Multicore Based Packet Splitting Approaches for High Speed Network Security

APAN 32nd Meeting
New Delhi
22 – 26 August 2011
C-DAC

Challenges In High Speed Packet Processing for Security

- Volume of network Traffic is High
- Current day attacks are more complex and network intensive in nature
- Packet prossing includes multiple subsystem
  - Network card driver
  - Capturing stack of the operating system
  - The monitoring application
- If any of these subsystems faces performance problems, it will affects the system performance

Bandwidth Vs Packet Processing Time

Bandwidth	Number of Packets	Per Packet Processing Time (Nano Seconds)
128 Kb	256	3906250
256 Kb	512	1953125
1 Mb	2048	488281
200 Mb	409600	2442
500 Mb	1024000	977
1 Gb	2097152	477
2 Gb	4194304	239
10 Gb	20971520	48

* Considered 64 Byte Packet for Calculation

Hardware - Approaches

- Since CPUs are designed for Generic purpose computation, specially designed Hardwares are used for high speed packet processing.

ASIC (Application Specific Integrated Circuit)

- Well-designed ASICs can be much faster than CPUs, but they are difficult and expensive to develop
- ASICs usually have limited programmability and must be redesigned as protocols and interfaces change

Network Processors

- Network processor tries to bridge the divide between ASICs and CPUs by providing a device that is as programmable as a CPU but as fast as an ASIC.

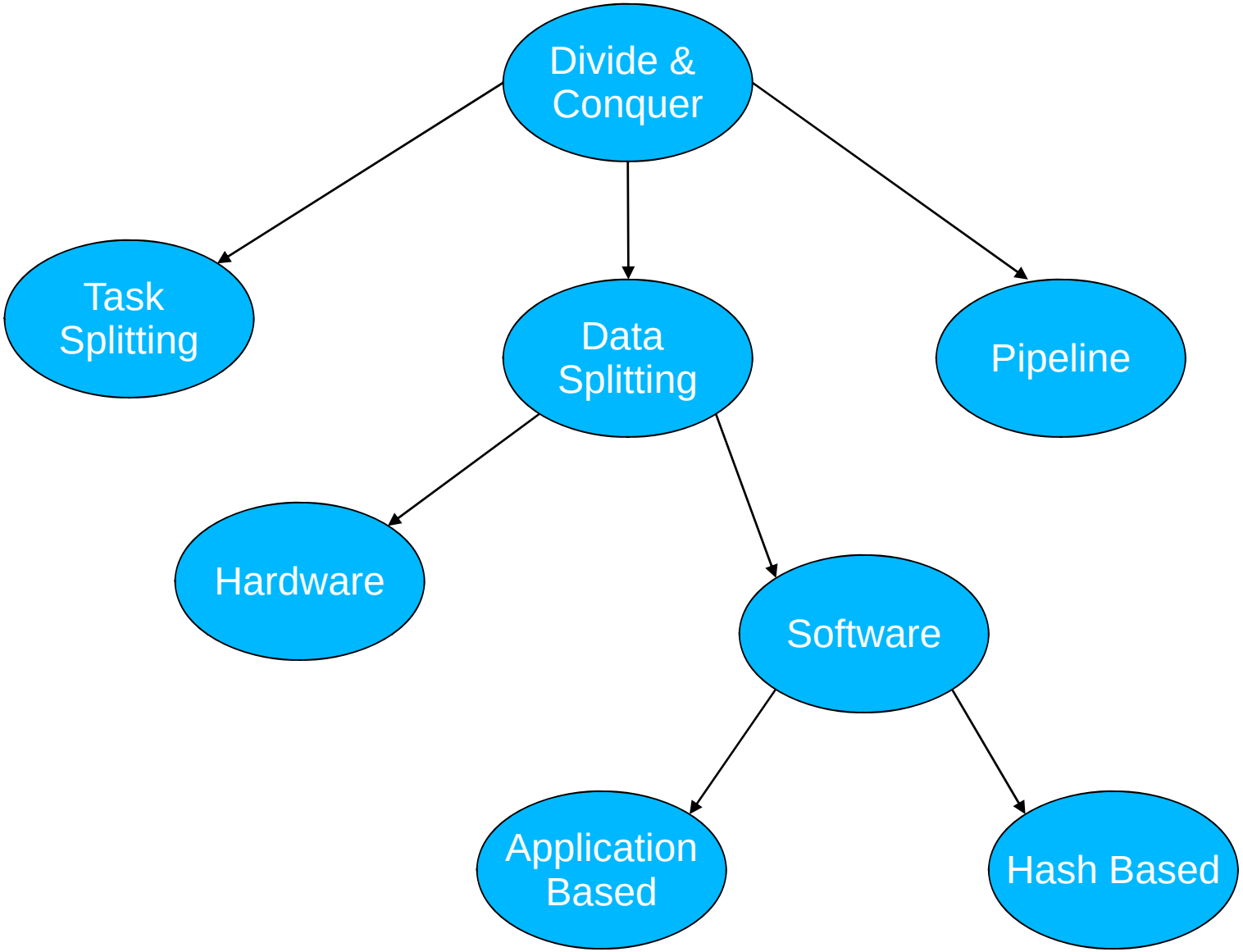
Software - Approaches

- Multi-Core Based Approach
- GPU Based Approach

Hyper Threading and Multi-core

- Hyper Threading (HT)
  - Single execution core is shared among multiple threads
  - When multiple threads are running, HT Technology interleaves the instructions in the execution pipeline
- Multi-core
  - Multi-core processors embed two or more independent execution cores into a single processor package.

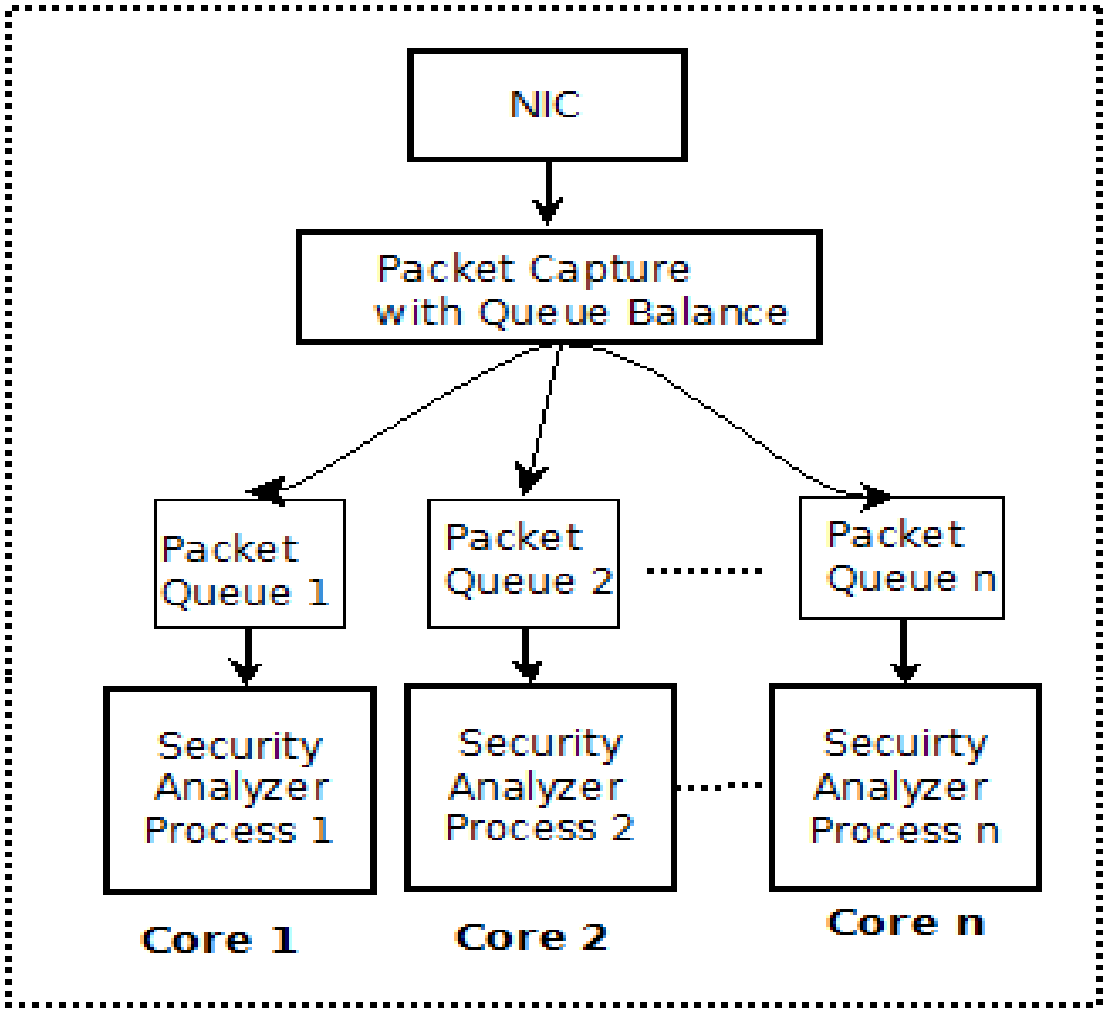
Packet Splitting Approaches



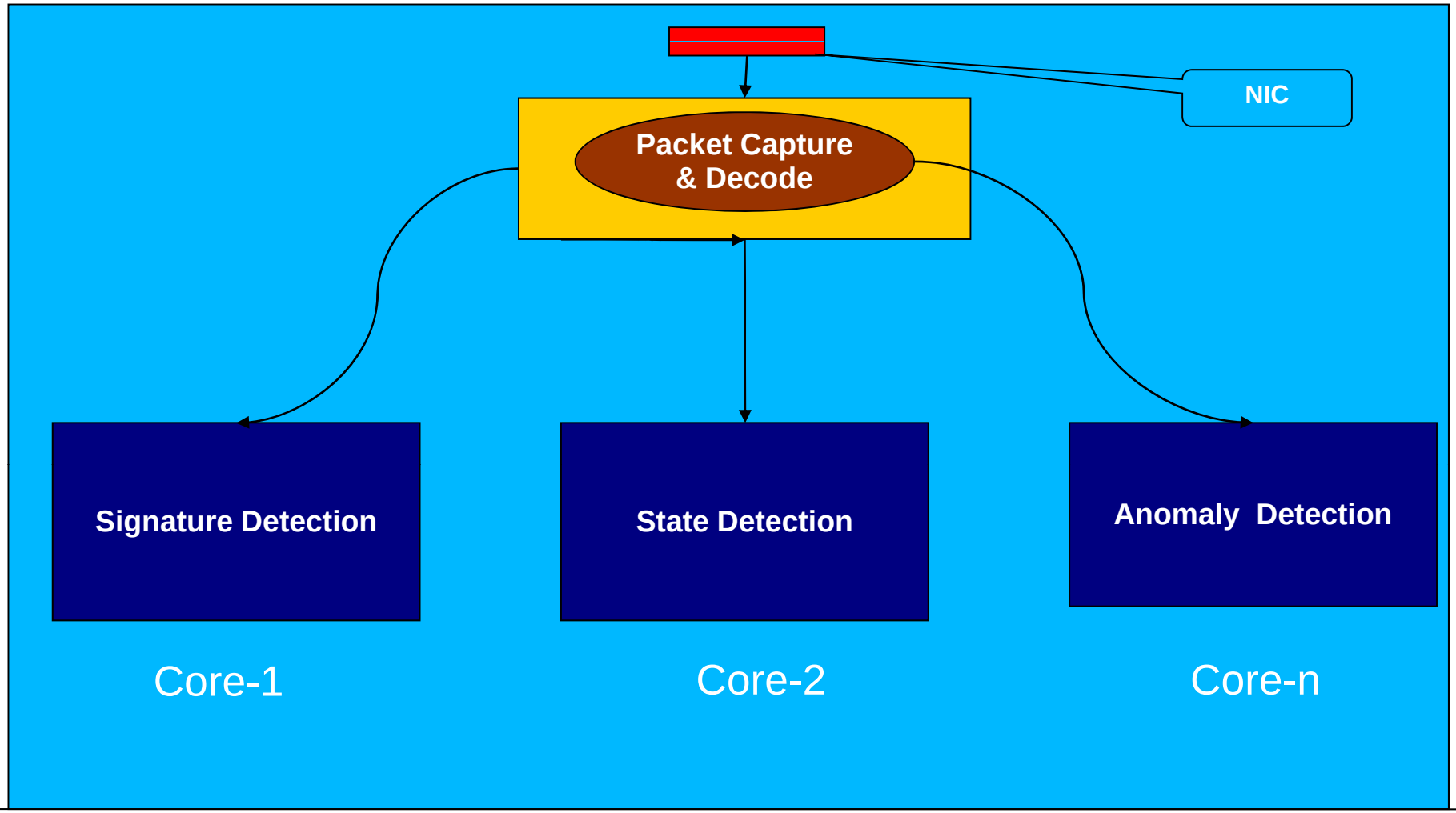
Packet Processing in Multi-core

- Data Parallelism
  - Each Core executes an Identical version of same packet processing algorithm
- Task Parallelism
  - Executes the components which are independent each other in parallel
- Pipeline Parallelism
  - multiple tasks need to be executed in a specific pre-defined order for each incoming packet

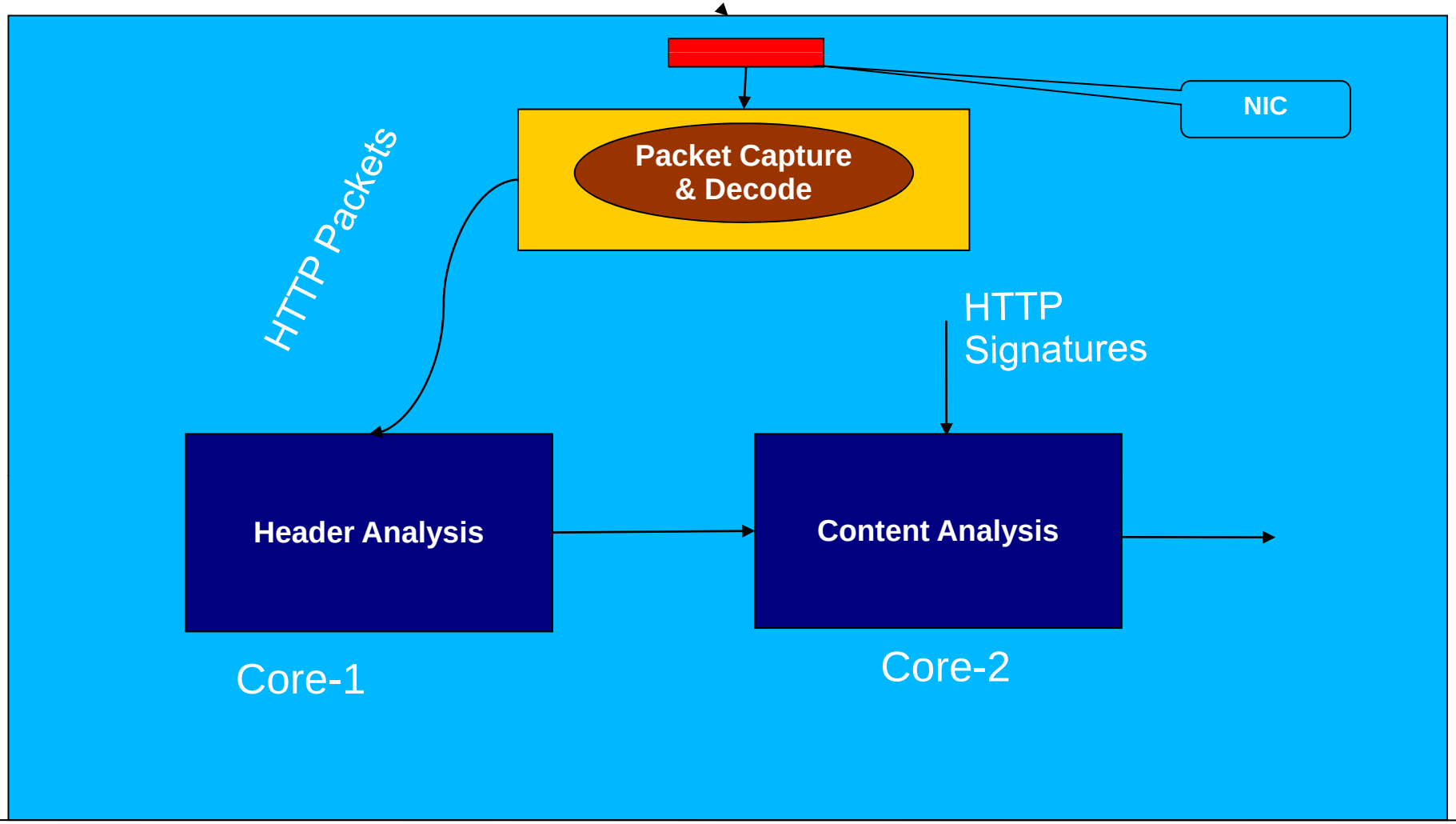
Multicore Based Approach
Data parallelism



Multi Core Based Approach
Task Parallelism



Multi Core Based Approach
Pipeline Parallelism



Data Spliting - Details

Hash based techniques	Application based techniques
• For Deployment no Prior understanding of the Network required	For Deployment Prior understanding of the Network required for partitioning the traffic
Balanced traffic splitting	Difficult to ensure balanced traffic splitting

Hash Based Packet Splitting Using NFQUEUE

- Netfiler system provides a special target NFQUEUE used to queue packets to user space programs

Uses source_ip, destination_ip, source_port, destination_port, protocol for hashing

Ensures connection stream (sessions)

Leverage the multi-core environment using multiple processes

Queue Balancing using NFQUEUE

- Packets are Balanced Across the given Queues
- Packets belonging to the same connection are put into same nfqueue
- Start Multiple instances of the user space program on Queue

  IPTABLE -A FORWARD -p <protocol> -j NFQUEUE --queue-balance 1:N

Packet Splitting Using NFQUEUE - Test Results

	Processor	Memory	Number of Cores	Number of Process	Throughput
	Intel Xeon Processors (3.16 Ghz)	2 Gb	4 (Two Dual Core)	3	270 Mbps
	Xeon CPU(X5460) 3.16Ghz	4 Gb	8 (2 Quad Core)	7	960 Mbps

GPU Based Packet Processing

- GPUs (Graphical Processing Units) are specialized for computationally intensive and highly parallel operations for graphic processing
- Modern GPUs have low design cost and their increased programmability makes them more flexible for network processing.
- Vendor provides high-level APIs that offer high programming capabilities

GPU Based Packet Processing

Gnort

- Implementation of Snort IDS in GPU provides maximum traffic processing throughput of 2.3 Gbps
  - Copy batch of packets to the GPU
  - Pattern matching on GPU
  - Transferring the results to CPU

Header Analysis for Highspeed Networks

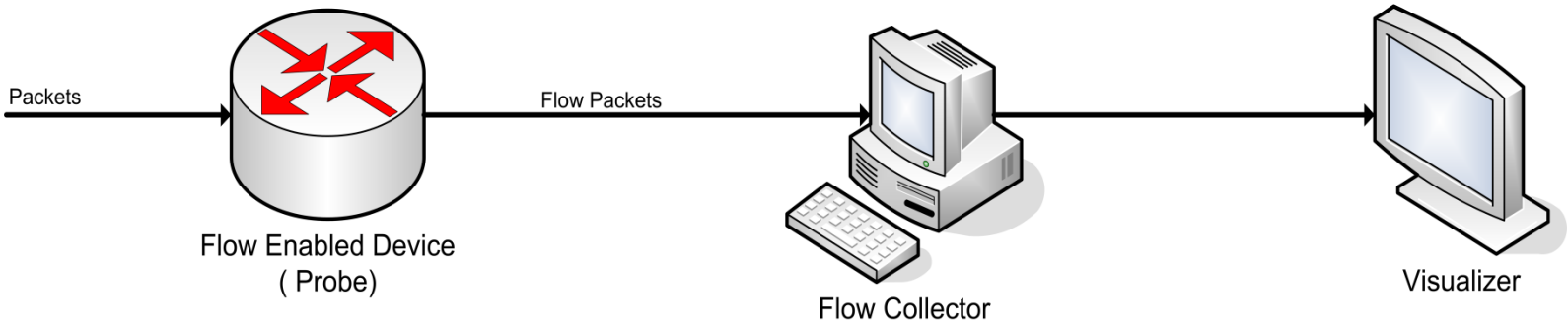
Flow Based Traffic Analysis

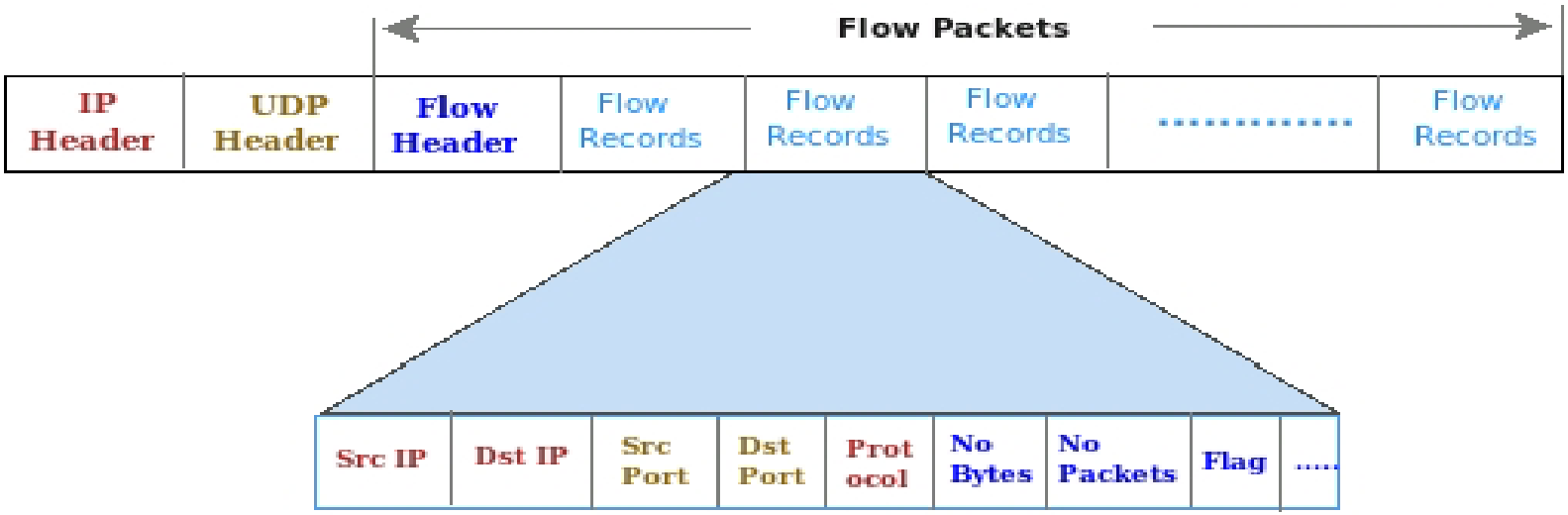
Flow

IP flow is a unidirectional series of IP packets of a given protocol traveling between a source and a destination IP/port pair within a certain period of time

- Aggregate information from different packets in to a flow
- Compared to packet based analysis , volume of data is very less – suitable for high speed network traffic analysis

Header Analysis for High speed Networks





References

- Exploiting Commodity Mulch-core Systems for Network Traffic Analysis Lucas Devi, Francisco Fusion
- Improving Network Performance in Mulch-Core Systems – Intel white paper
- An Architecture for Exploiting Multi-Core Processors to Parallelize Network Intrusion Prevention - Vern Paxson,Robin Sommer
- Comparing and Improving Current Packet Capturing Solutions based on Commodity Hardware Lothar Braun, Alexander Didebulidze, Nils Kammenhuber, Georg Carle
- Gnort: High Performance Network Intrusion Detection Using Graphics Processors - Giorgos Vasiliadis, Spiros Antonatos, Michalis Polychronakis, Evangelos P. Markatos, and Sotiris Ioannidis

Thank you

murali@cdac.in