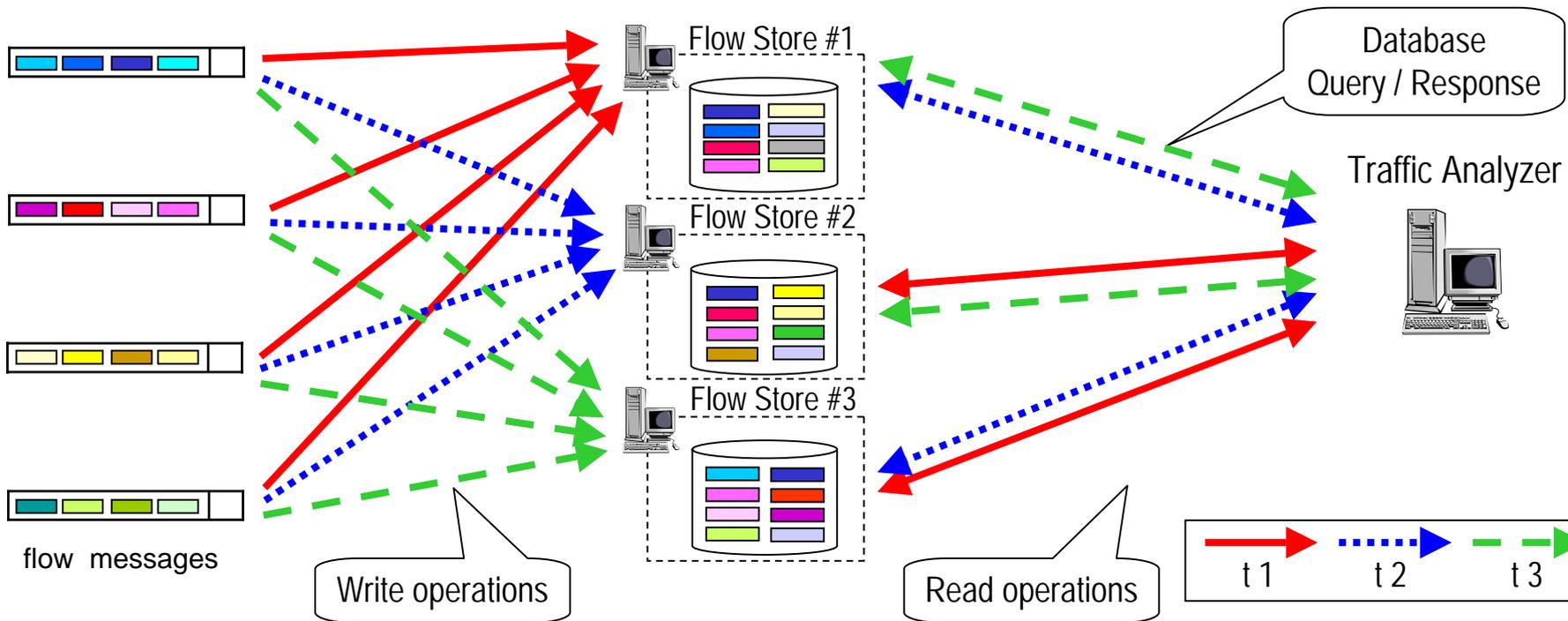
Table

- analysis task
  insert time, query response time   , Simple Analyzer

  –   packet trace,   data

Time Sliding Window

- NG-MON

  –

Top N Scheme

- N
  ex) 1   packet   top N
                                         top N   1

        top N

     -

     - packet count   bytes

- N

More …

Schedule

	November				December		
	11	18	25	30	2	9	13
Webtrafmon II		▮					
Top N Scheme :			▮				
N							
NG-MON Simple Analyzer			▮				
		▮▮▮▮▮					
					▮▮▮▮▮		
				▮			
Defense							▮