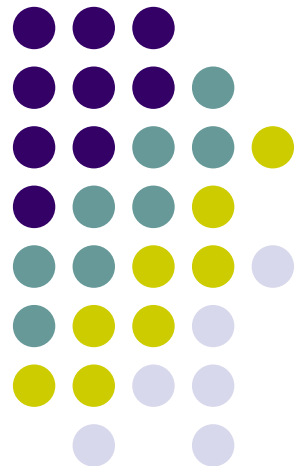
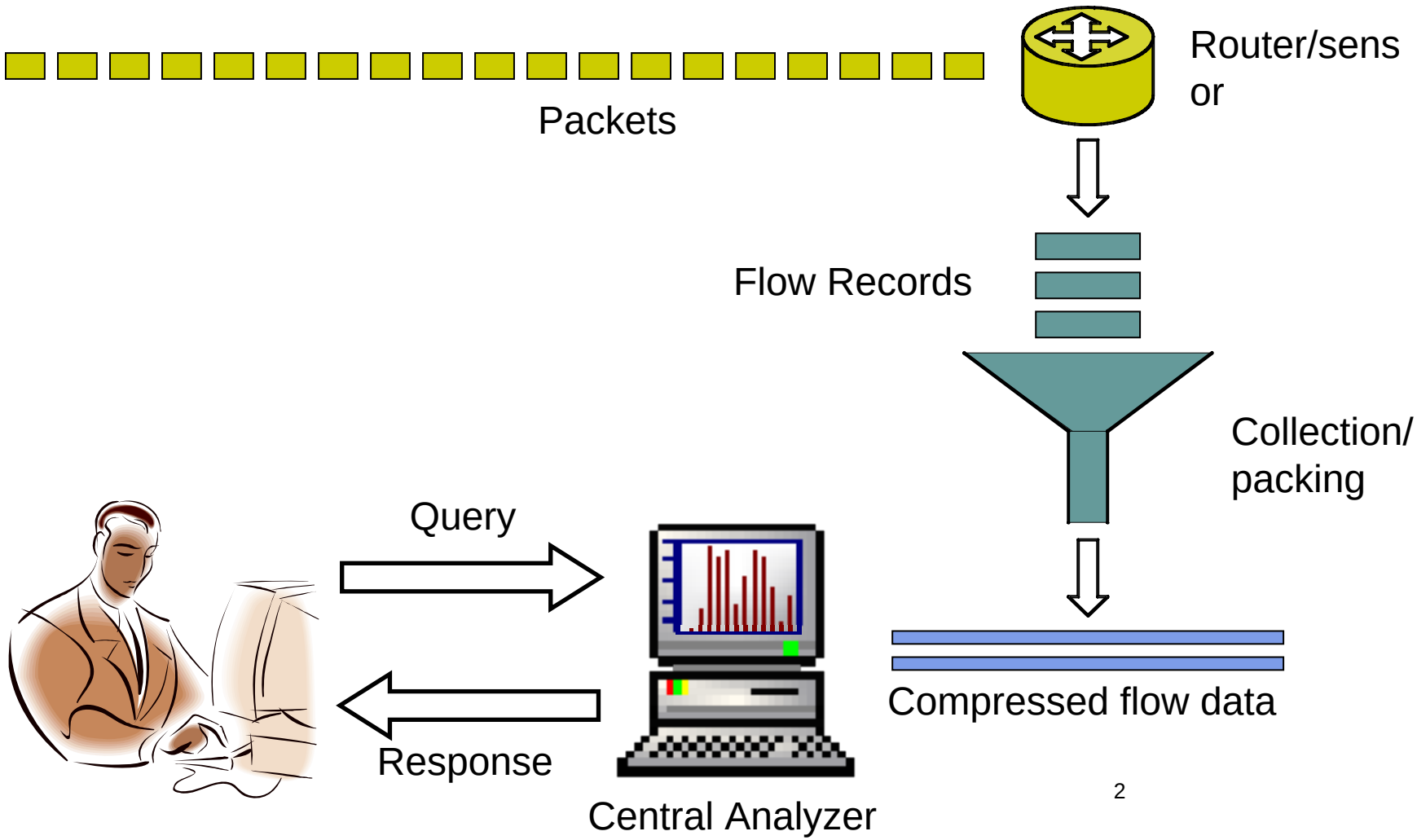
Scalable Flow Analysis

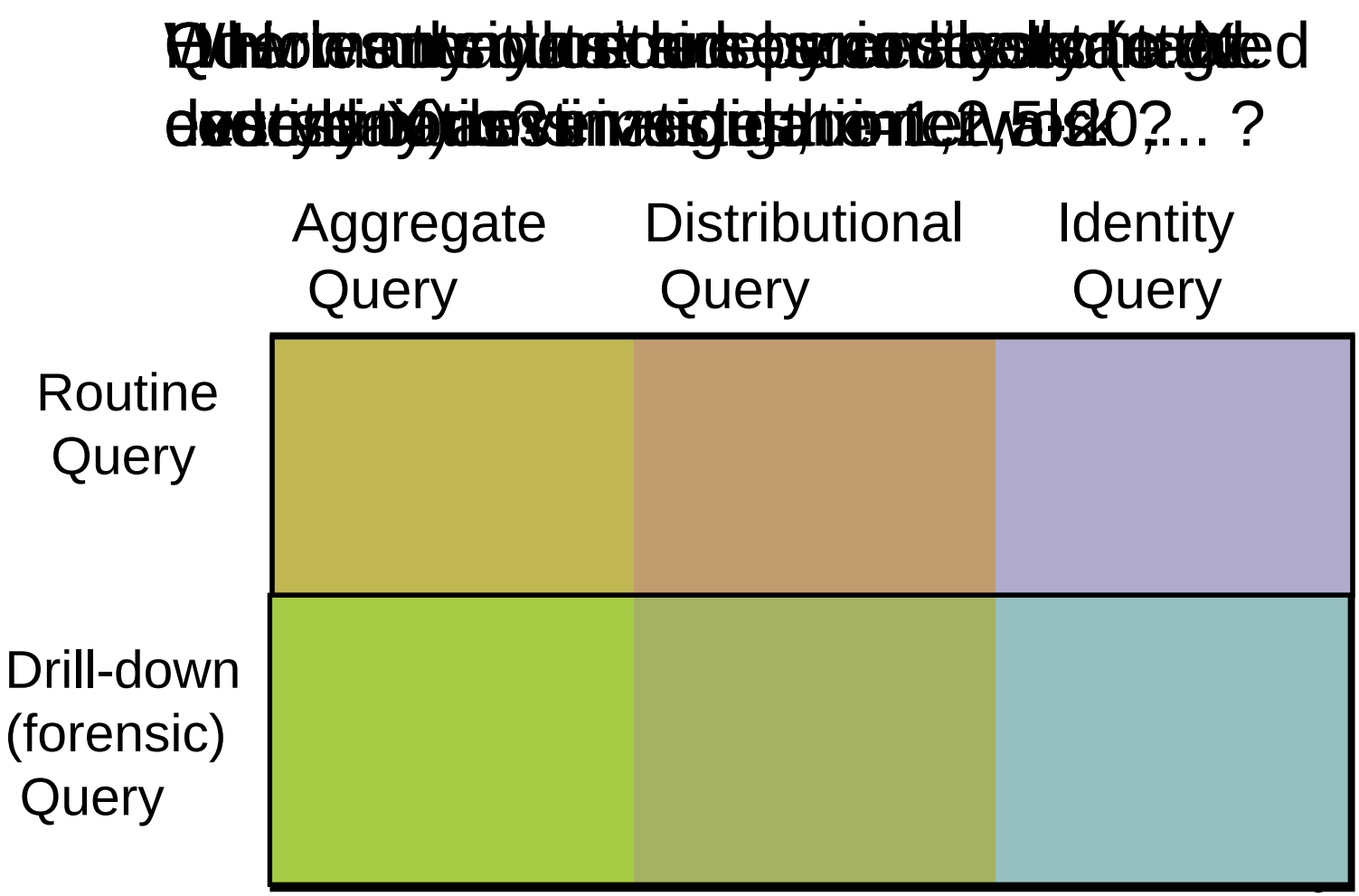
Abhishek Kumar
Sapan Bhatia
Georgia Tech



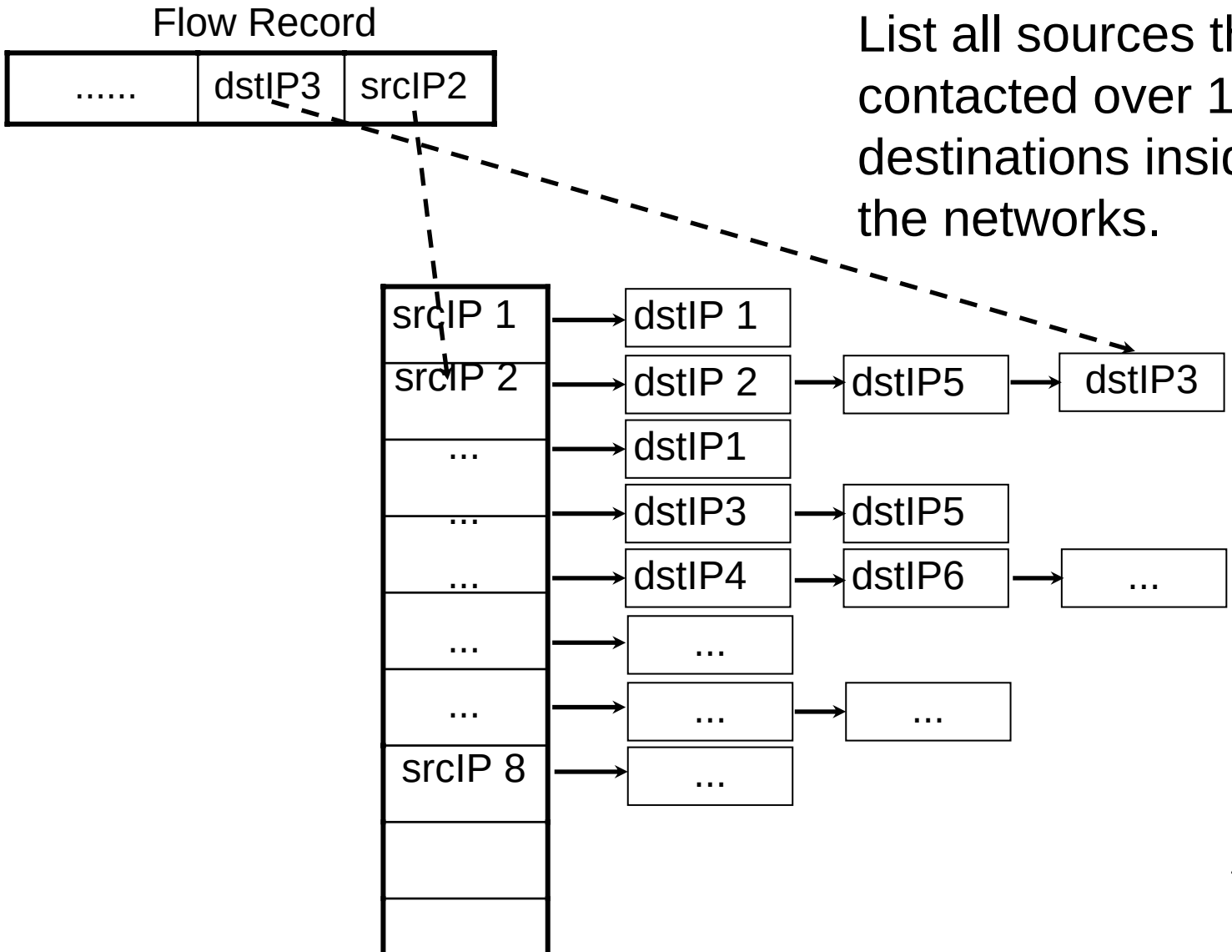
Flow Collection and Analysis Architecture



An informal Taxonomy

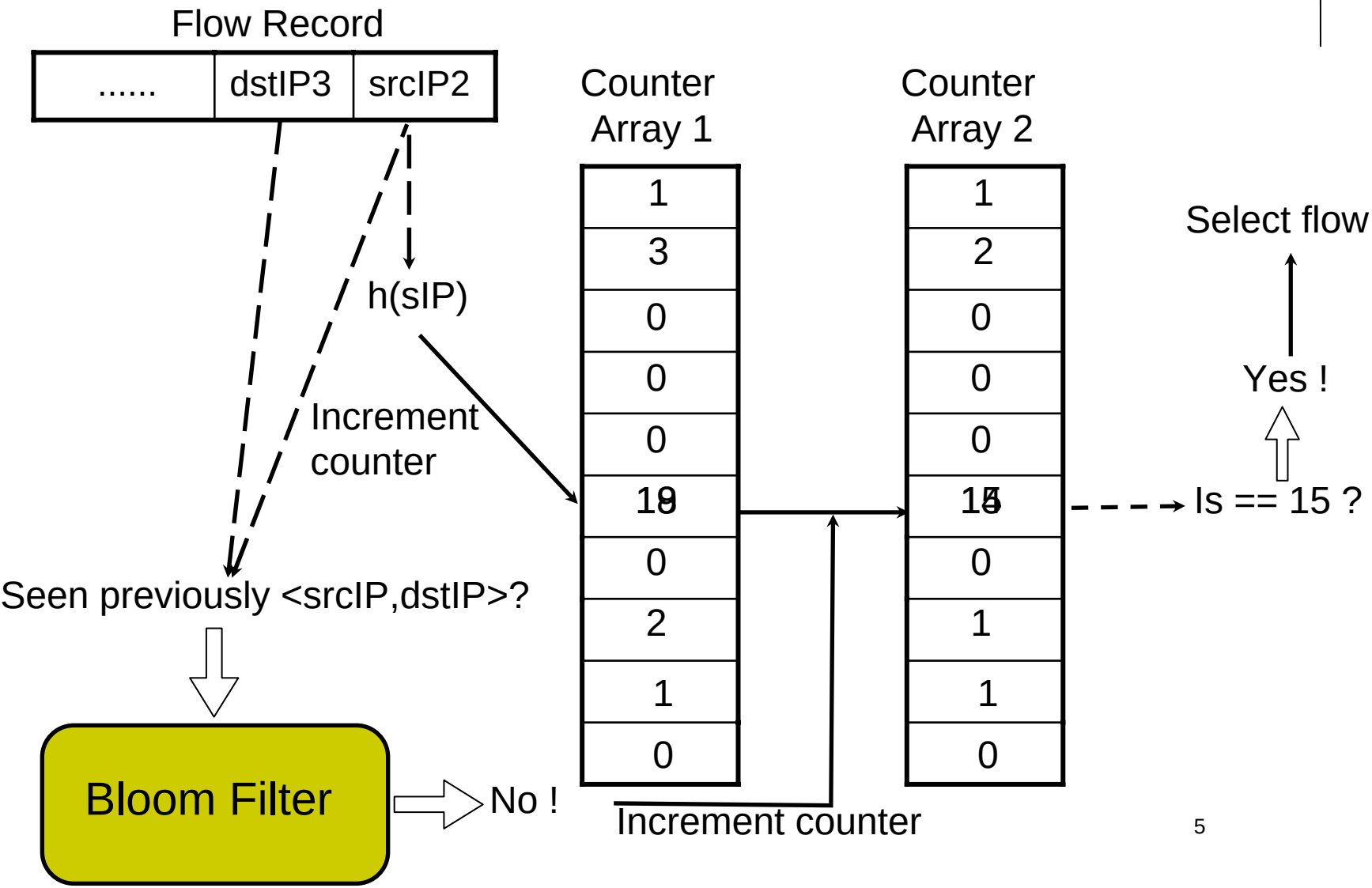


An example query

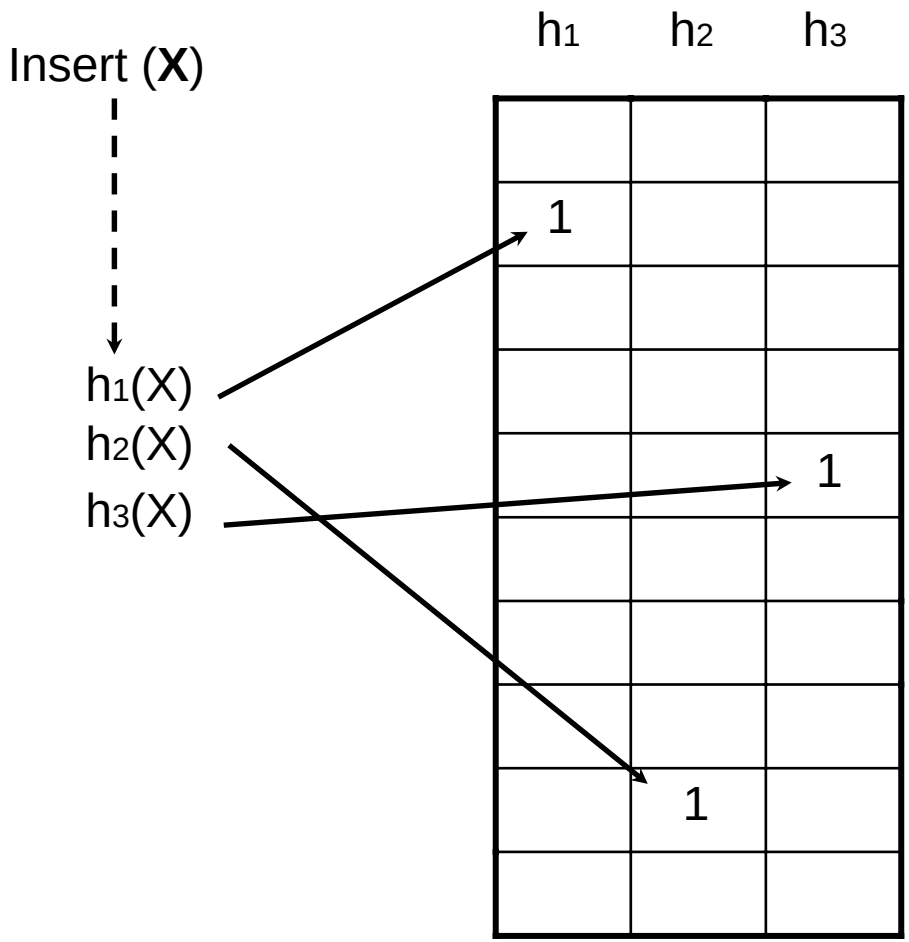


List all sources that contacted over 15 destinations inside the networks.

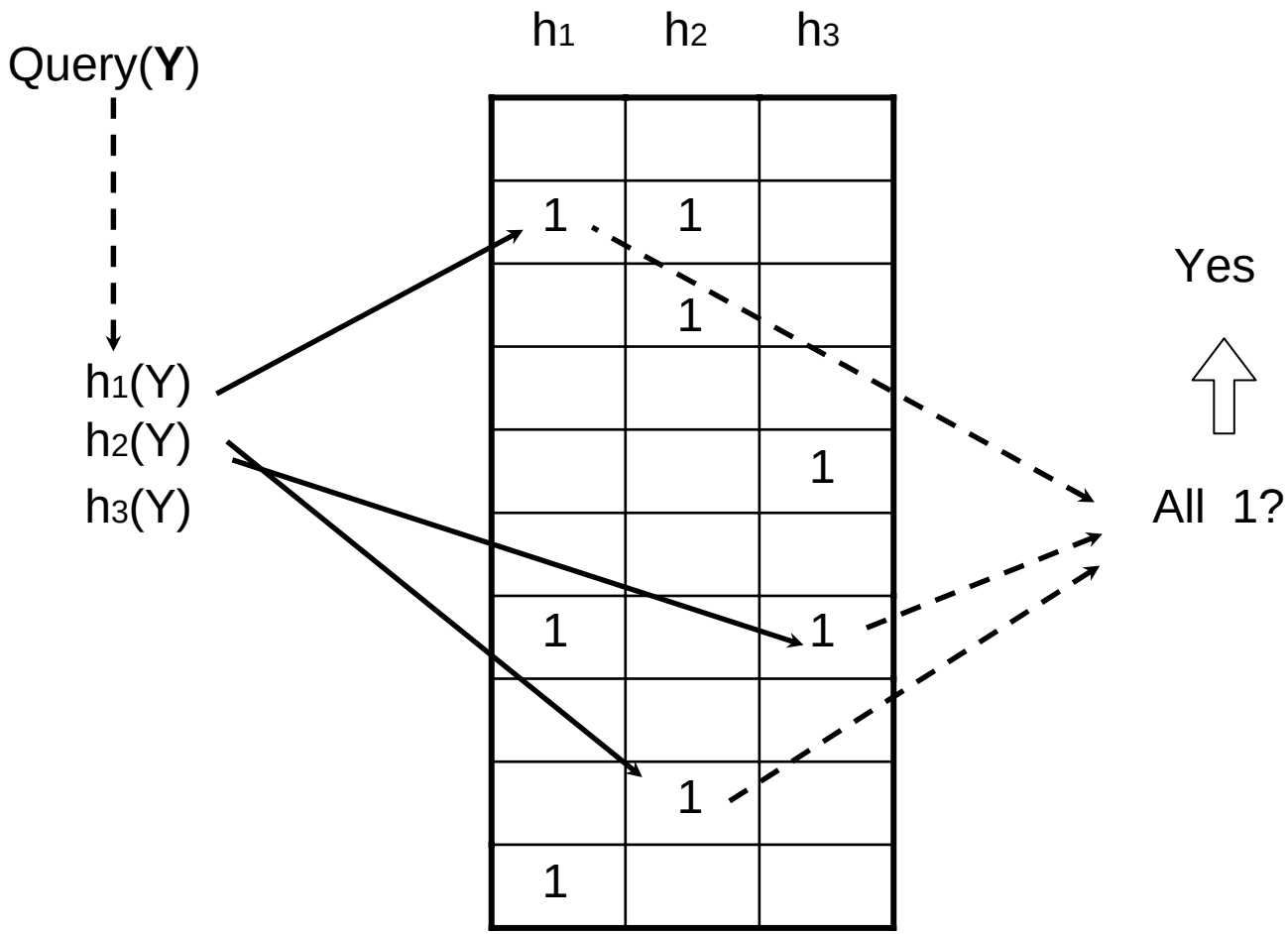
Proposed Solution (Preprocessing)



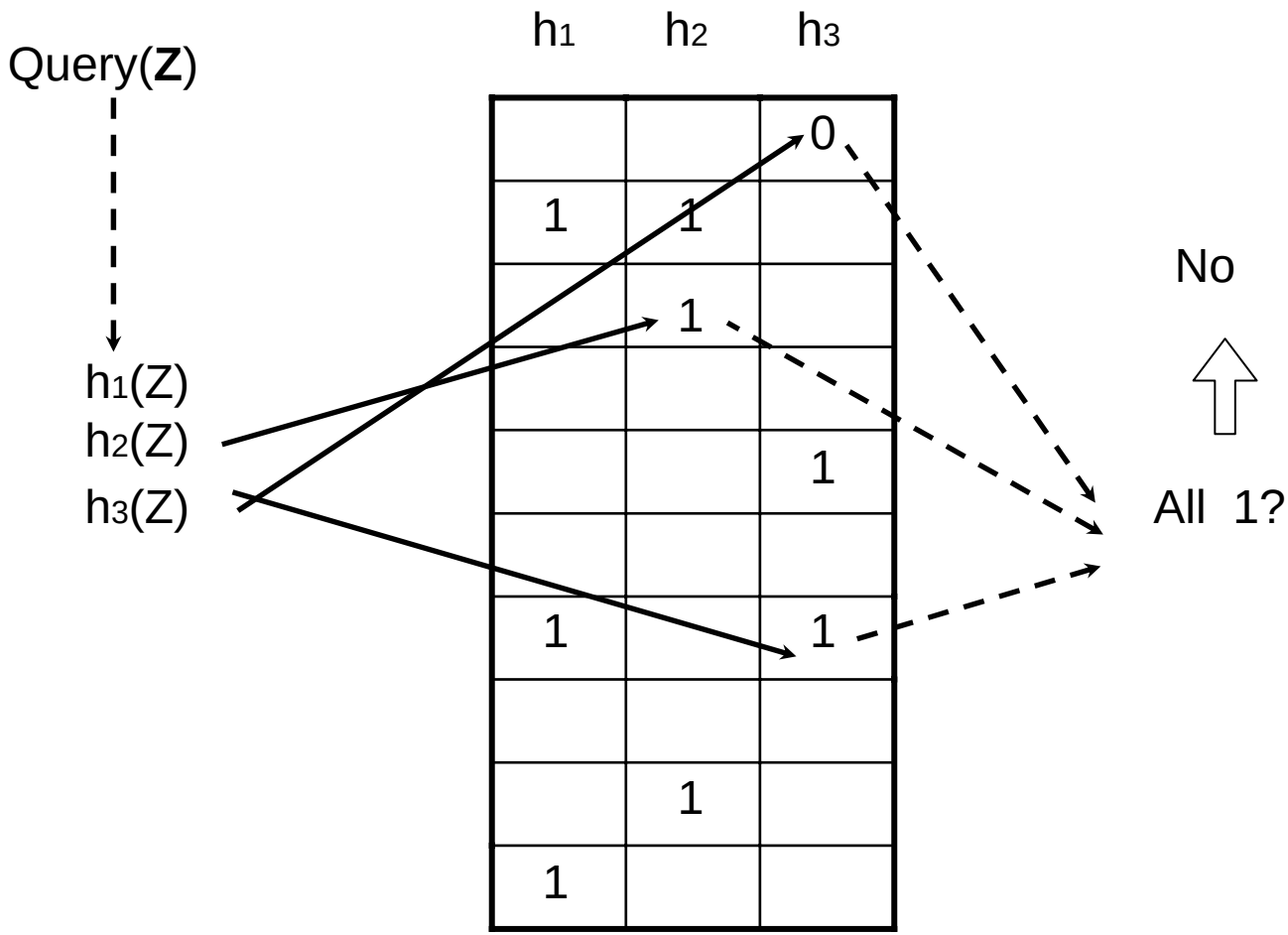
Bloom filter (insert)



Bloom filter (query)



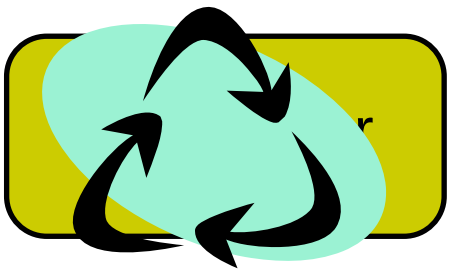
Bloom filter (query)



Proposed Solution (State after preprocessing)

Flow Records

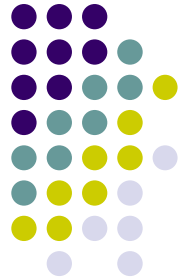
.....	dstIP3	srcIP2
.....	dstIP7	srcIP9

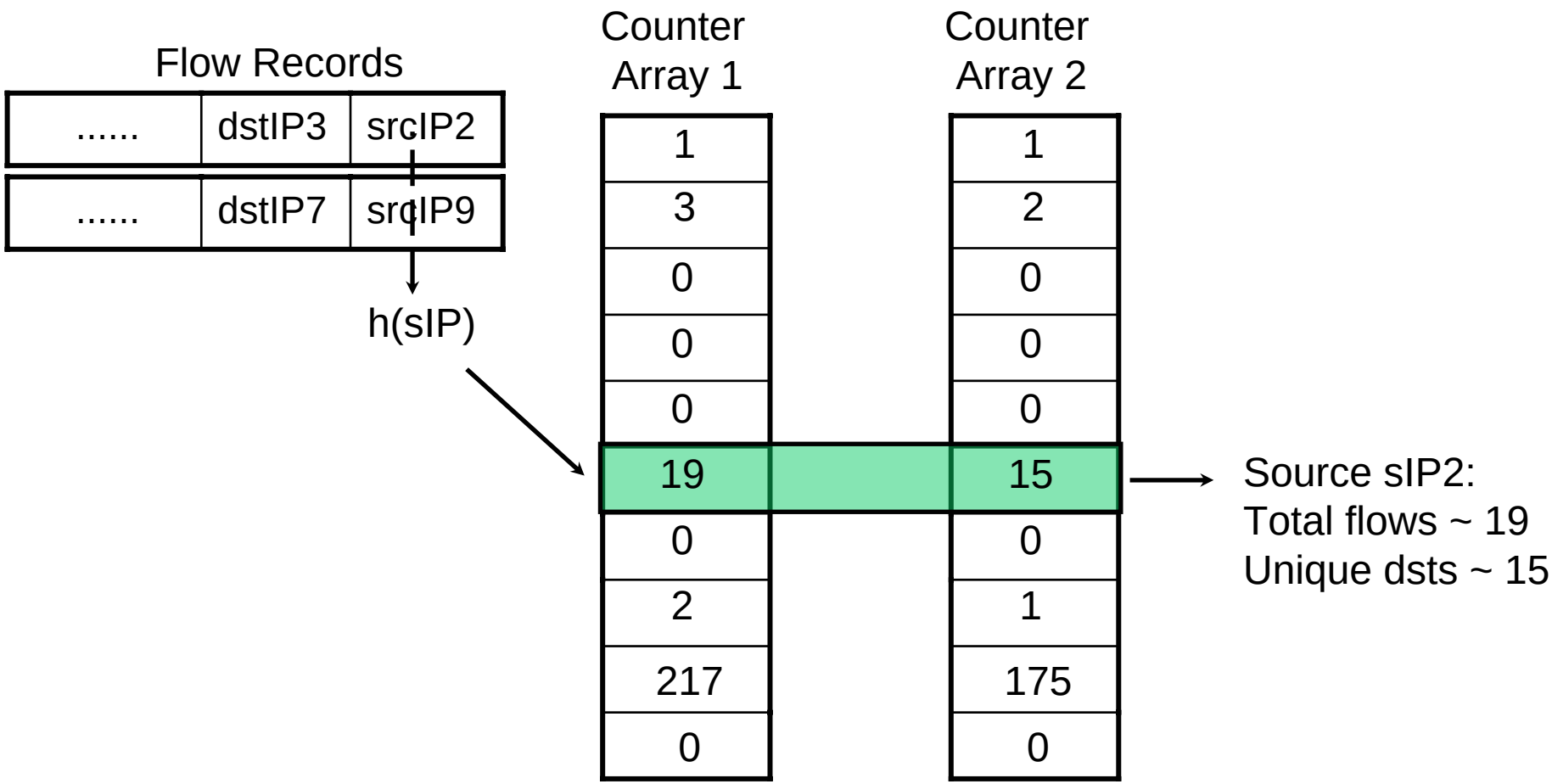


Counter Array 1
1
3
0
0
0
19
0
2
217
0

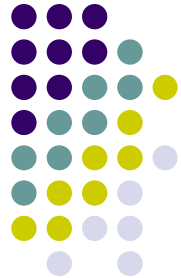
Counter Array 2
1
2
0
0
0
15
0
1
175
0

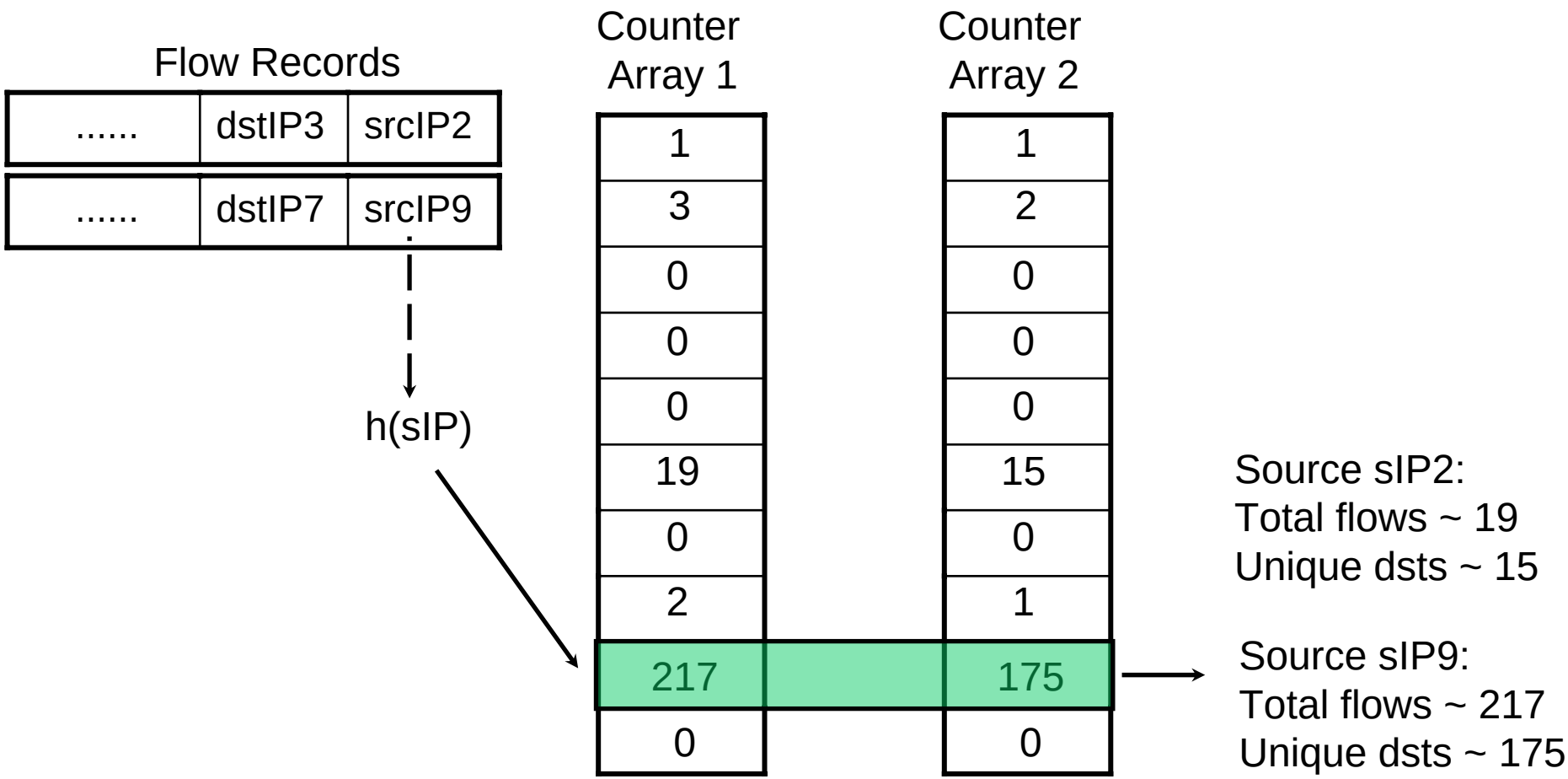
Proposed Solution (Query processing)



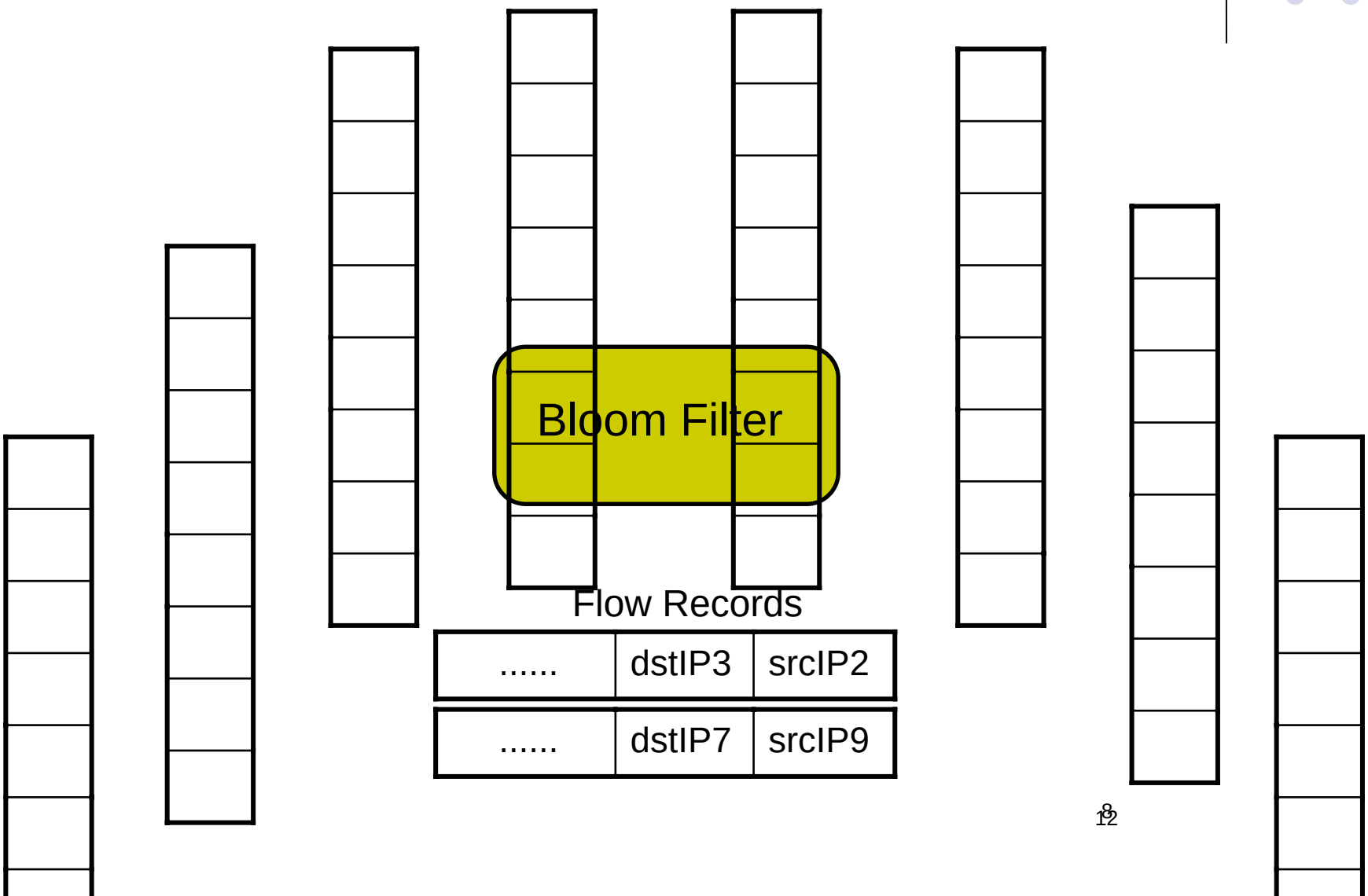


Proposed Solution (Query processing)

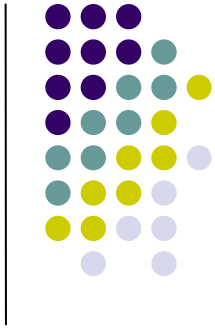




Can we build a more comprehensive system ?

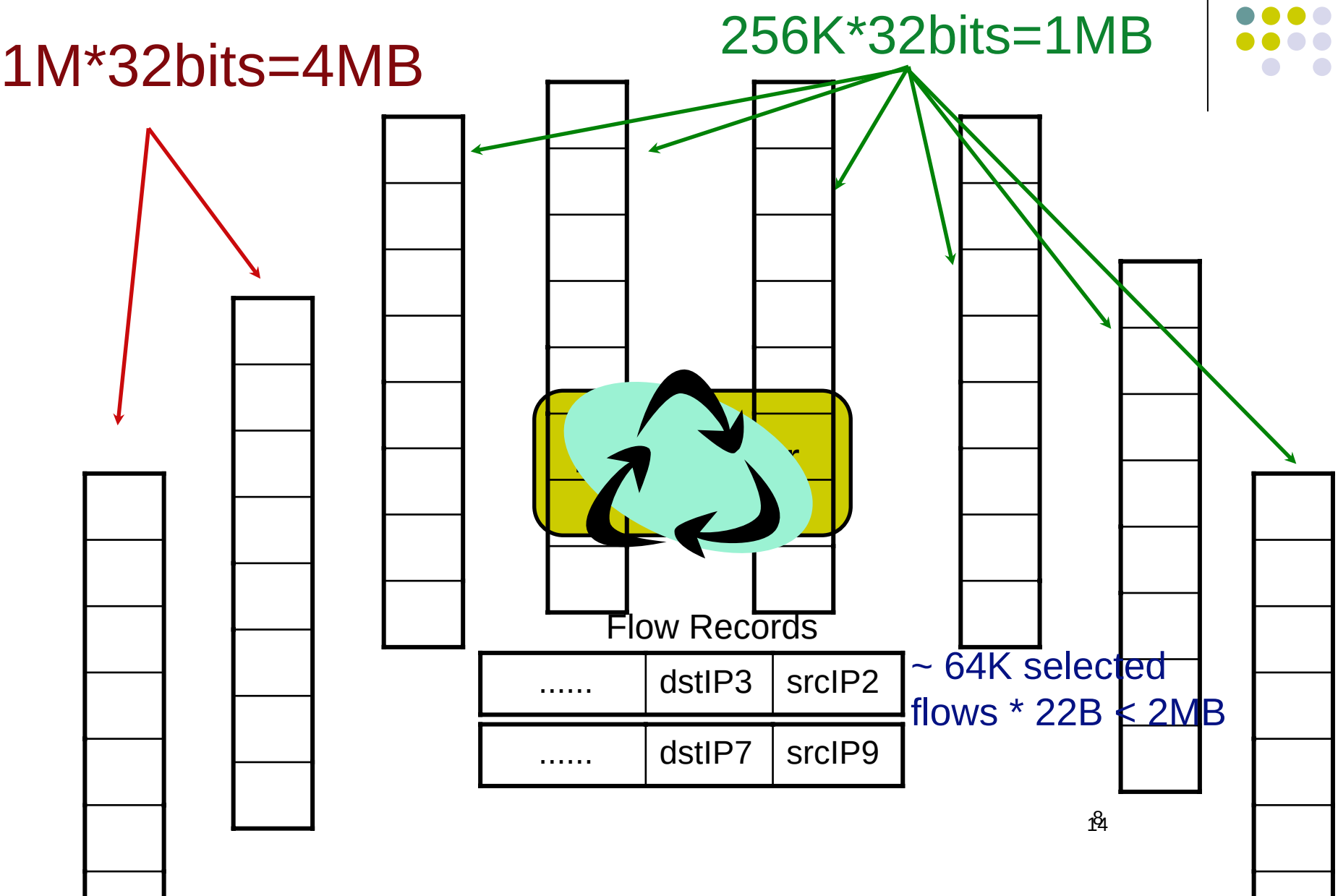


What will it track ?

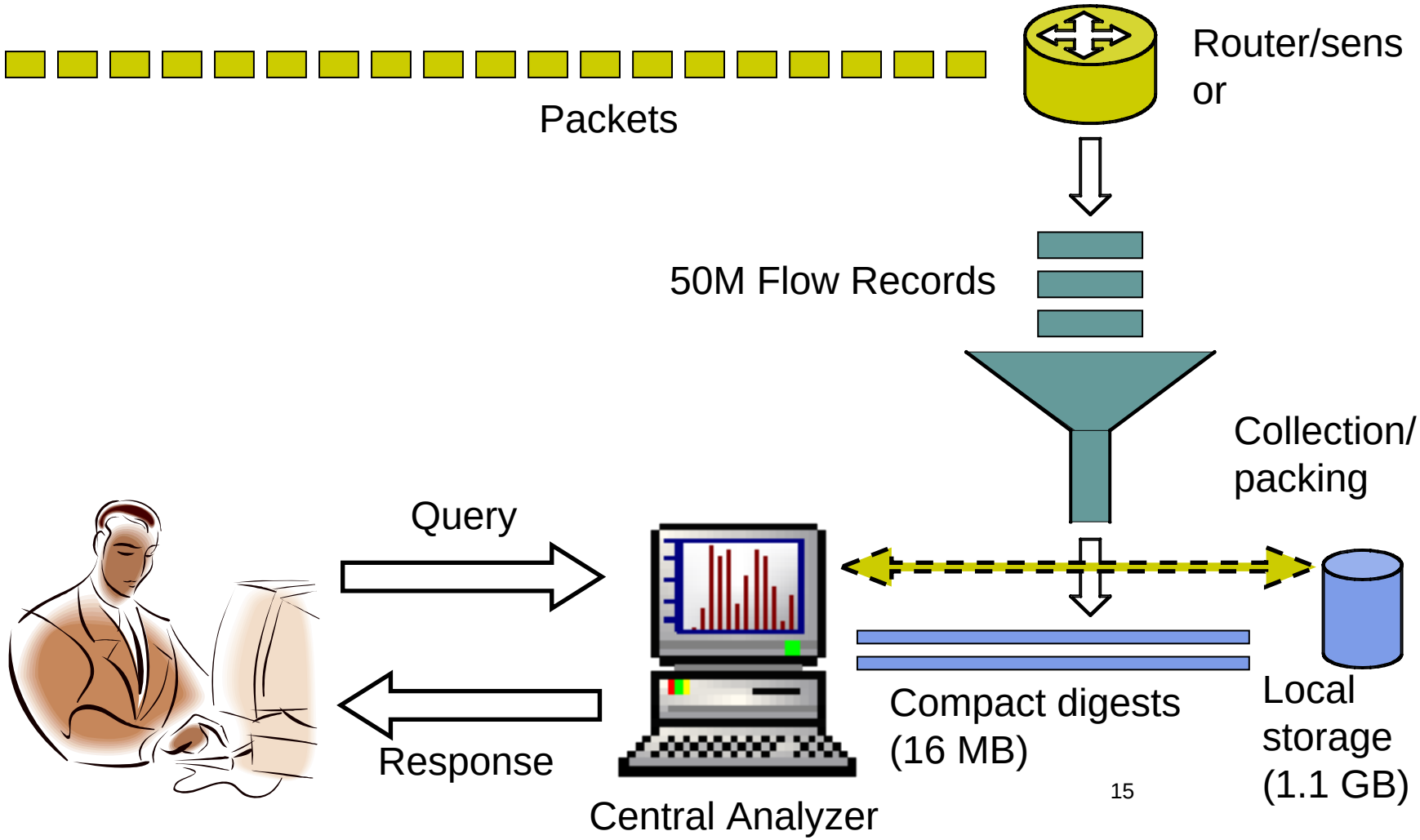


Metric	Key Field(s)	Aggregate Queries	Distributional queries	Idenity Queries
Bytes	5-tuple	Total Bytes, Flows	Flows with x<bytes<y	Large Flows
Packets	5-tuple	Total Pkts, Flows	Flows with x Pkts	Large flows by pkts
Total Flows	Source IP	Total sources	Sources sending x flows	Sources sending many flows (> Threshold)
Unique Destinations	Source IP	Total sources	Sources contacting x destinations	Sources contacting many destinations
Total Flows	Dest IP	Total Destinations	Destinations receiving x flows	Destinations receiving many flows
Unique Sources	Dest IP	Total Destinations	Destinations contacted by x sources	Destinations contacted by many sources
Total Flows	<dIP, dPort, proto>	Total 3-tuples	3-tuples receiving x flows	3-tuples receiving many flows
Unique Sources	<dIP, dPort, proto>	Total 3-tuples	3-tuples contacted by x sources	3-tuples contacted by many sources

flows?


1M*32bits=4MB
256K*32bits=1MB
Flow Records
..... dstIP3 srcIP2
..... dstIP7 srcIP9
~ 64K selected flows * 22B < 2MB

Flow Collection and Analysis Architecture



Thank you !

- Questions and comments
- Contact: akumar@cc.gatech.edu