P4-IPS:

Deploying Intrusion Prevention System with Machine Learning on P4 Switch

Prof. **Charles H.-P. Wen**

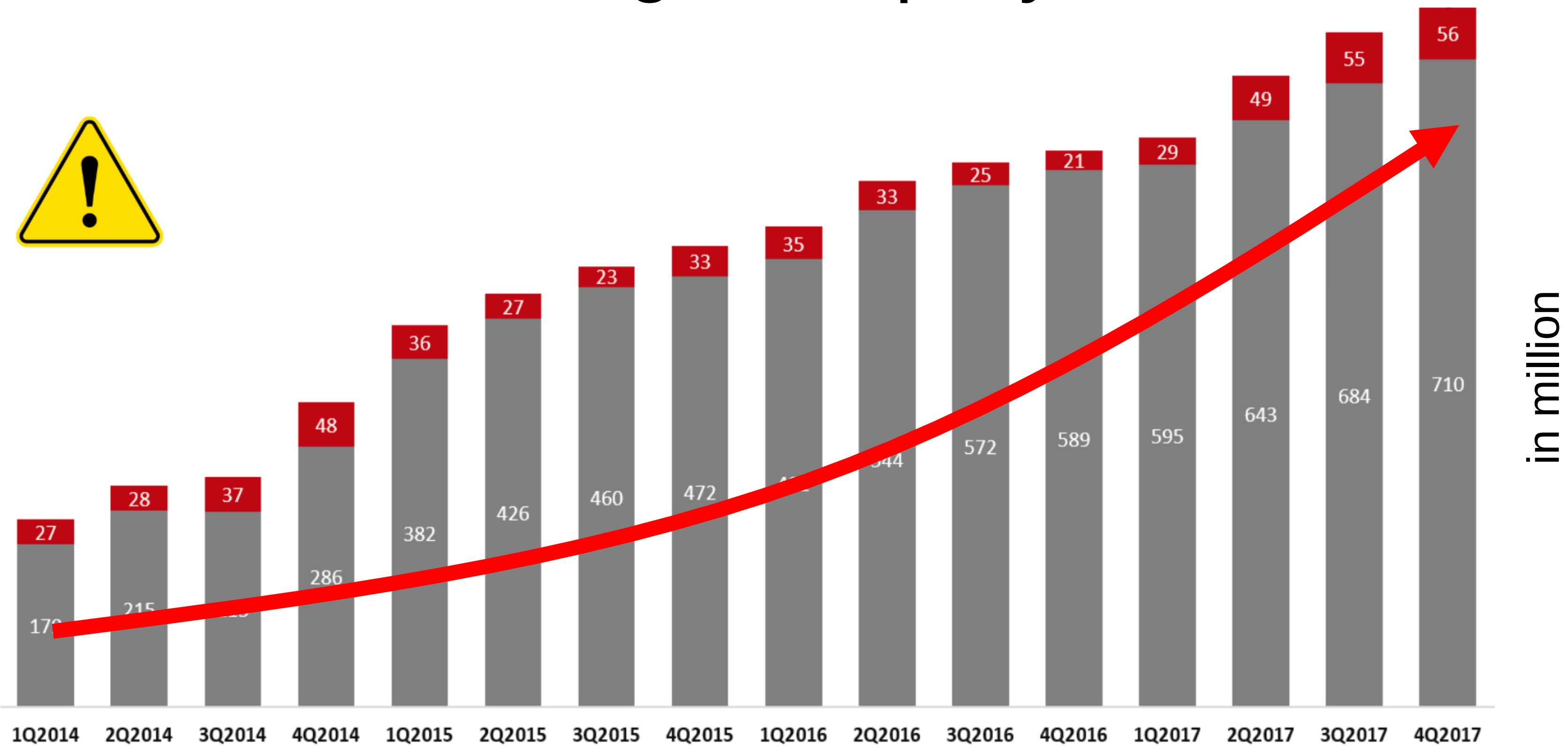
Computational Intelligence on Automation (C.I.A.) Lab,

National Yang Ming Chiao Tung University

This project is partially sponsored by **Edgecore Networks

IoT Security

- IoT security is **unignorable** nowadays
  - – various IoT malwares grow rapidly

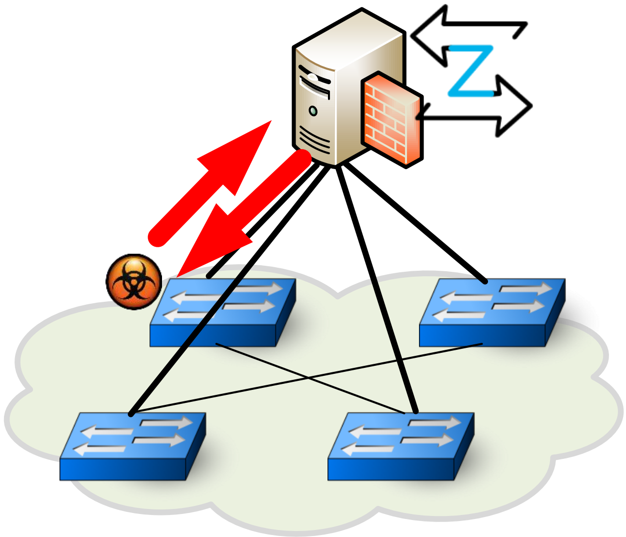


*from Counterpoint

Intrusion Prevention System

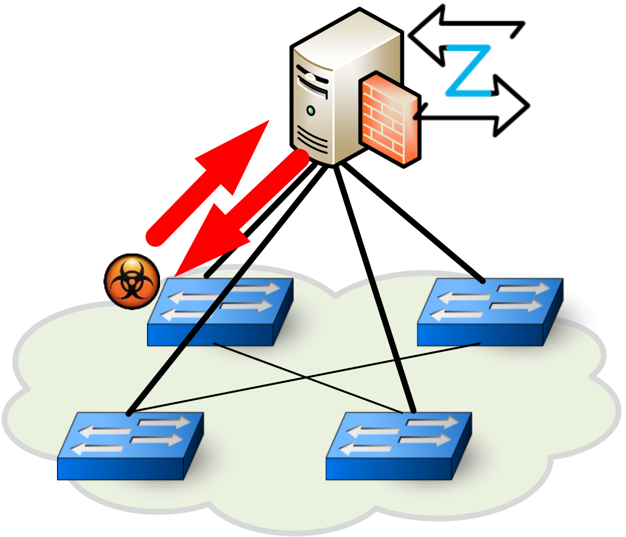
- Existing solutions of **intrusion prevention systems (IPS)**
  - Hardware IPS
  - SDN + VNF (e.g., Zeek)

⇨ trade-off between **performance** and **cost**

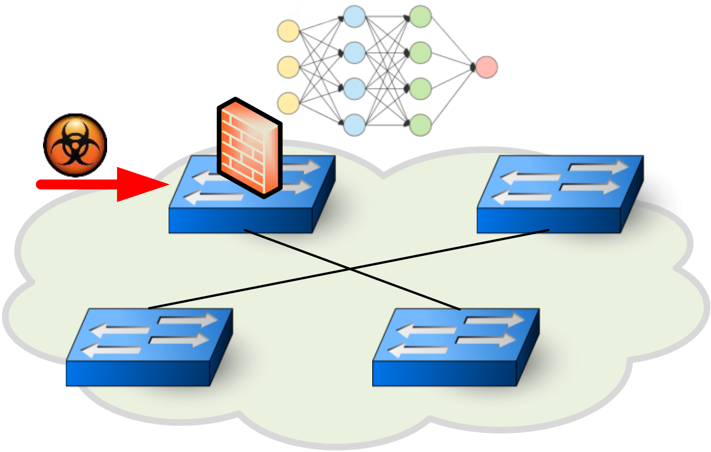


Enhancing SDN-based IPS

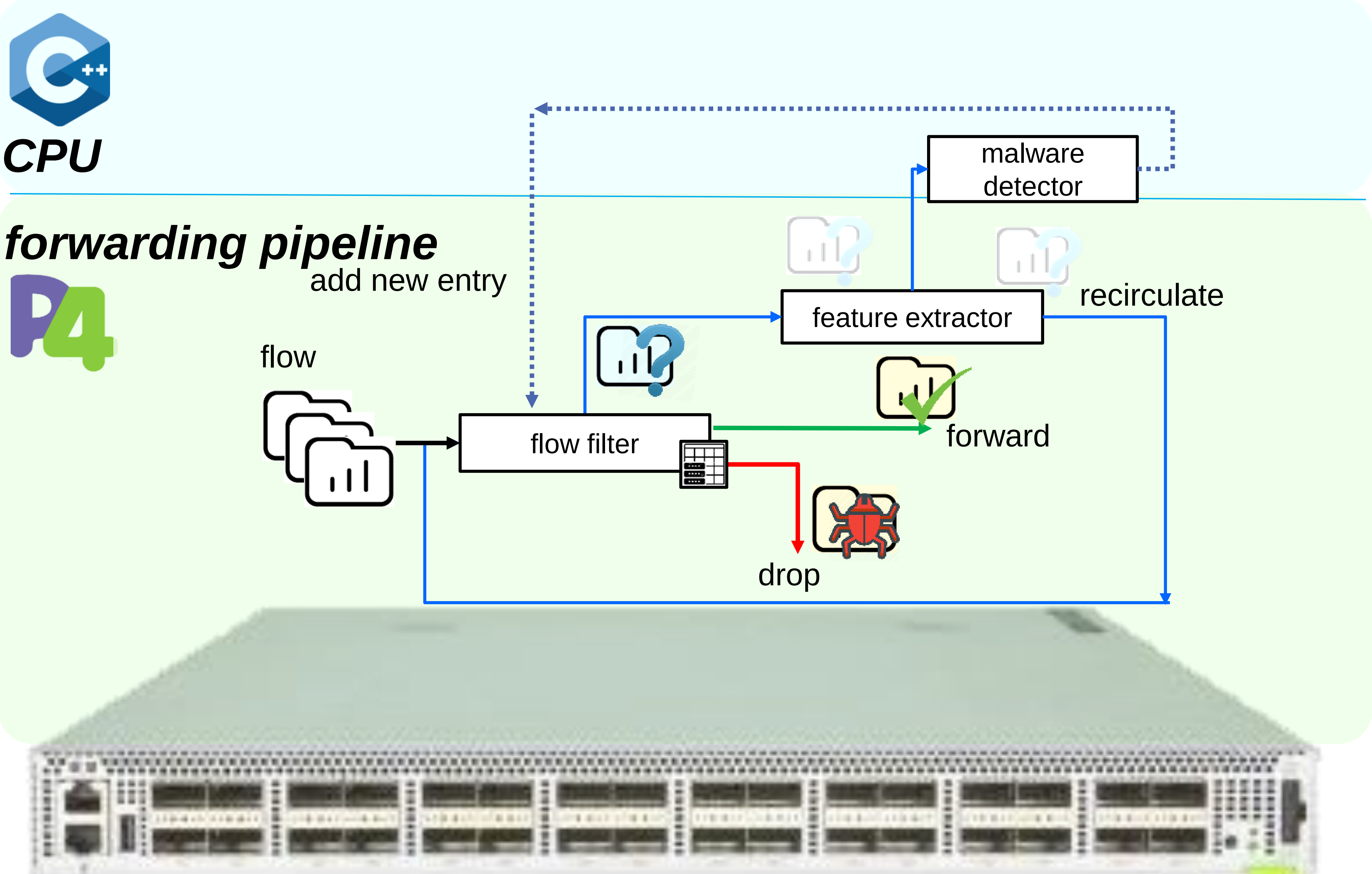
- SDN-based IPS
  - interact with SDN controller
  - external VNF is time-consuming
  - long response time



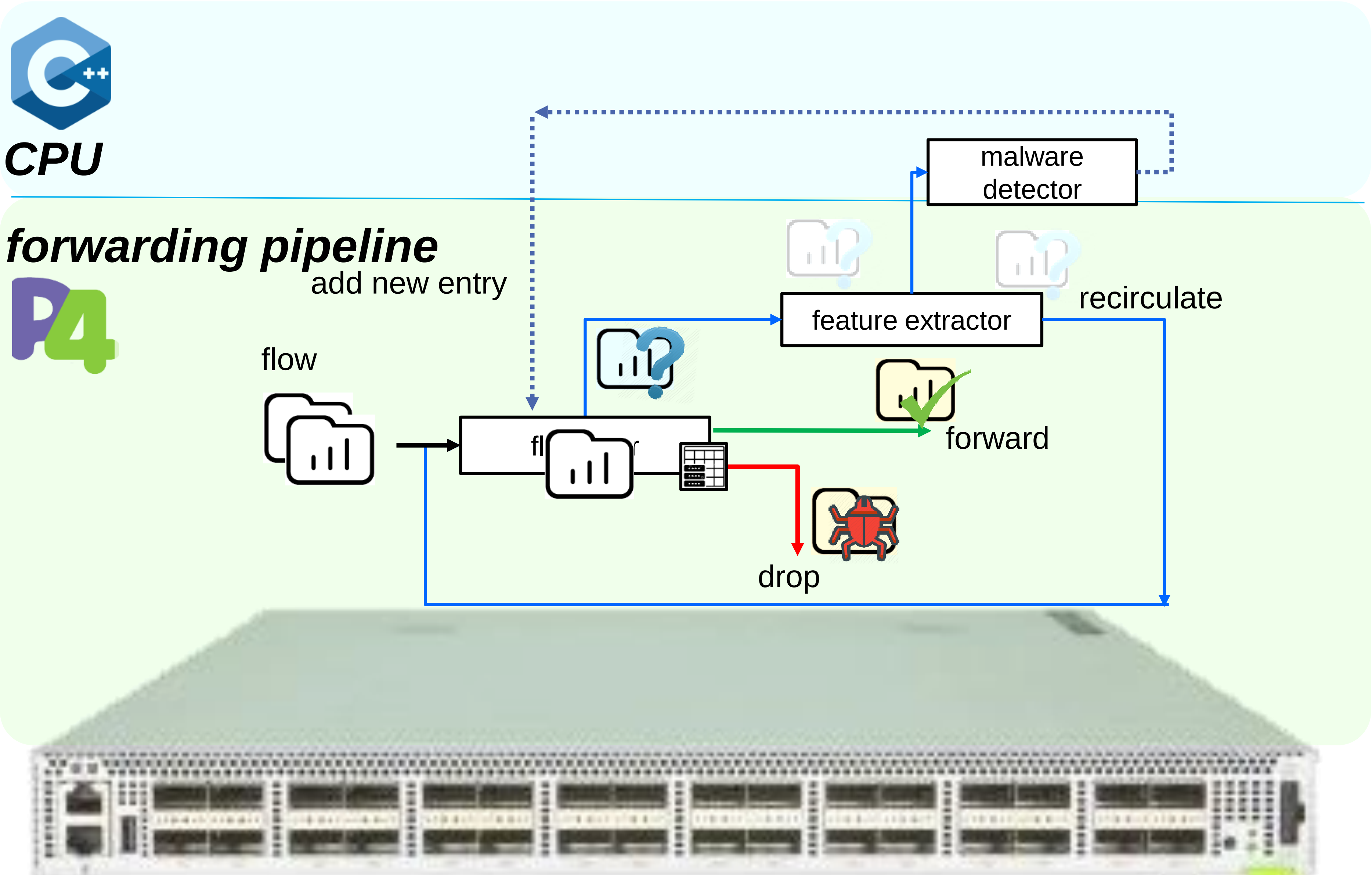
- P4-assisted IPS
  - enable **in-switch processing**
  - fast **neural-network computing** on switch CPU
  - shorter response time



Overview of P4-IPS



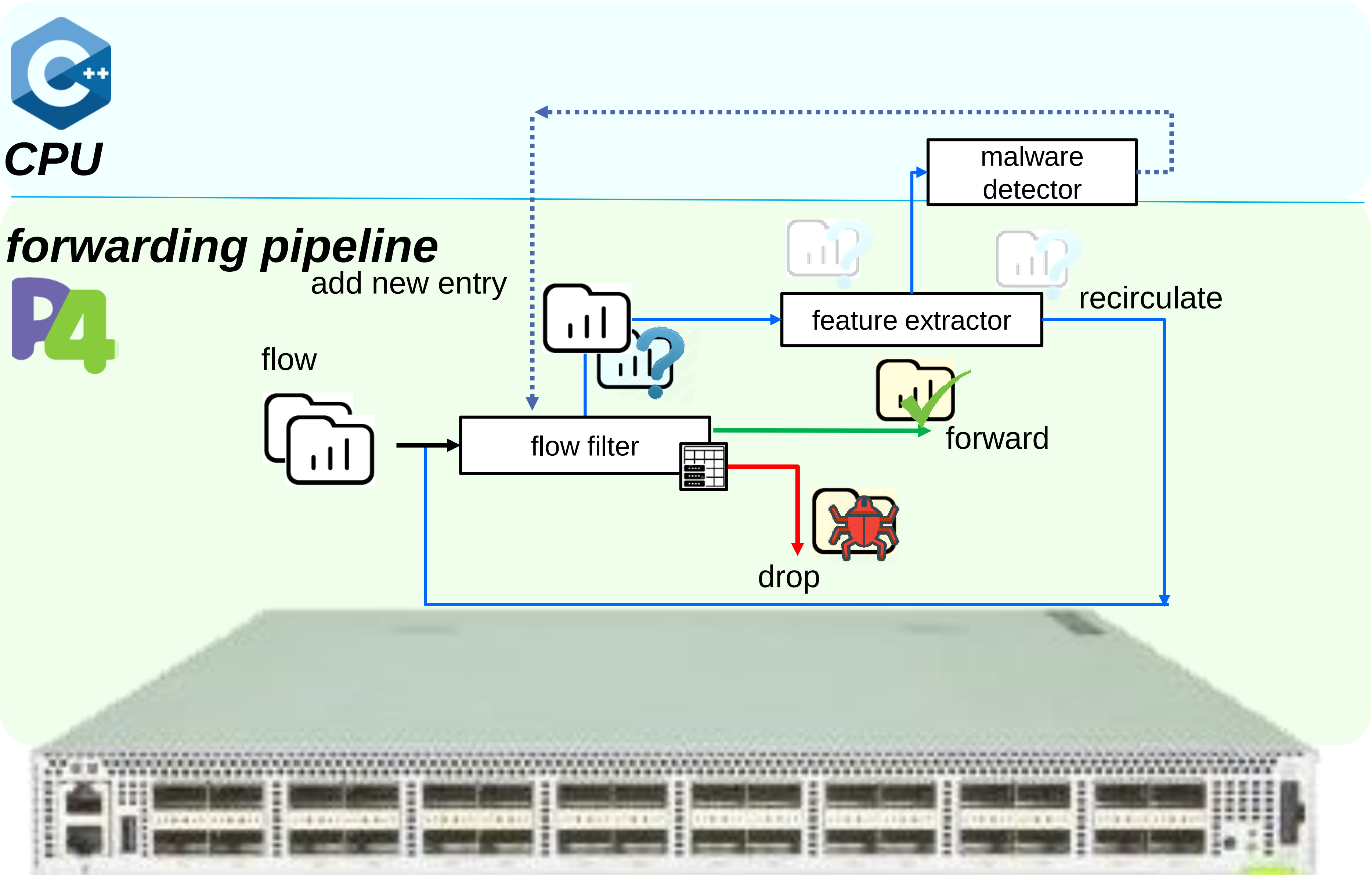
Overview of P4-IPS



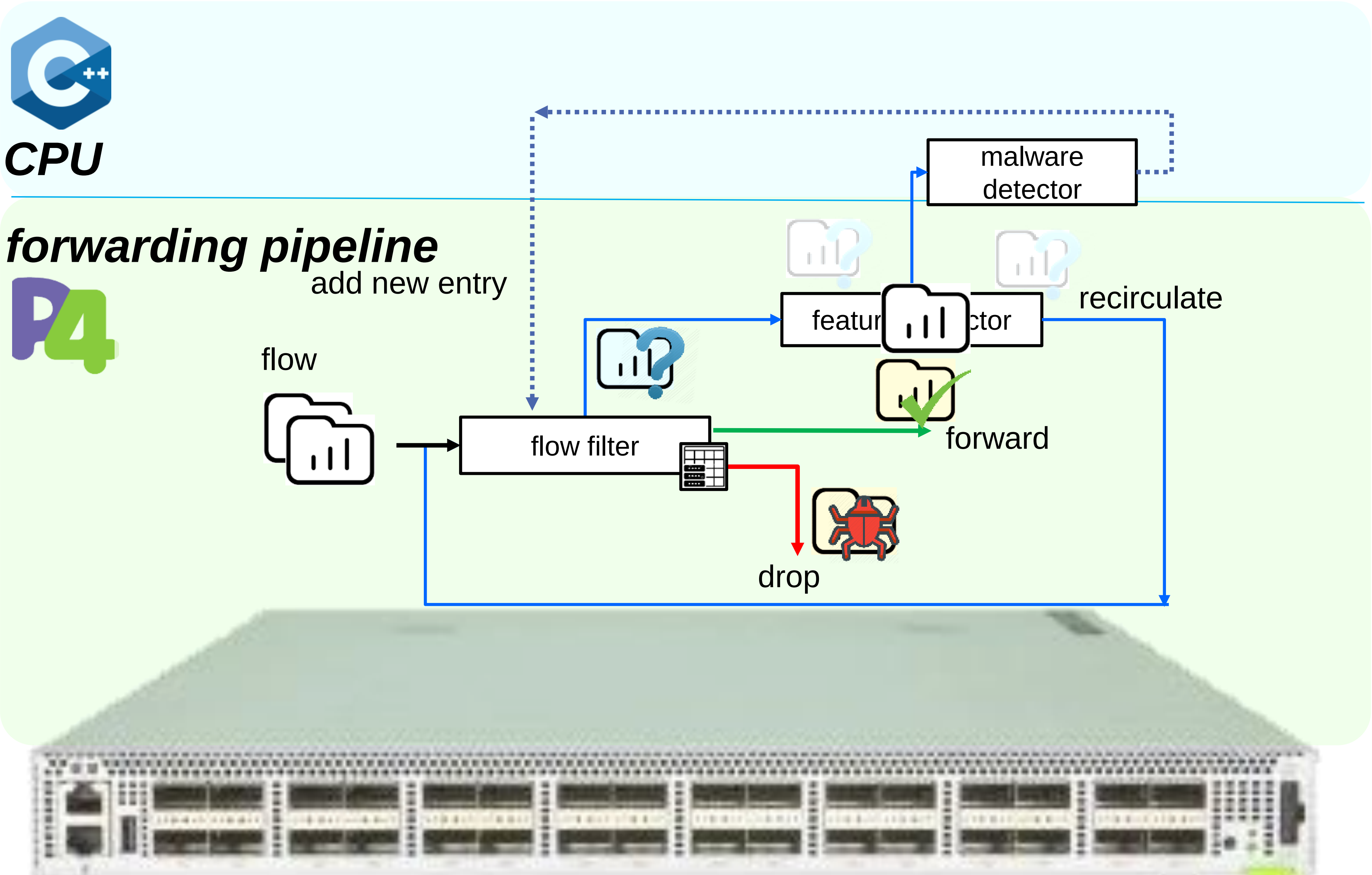
CPU

forwarding pipeline

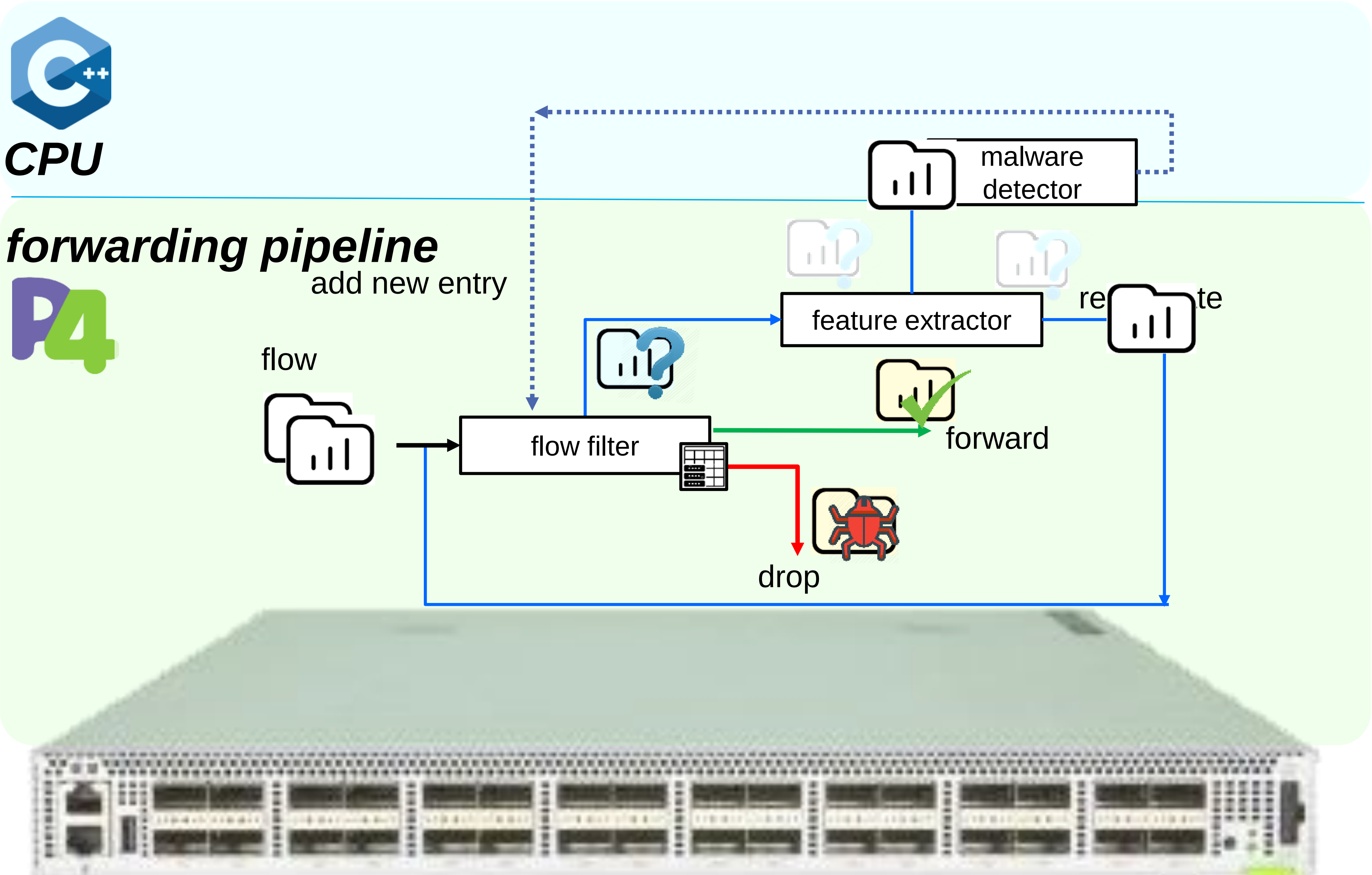
Overview of P4-IPS



Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

flow

flow filter

feature extractor

malware detector

re

te

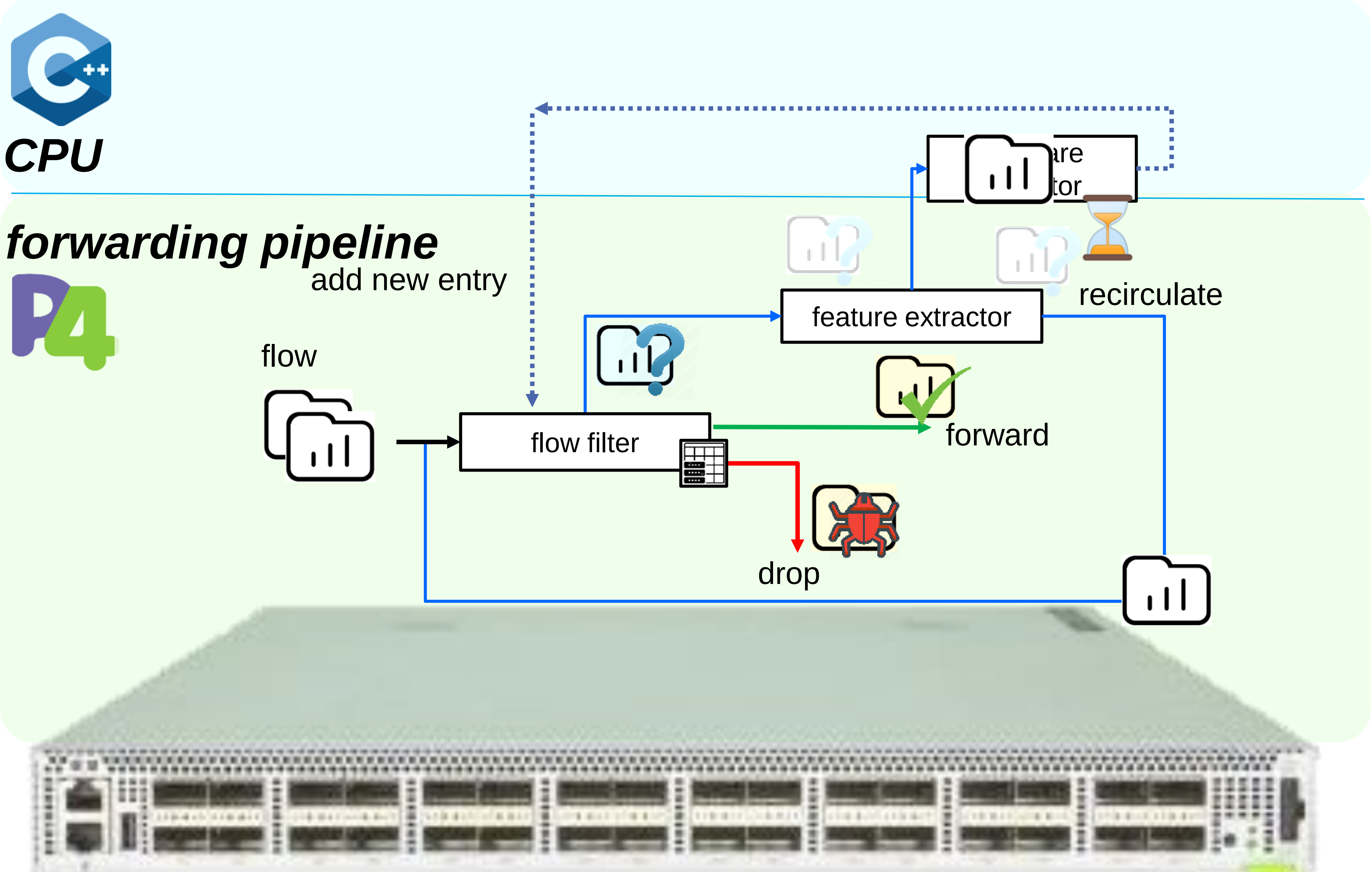
forward

drop

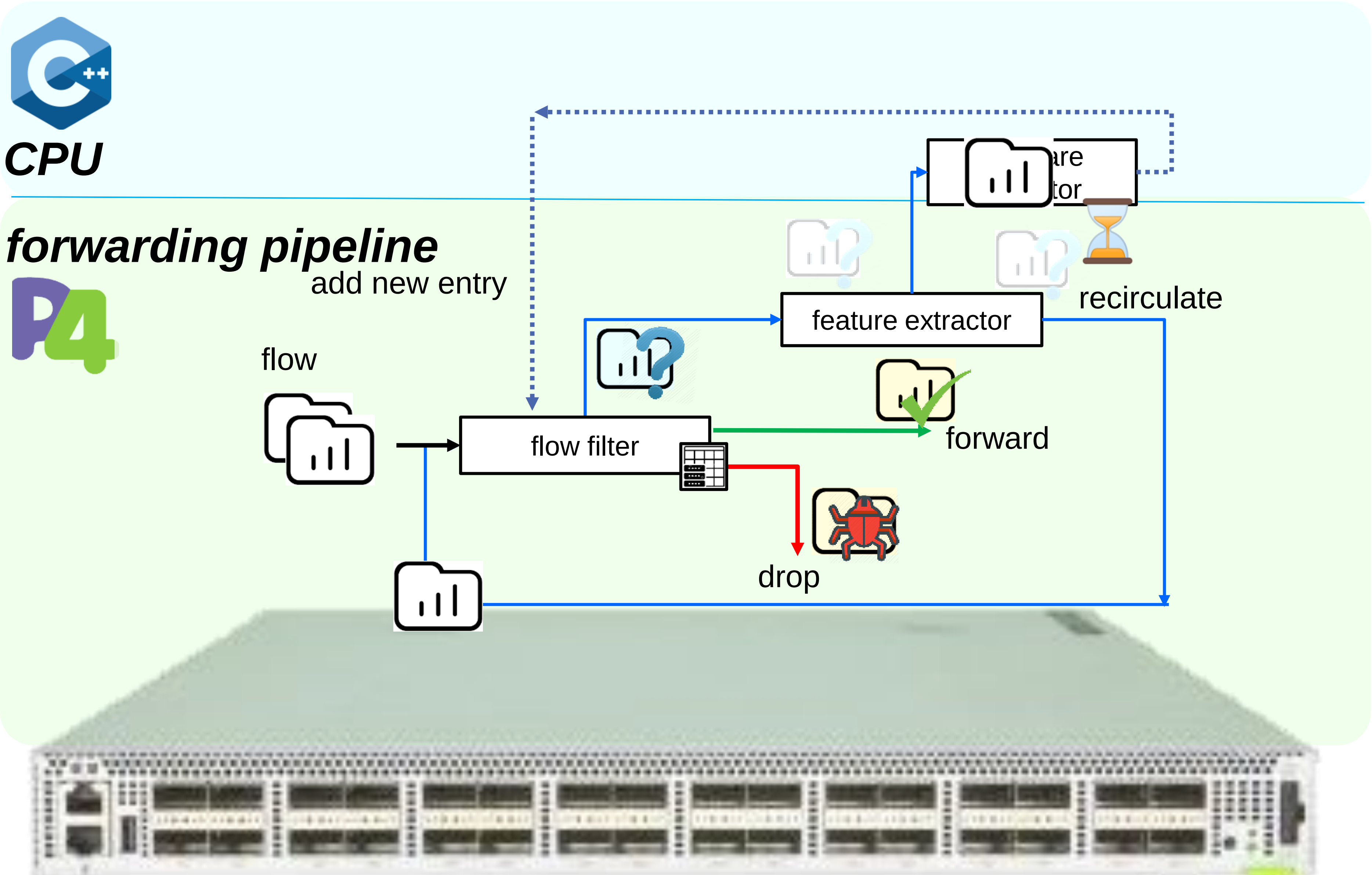
Overview of P4-IPS

National Chiao Tung University

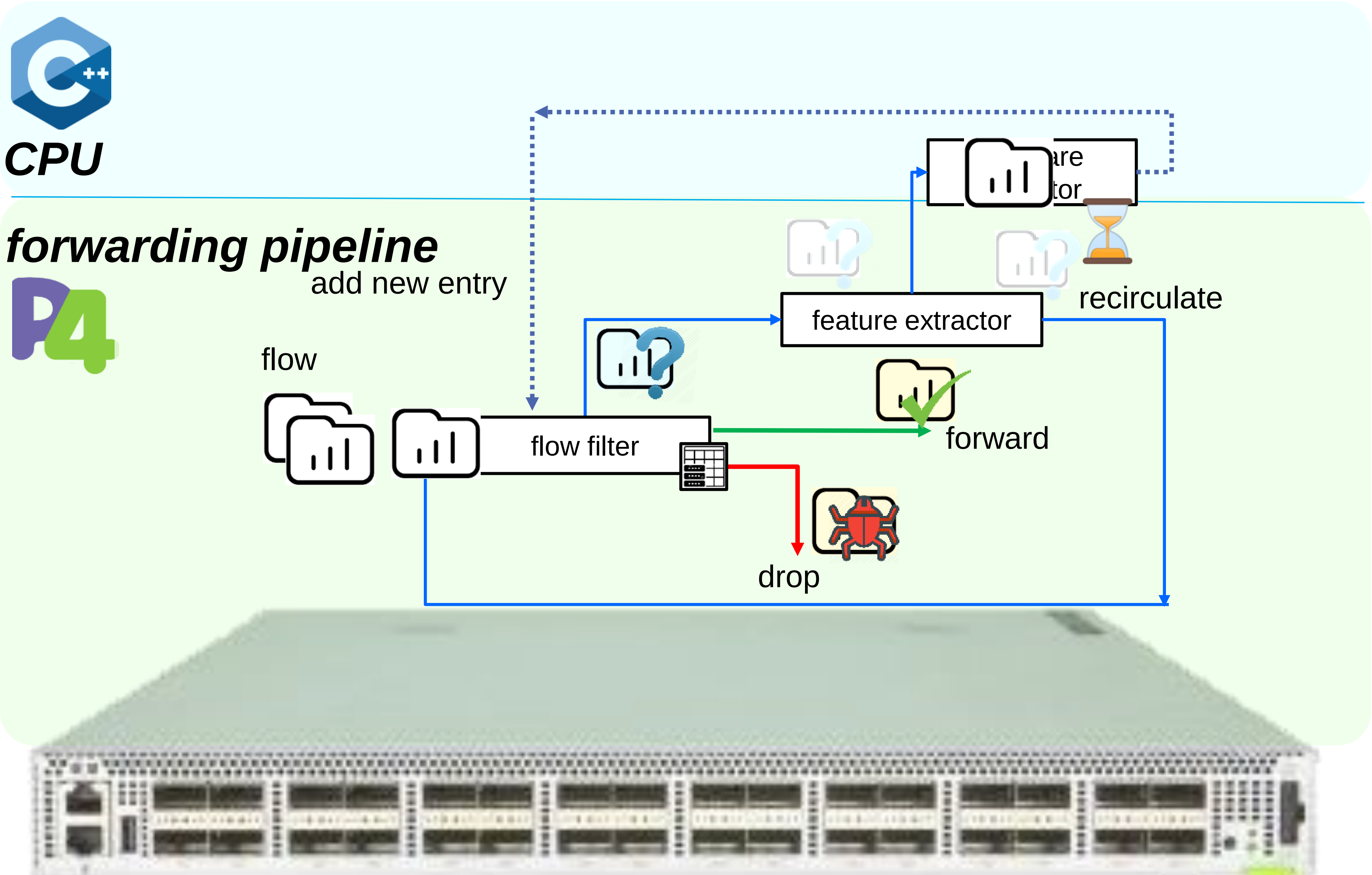
NETWORKS



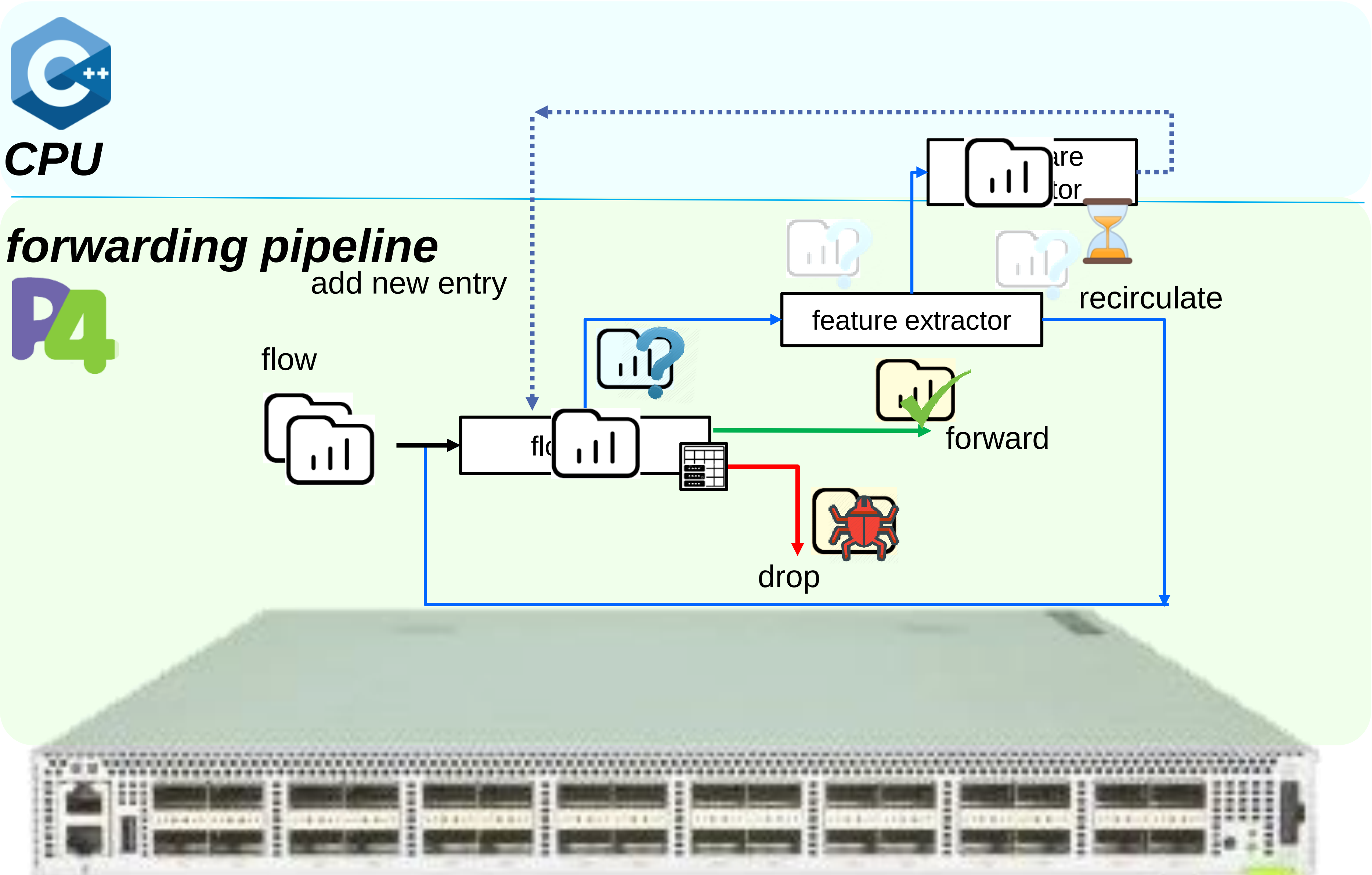
Overview of P4-IPS



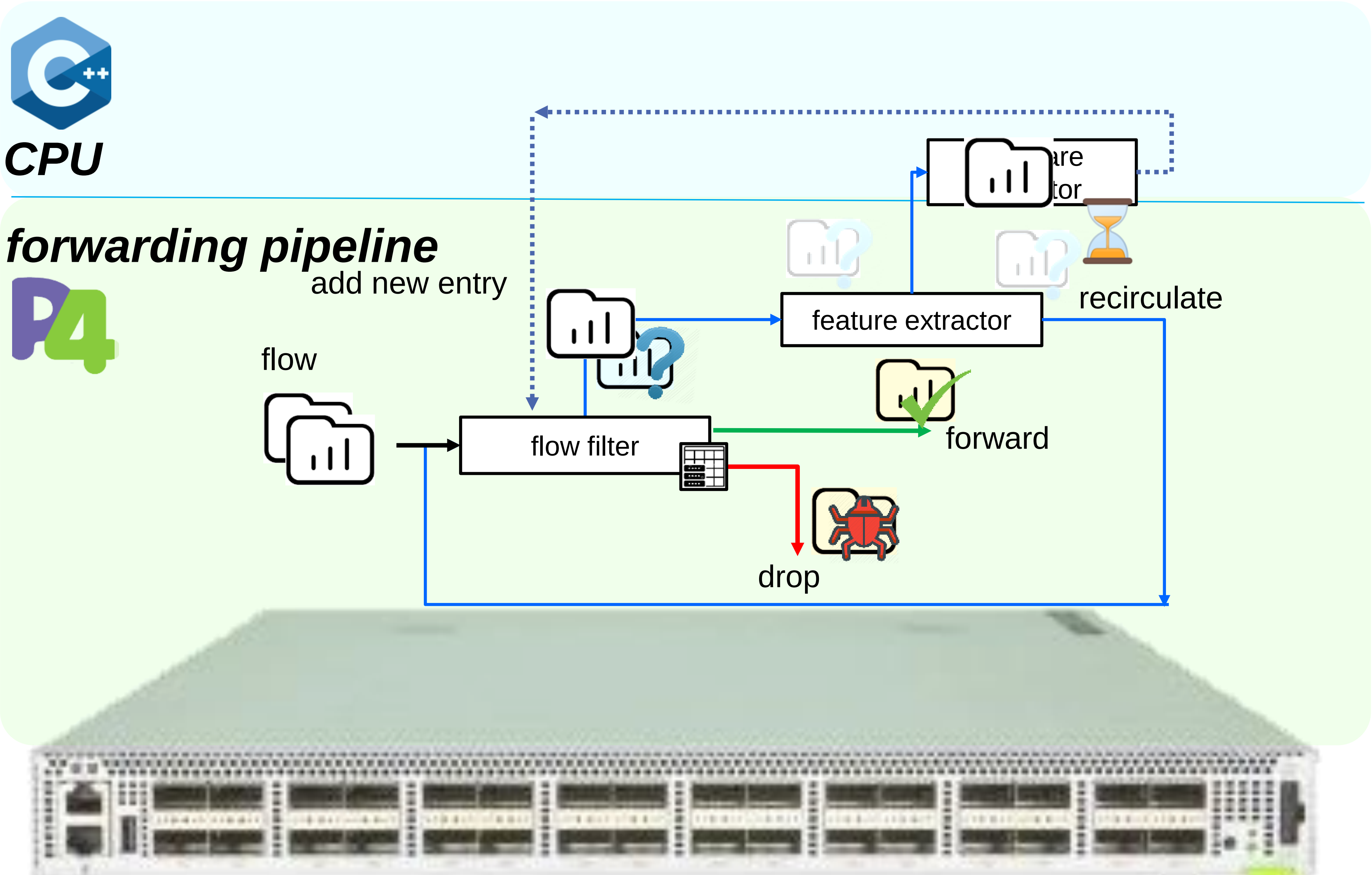
Overview of P4-IPS



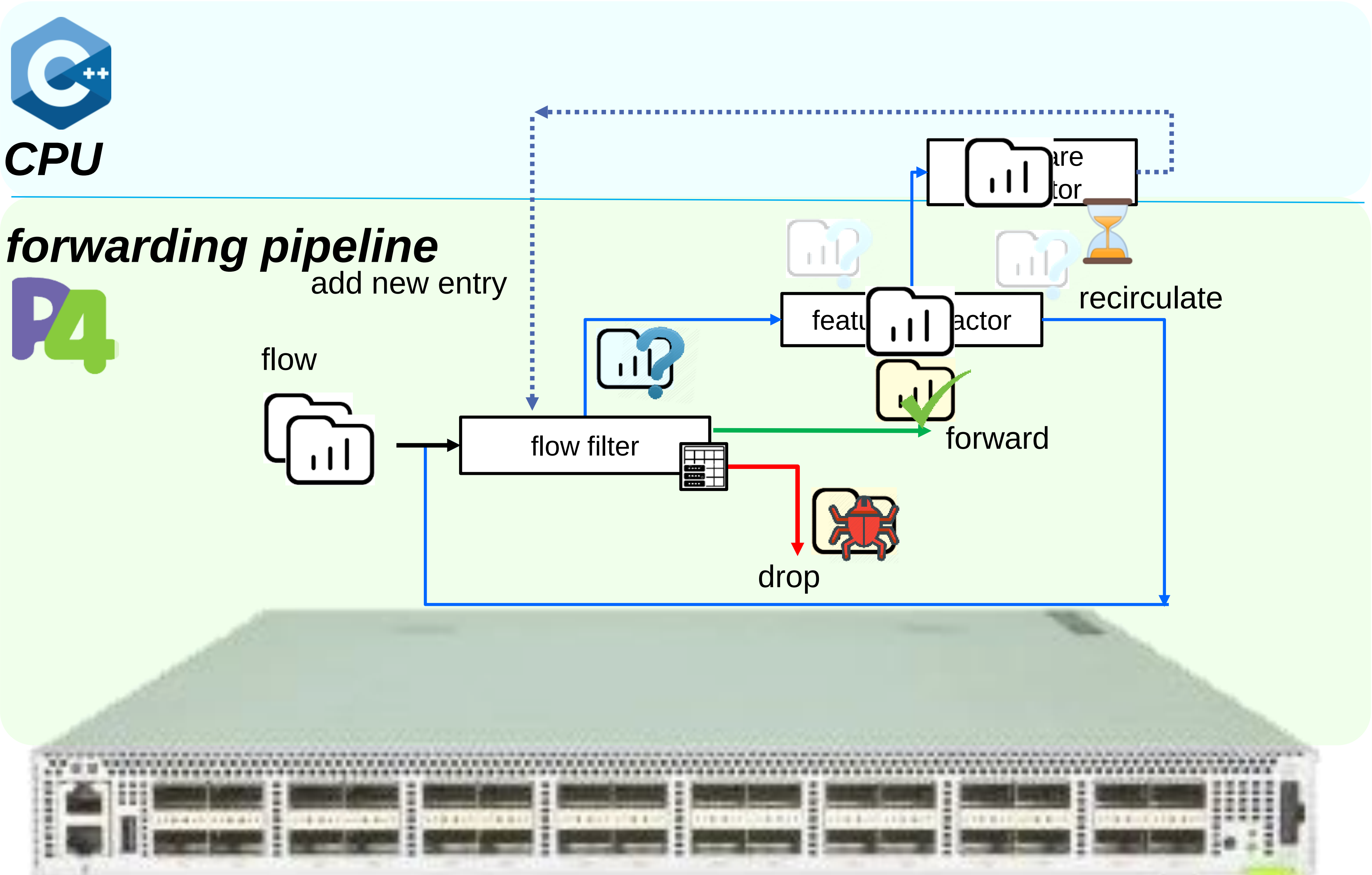
Overview of P4-IPS



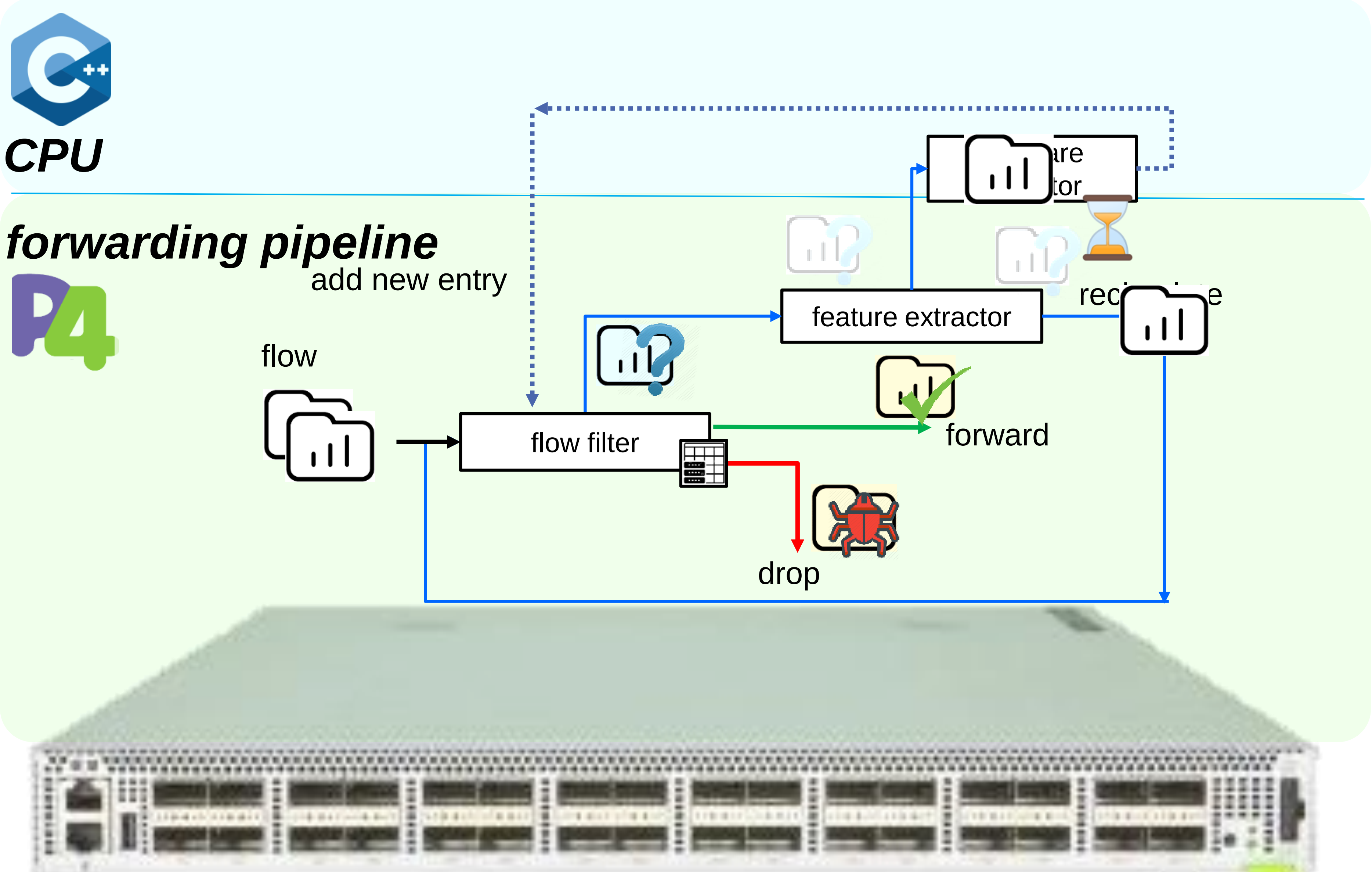
Overview of P4-IPS



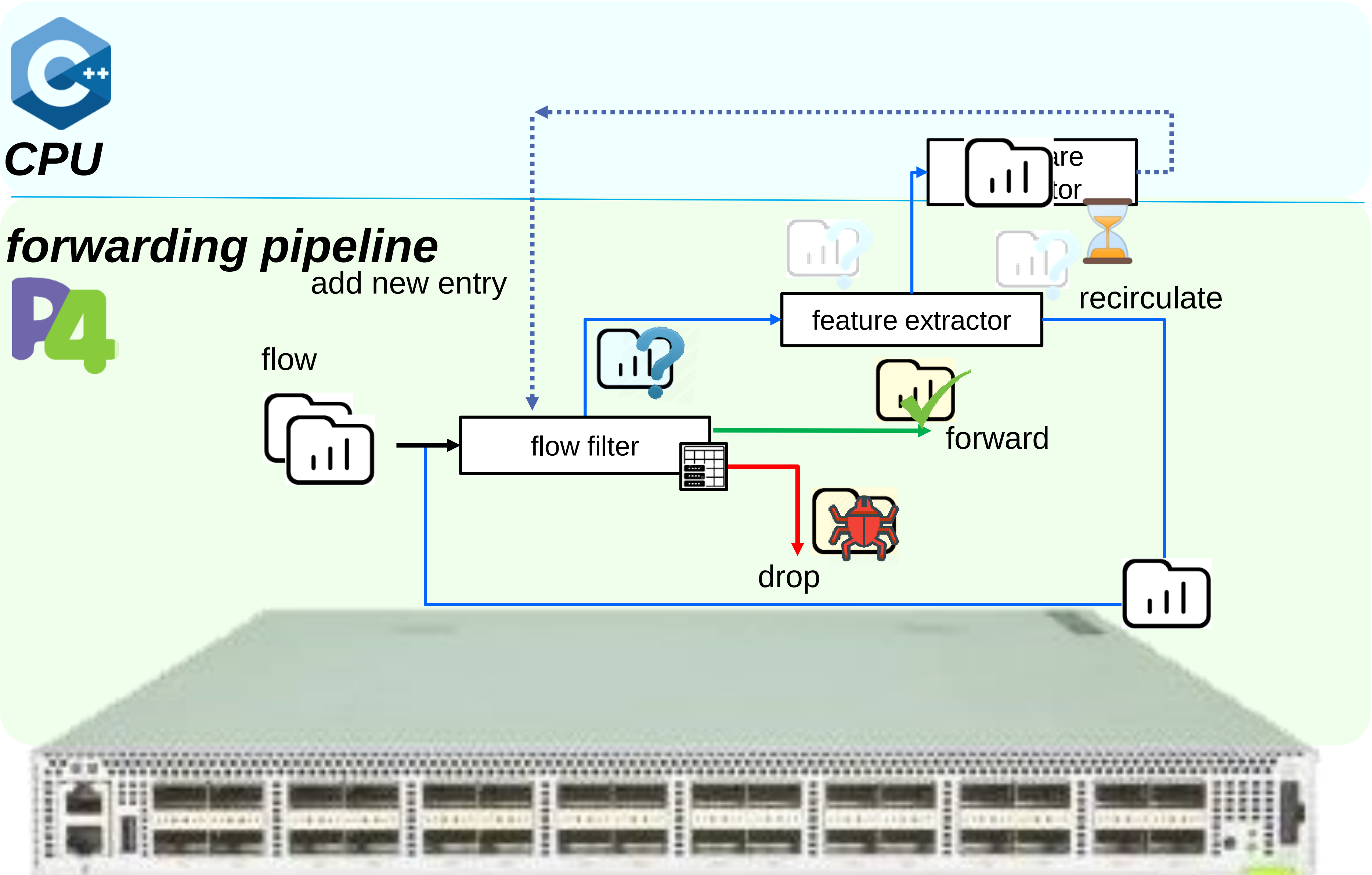
Overview of P4-IPS



Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

are
tor

recirculate

feature extractor

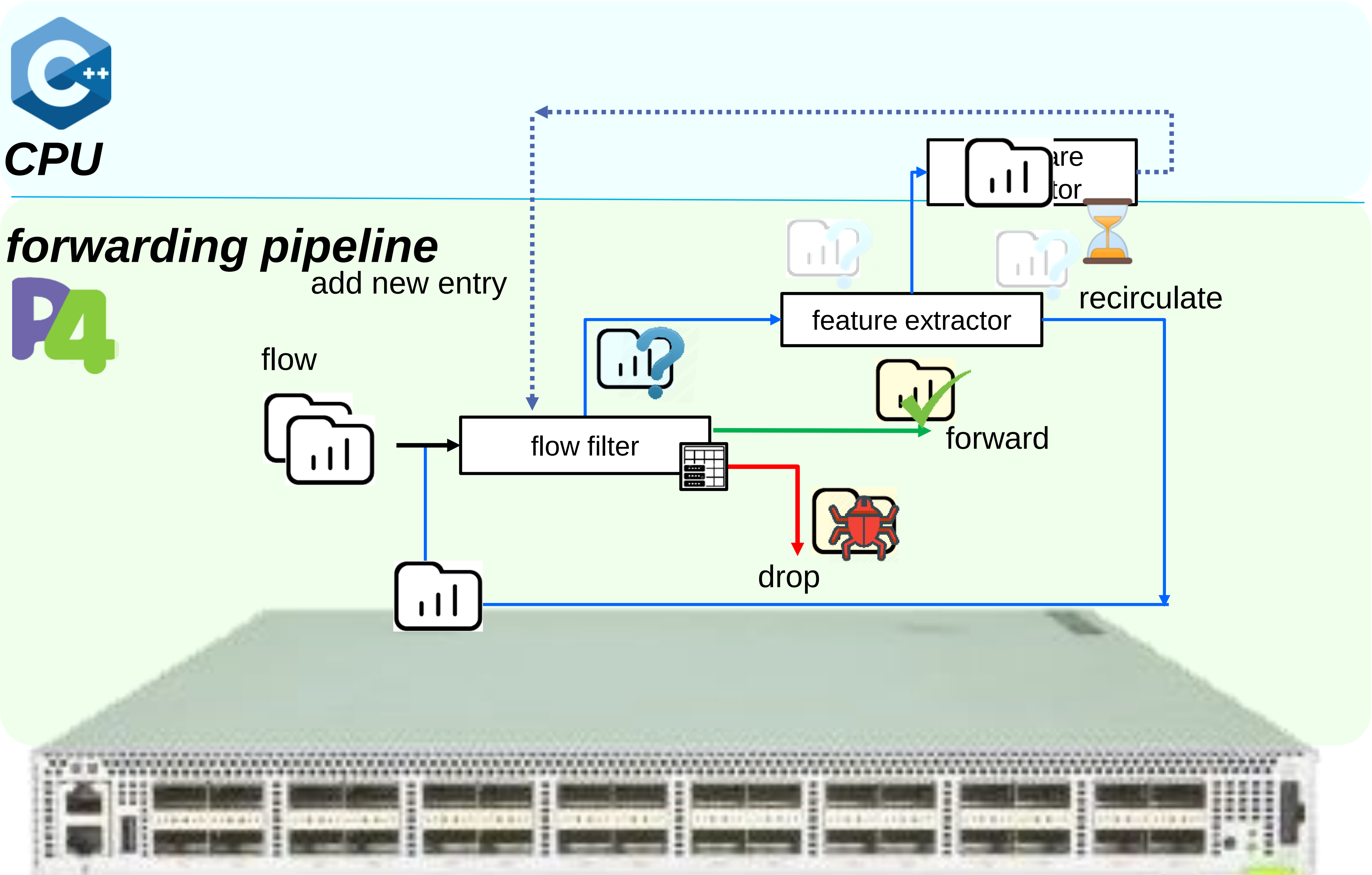
flow

flow filter

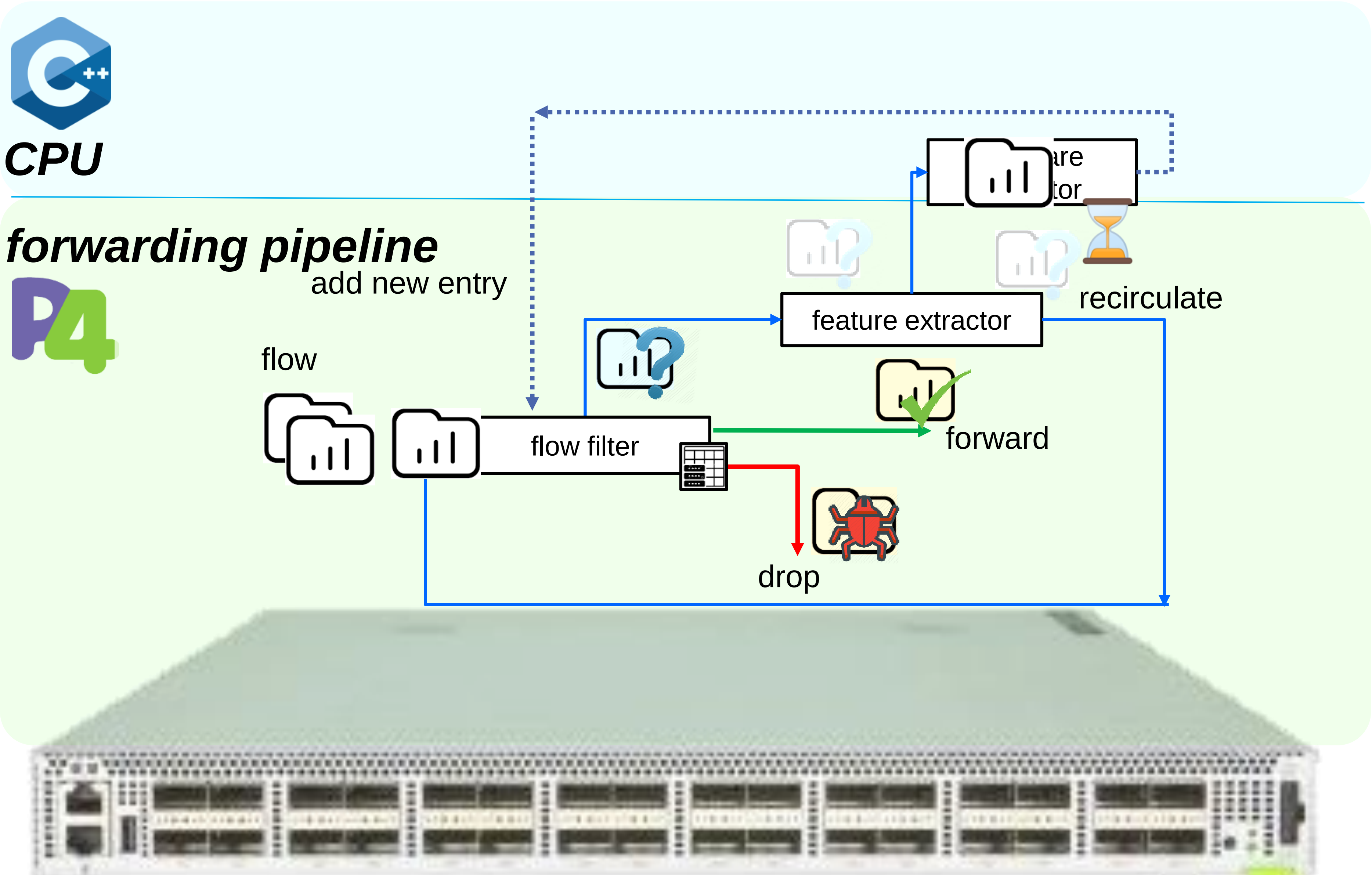
forward

drop

Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

flow

flow filter

feature extractor

are

tor

recirculate

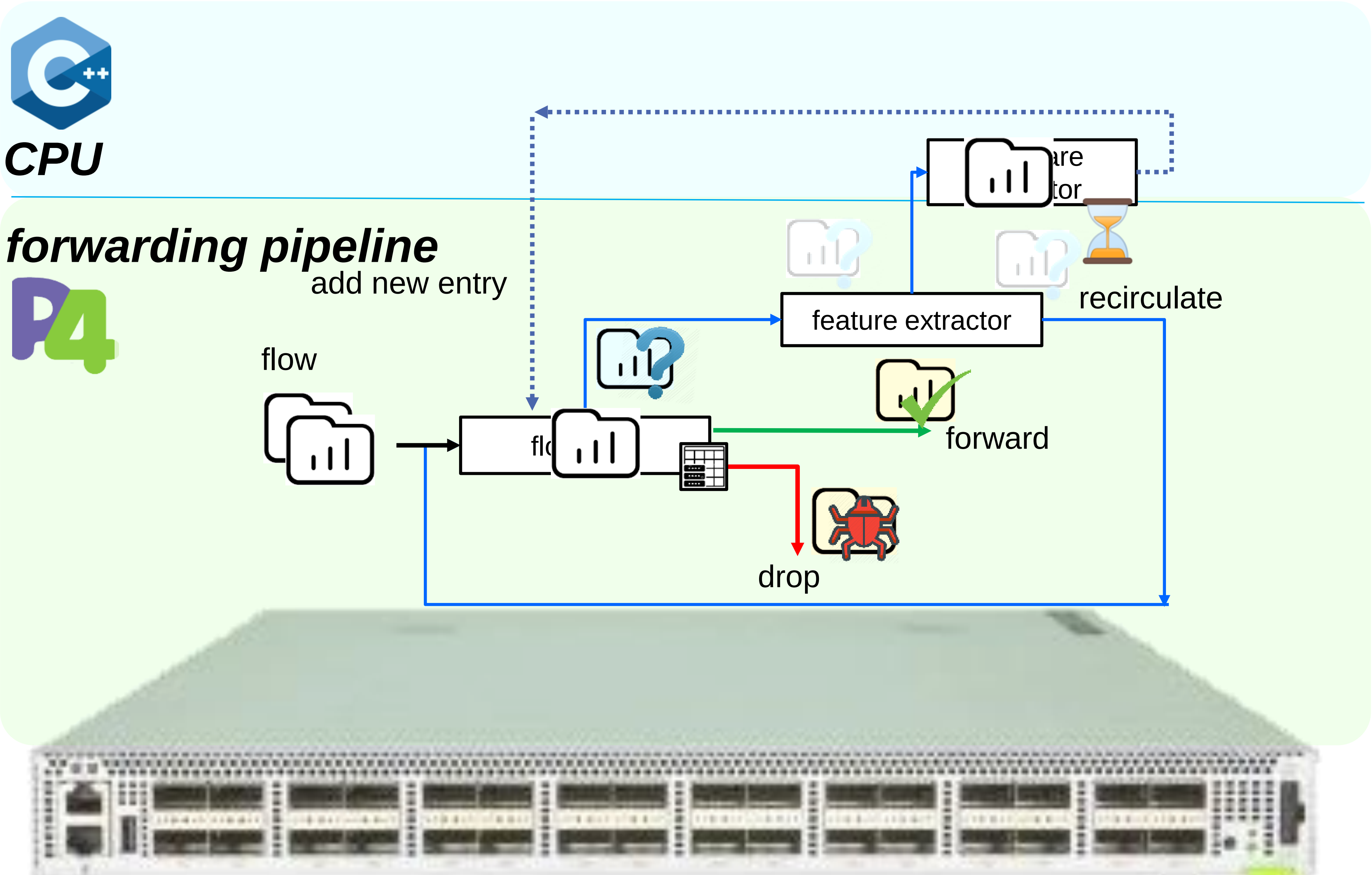
forward

drop

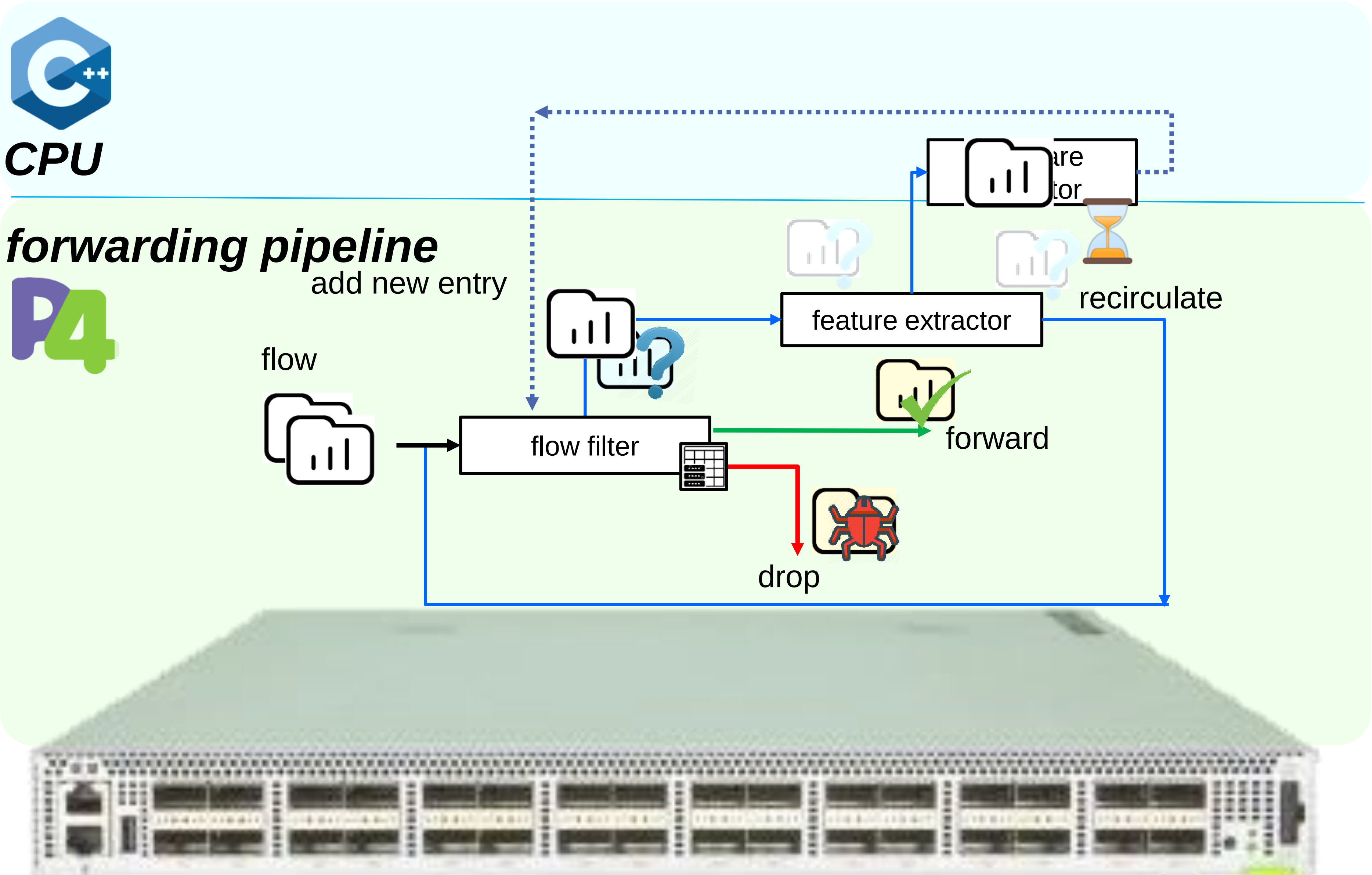
Overview of P4-IPS

National Chiao Tung University

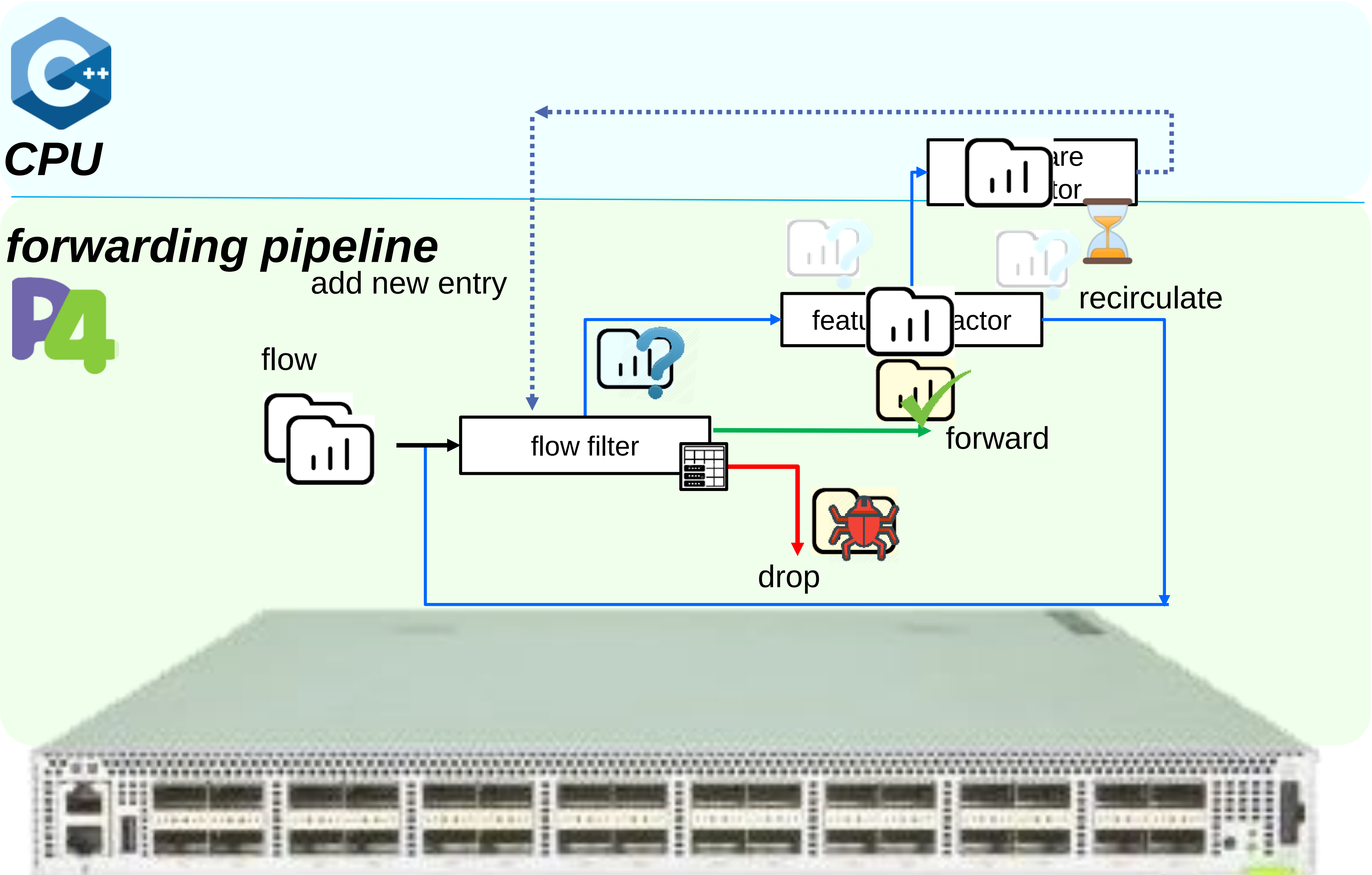
Edge-corE NETWORKS



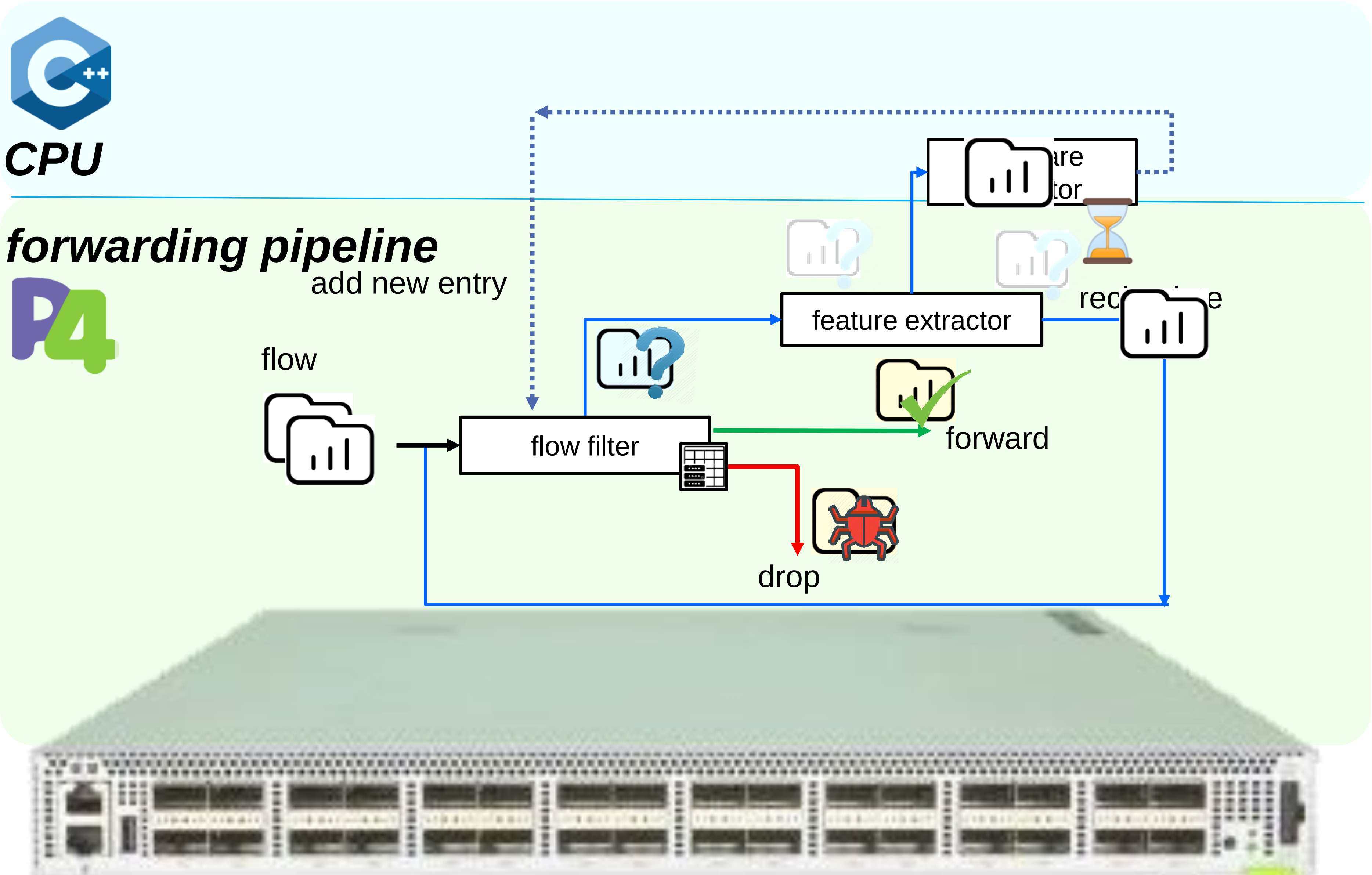
Overview of P4-IPS



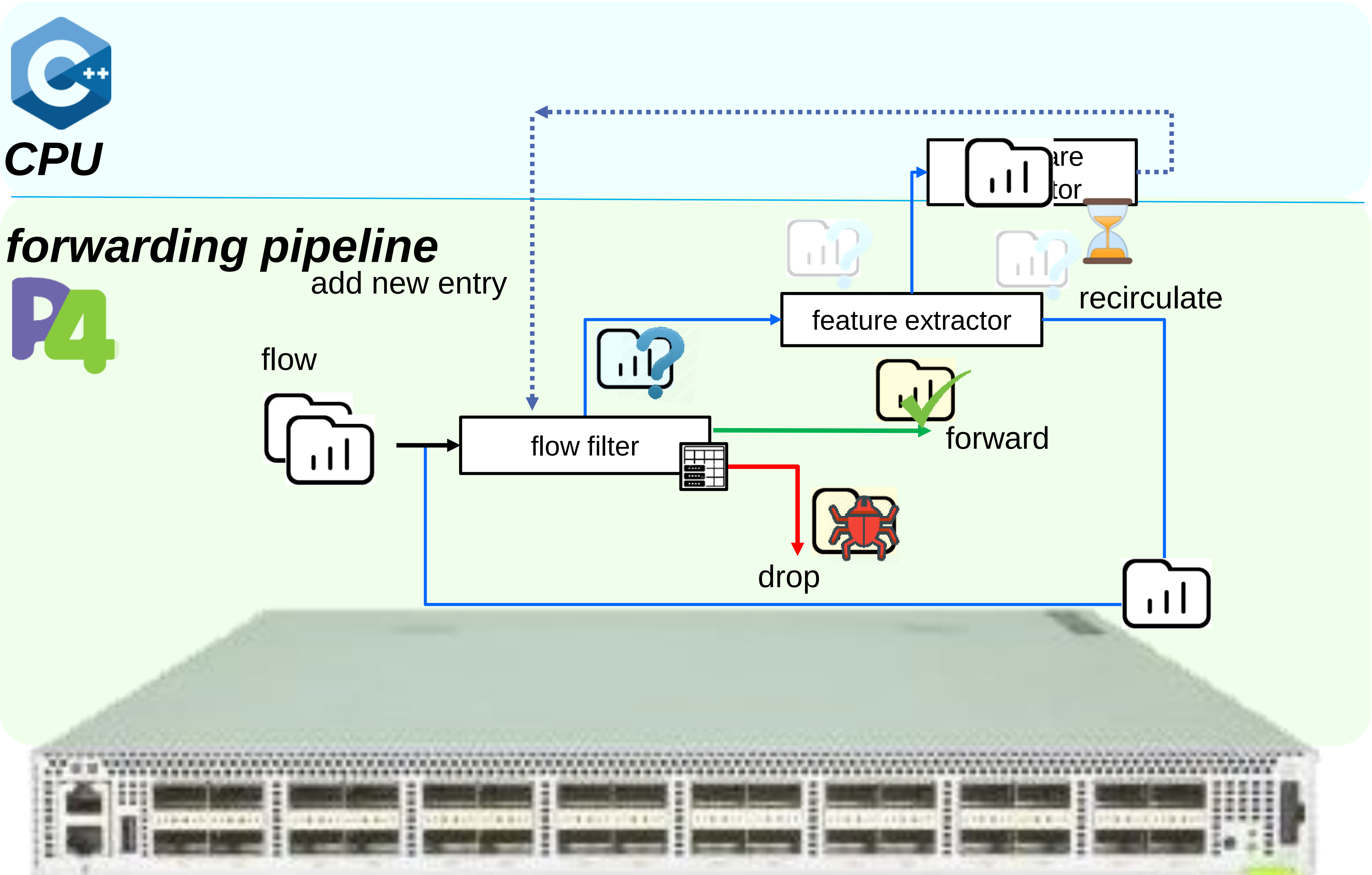
Overview of P4-IPS



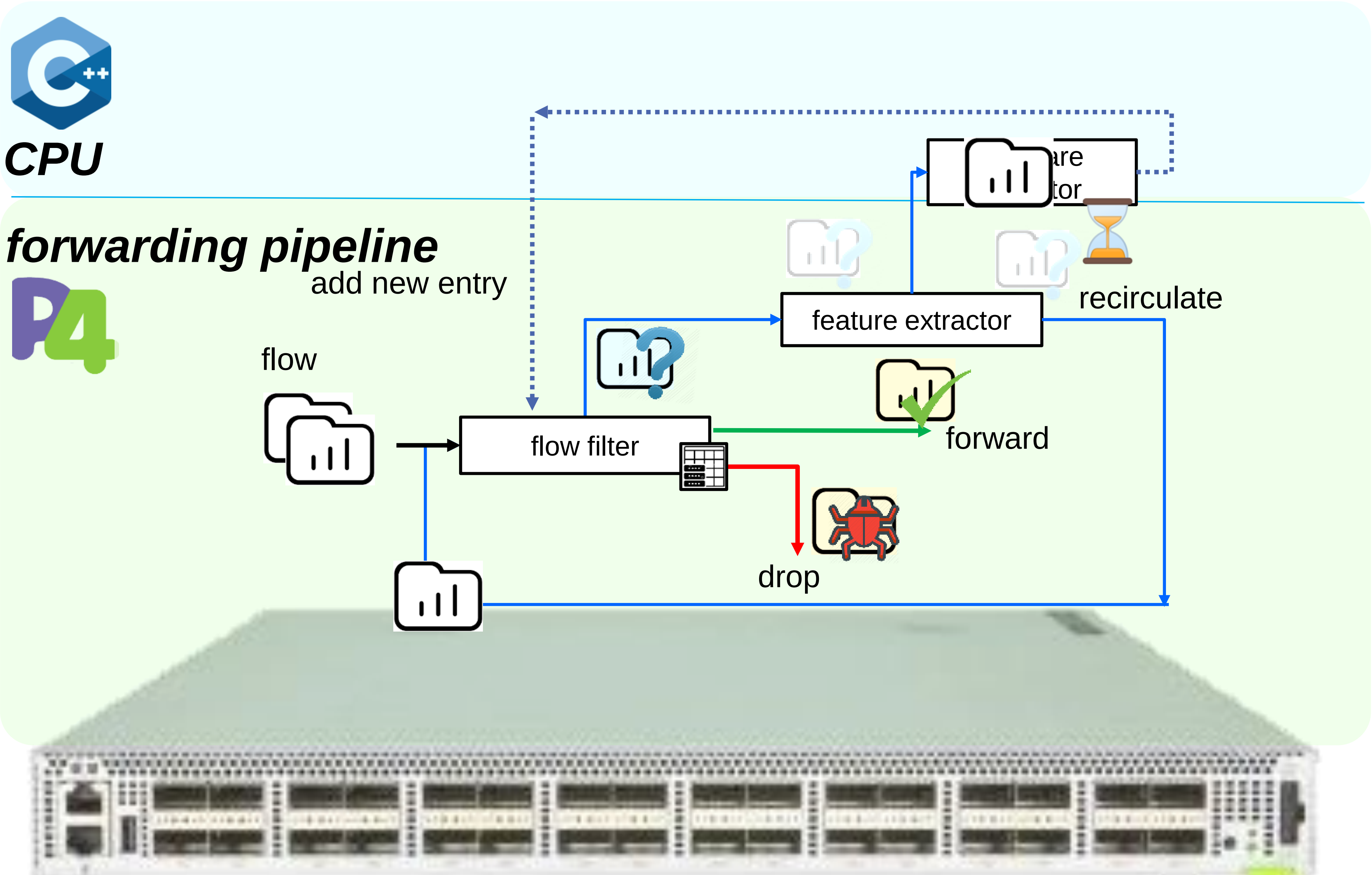
Overview of P4-IPS



Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

flow

flow filter

feature extractor

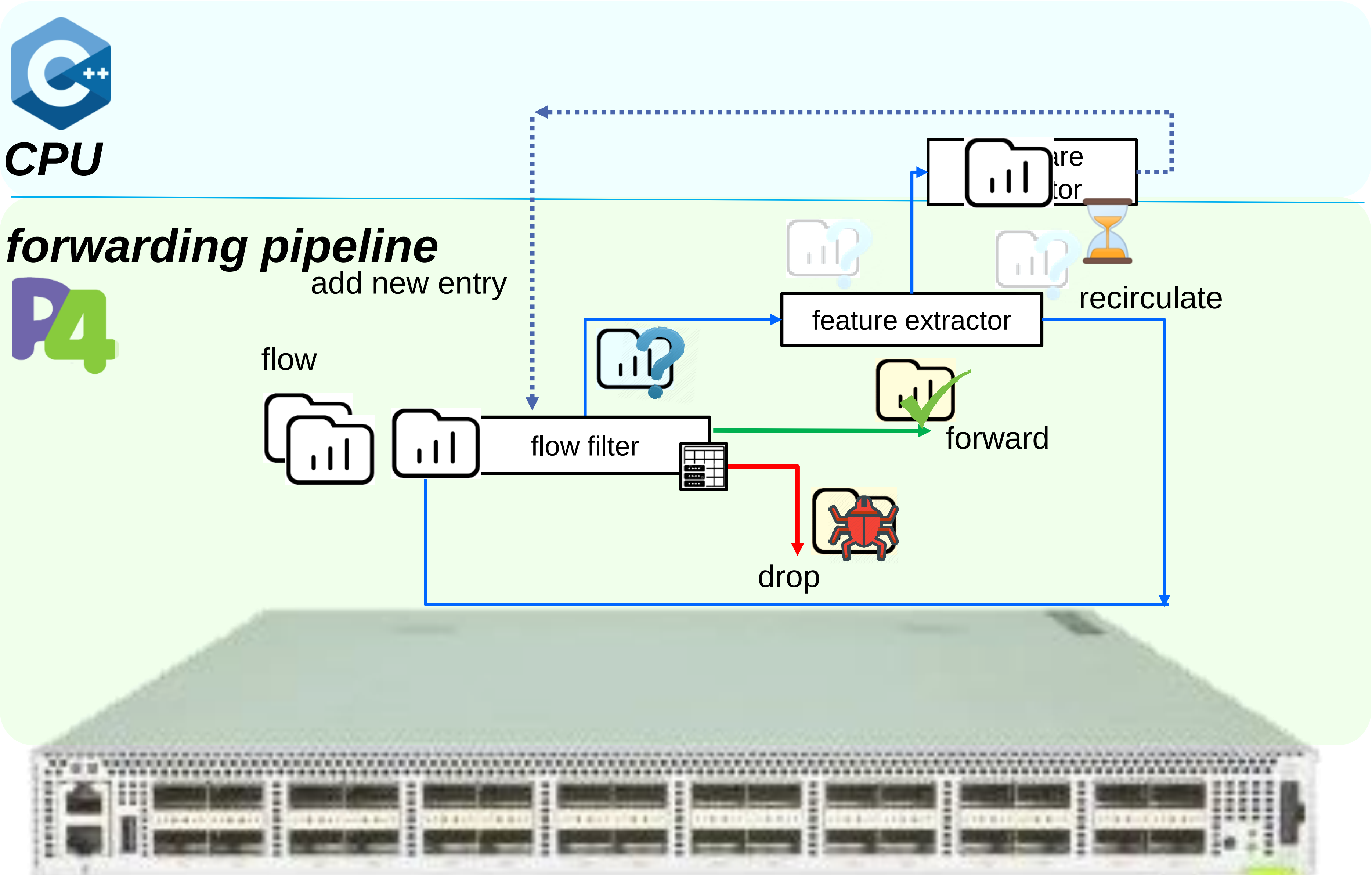
are
tor

recirculate

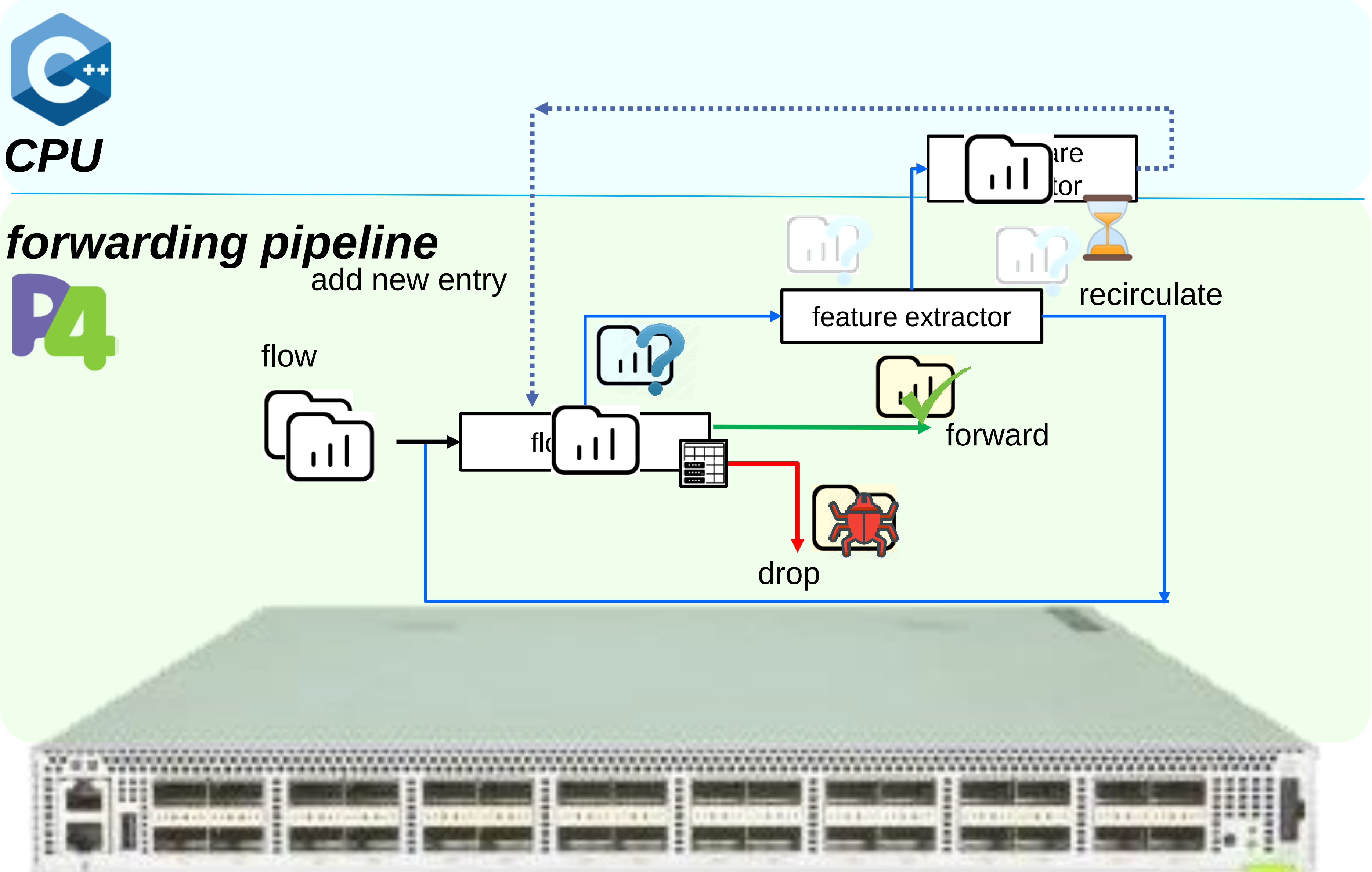
forward

drop

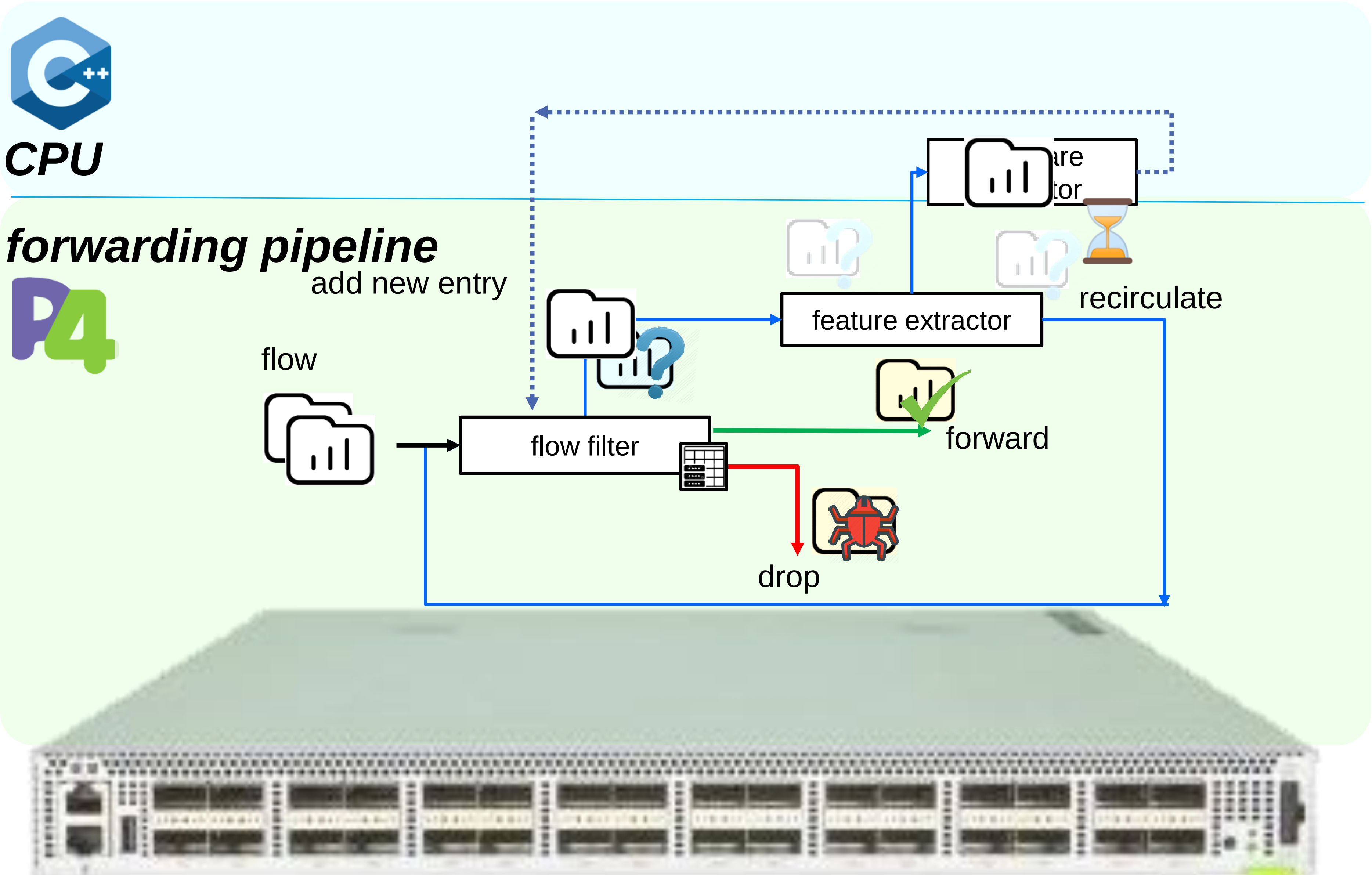
Overview of P4-IPS



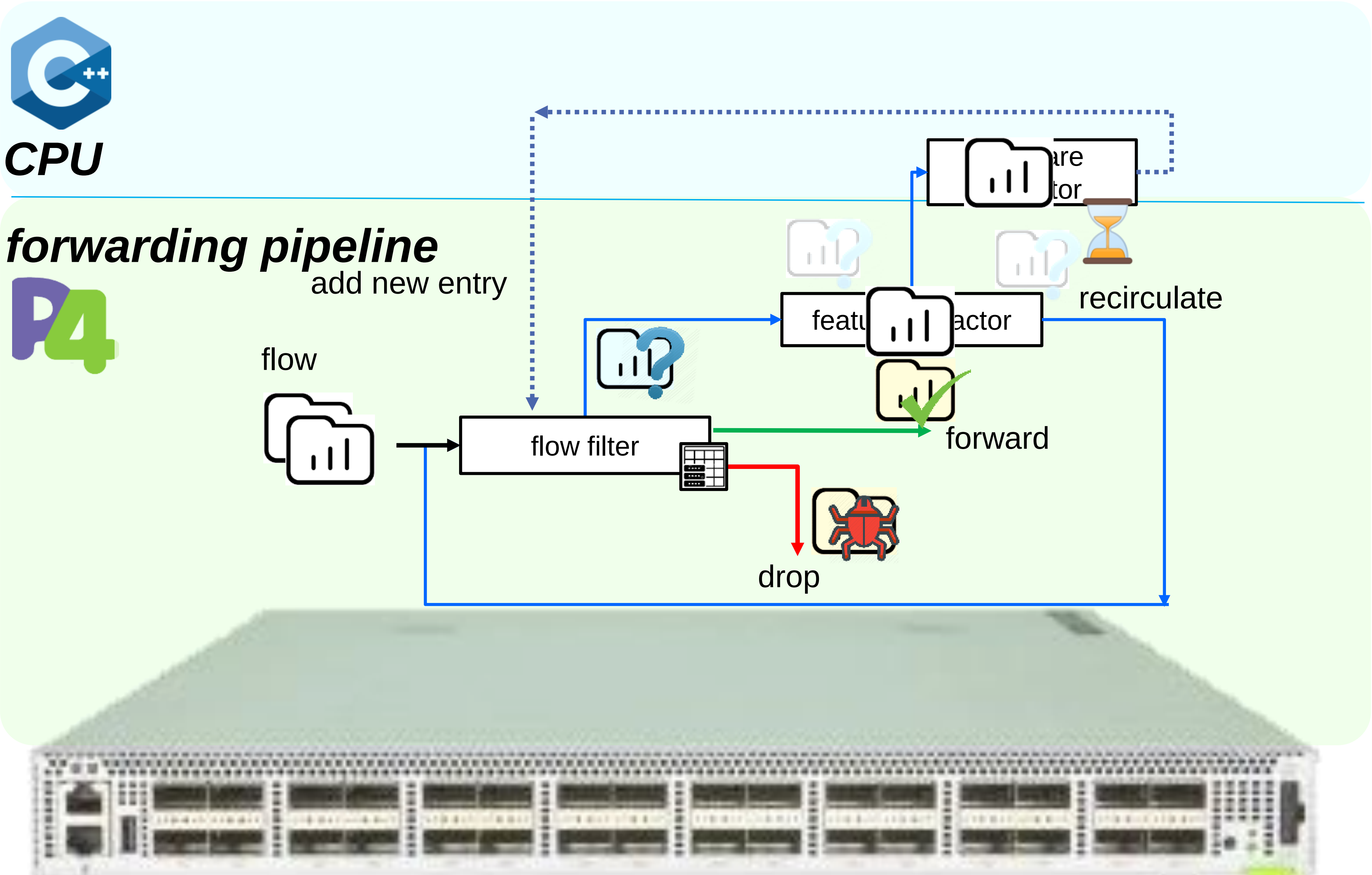
Overview of P4-IPS



Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

flow

flow filter

featu actor

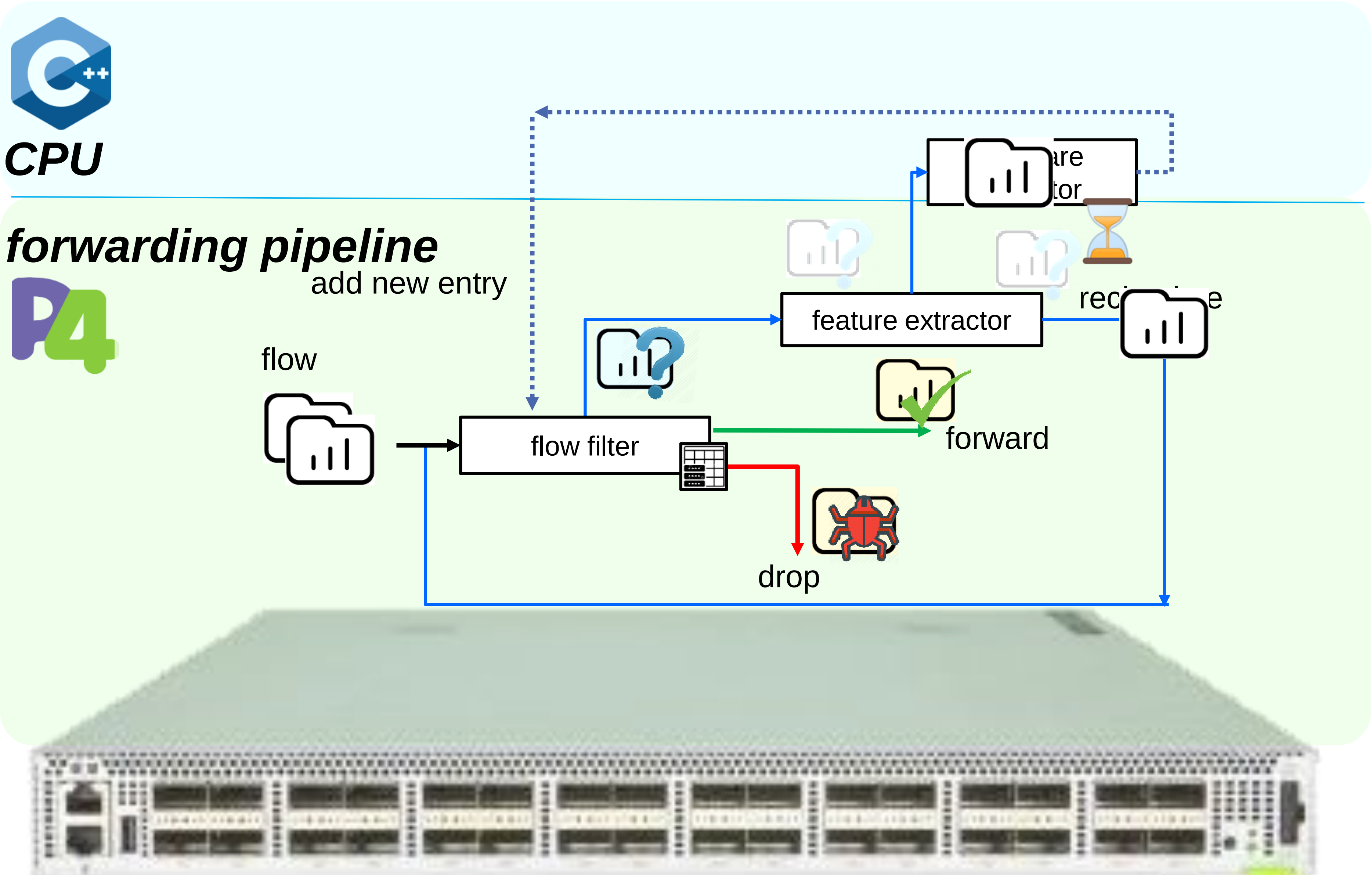
are
tor

recirculate

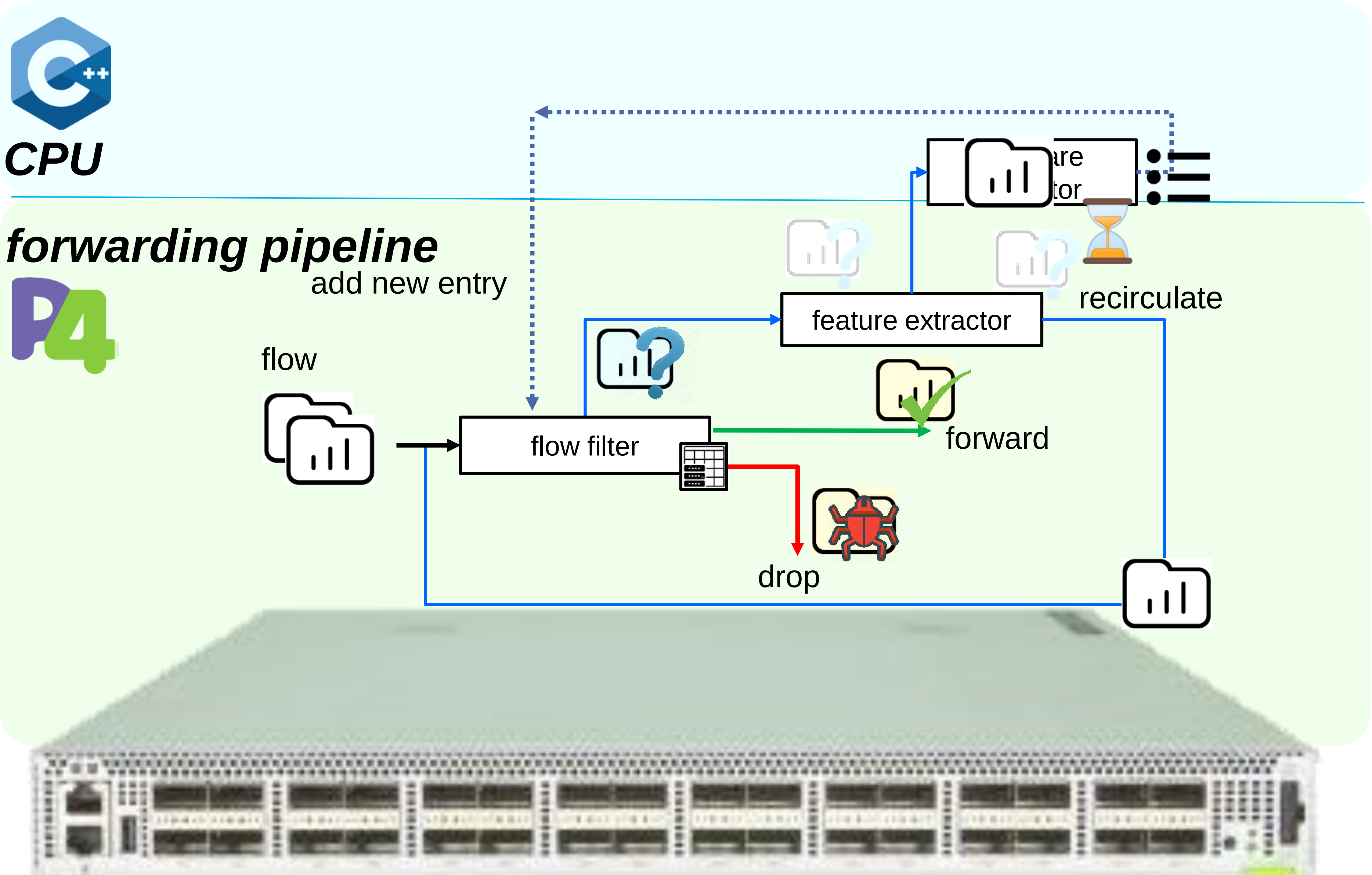
forward

drop

Overview of P4-IPS



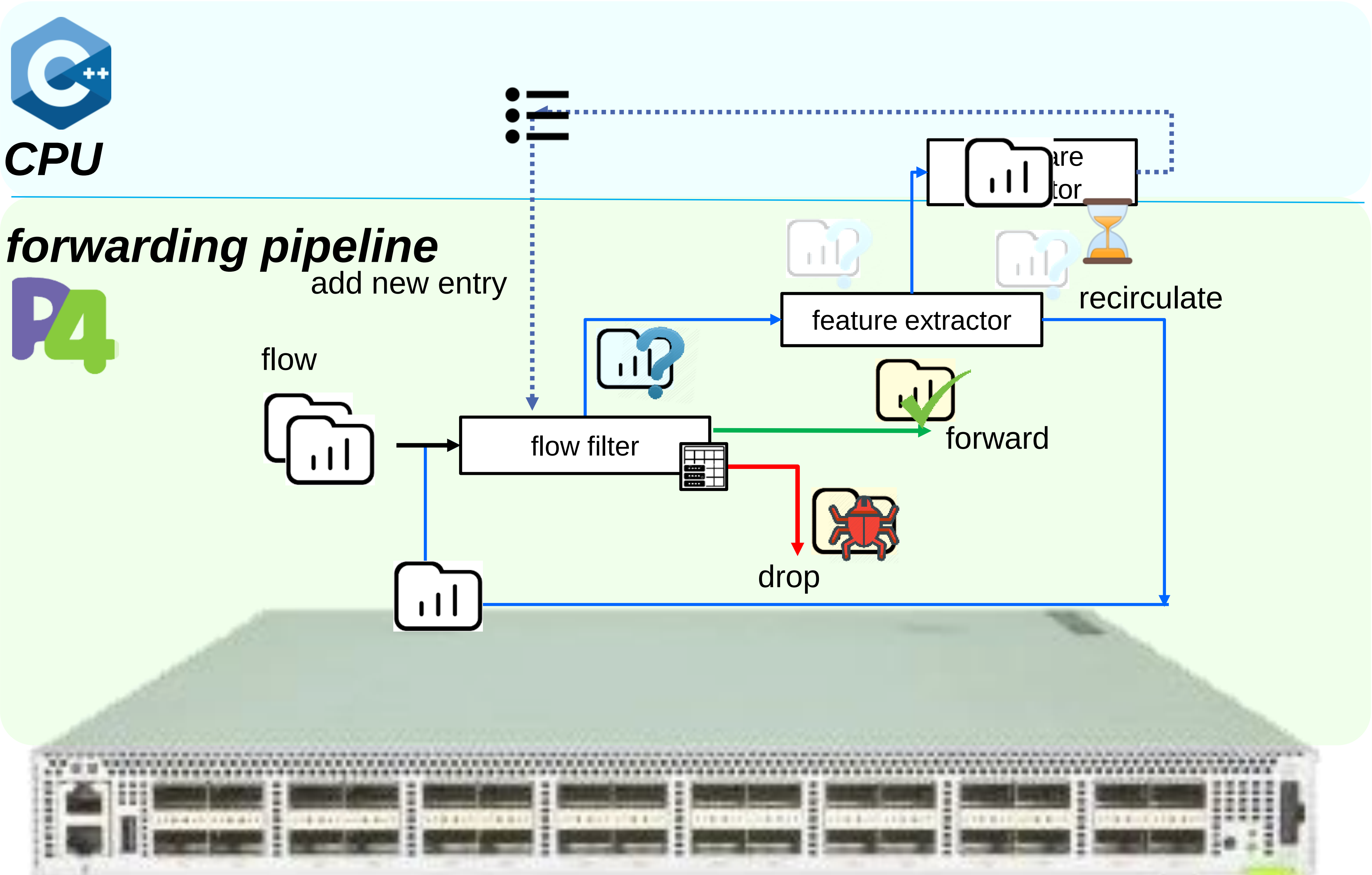
Overview of P4-IPS



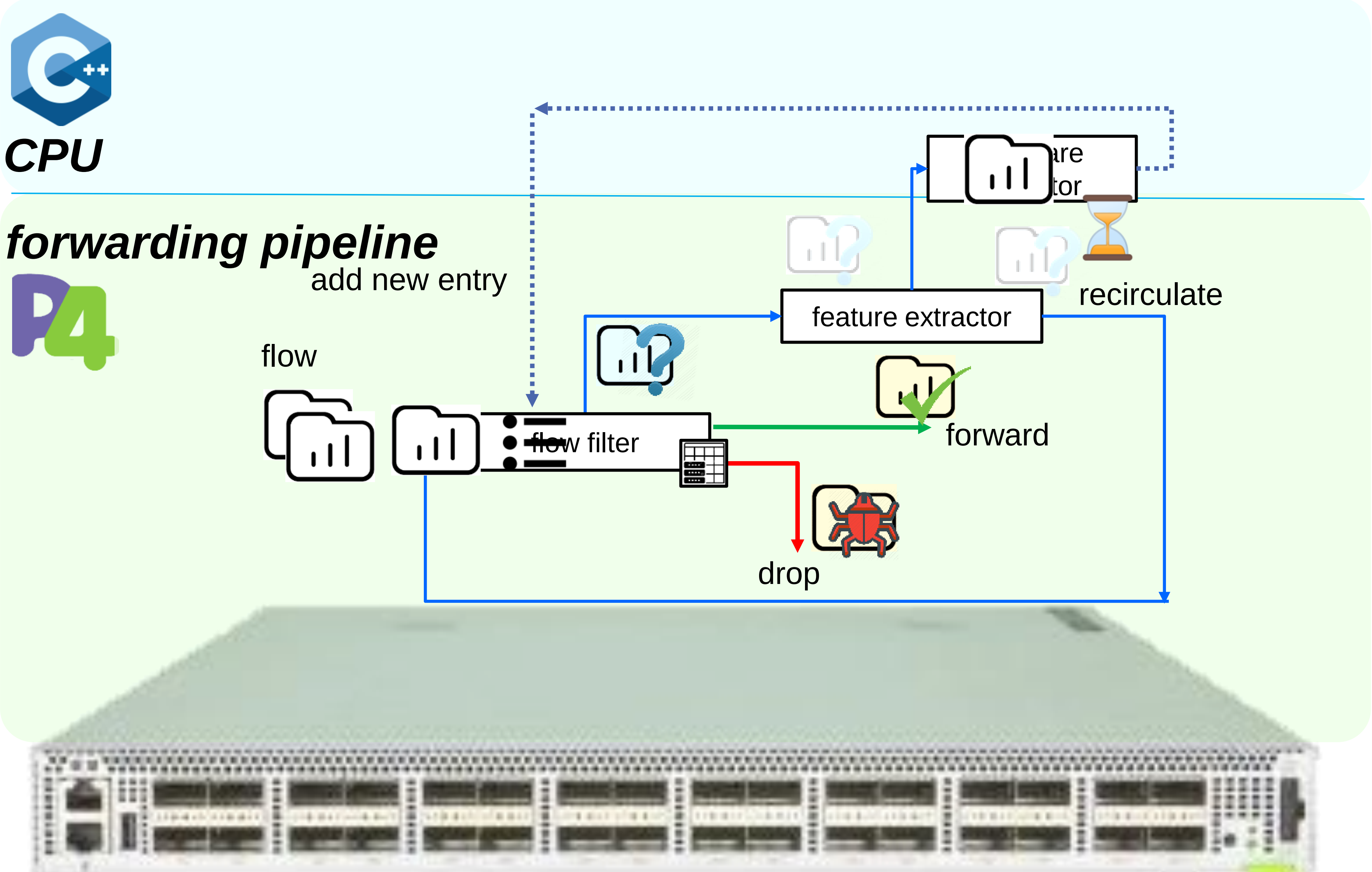
Overview of P4-IPS

國立交通大學
National Chiao Tung University

Edge-corE NETWORKS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

are
tor

recirculate

feature extractor

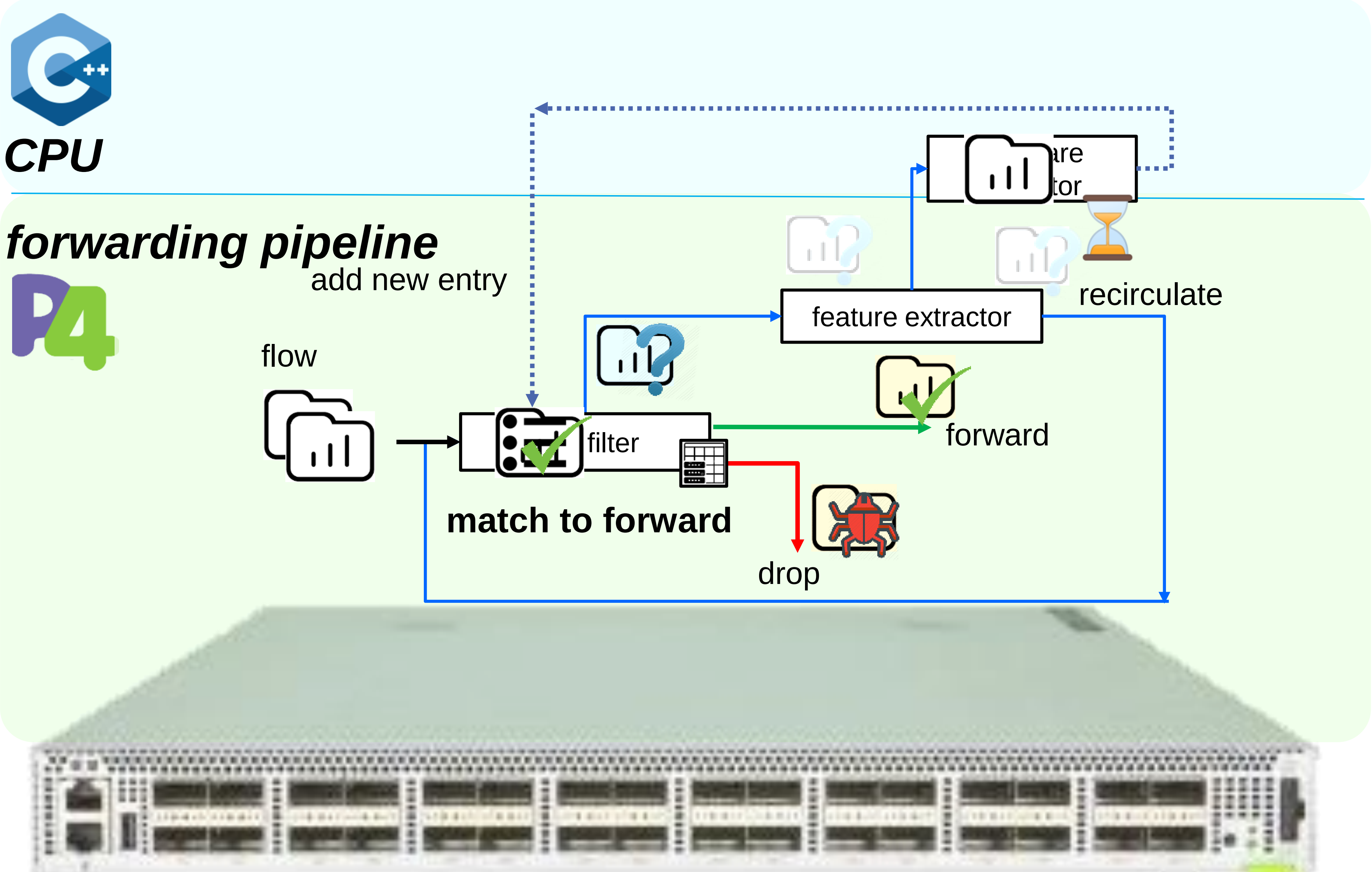
flow

flow filter

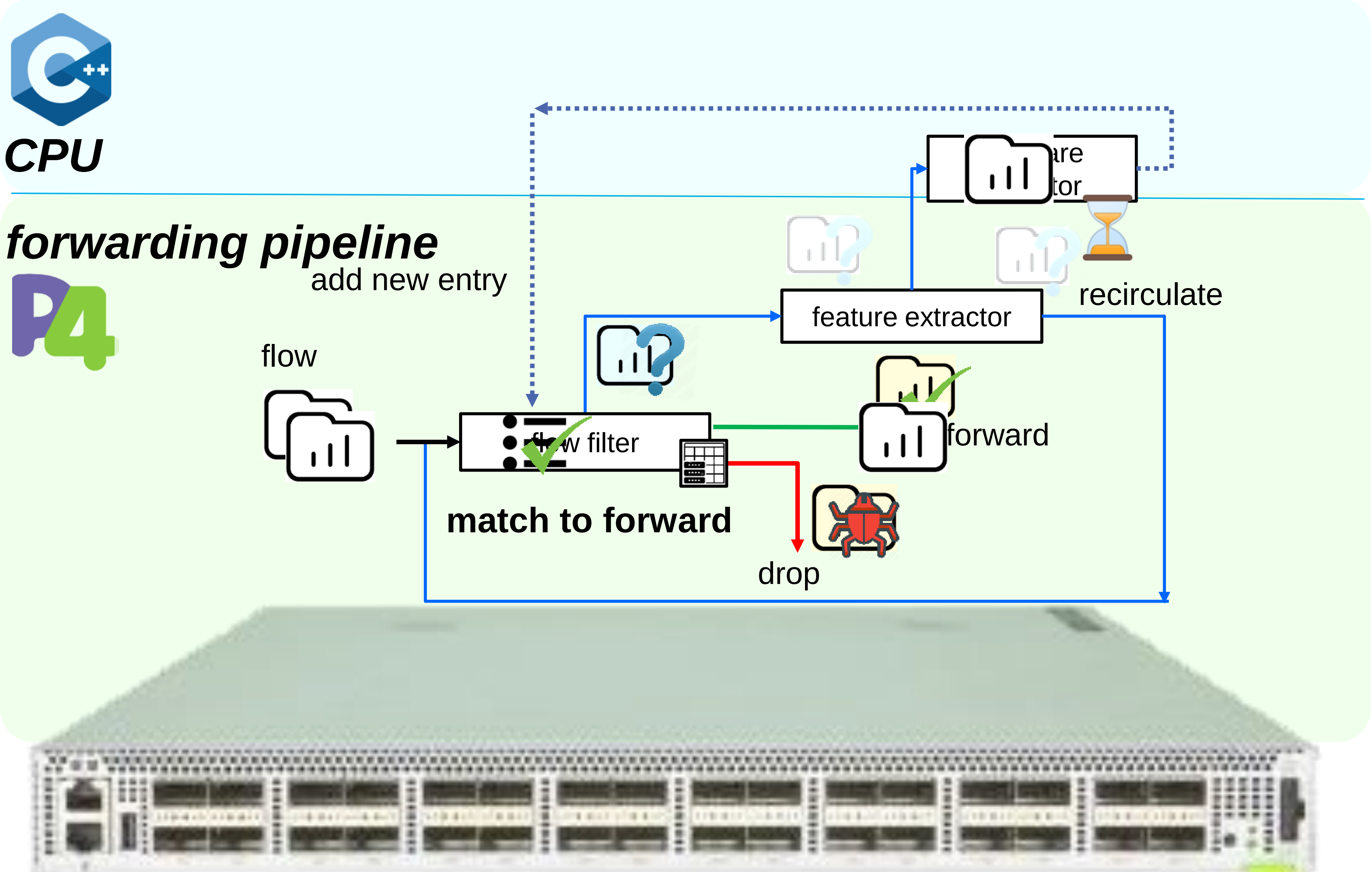
forward

drop

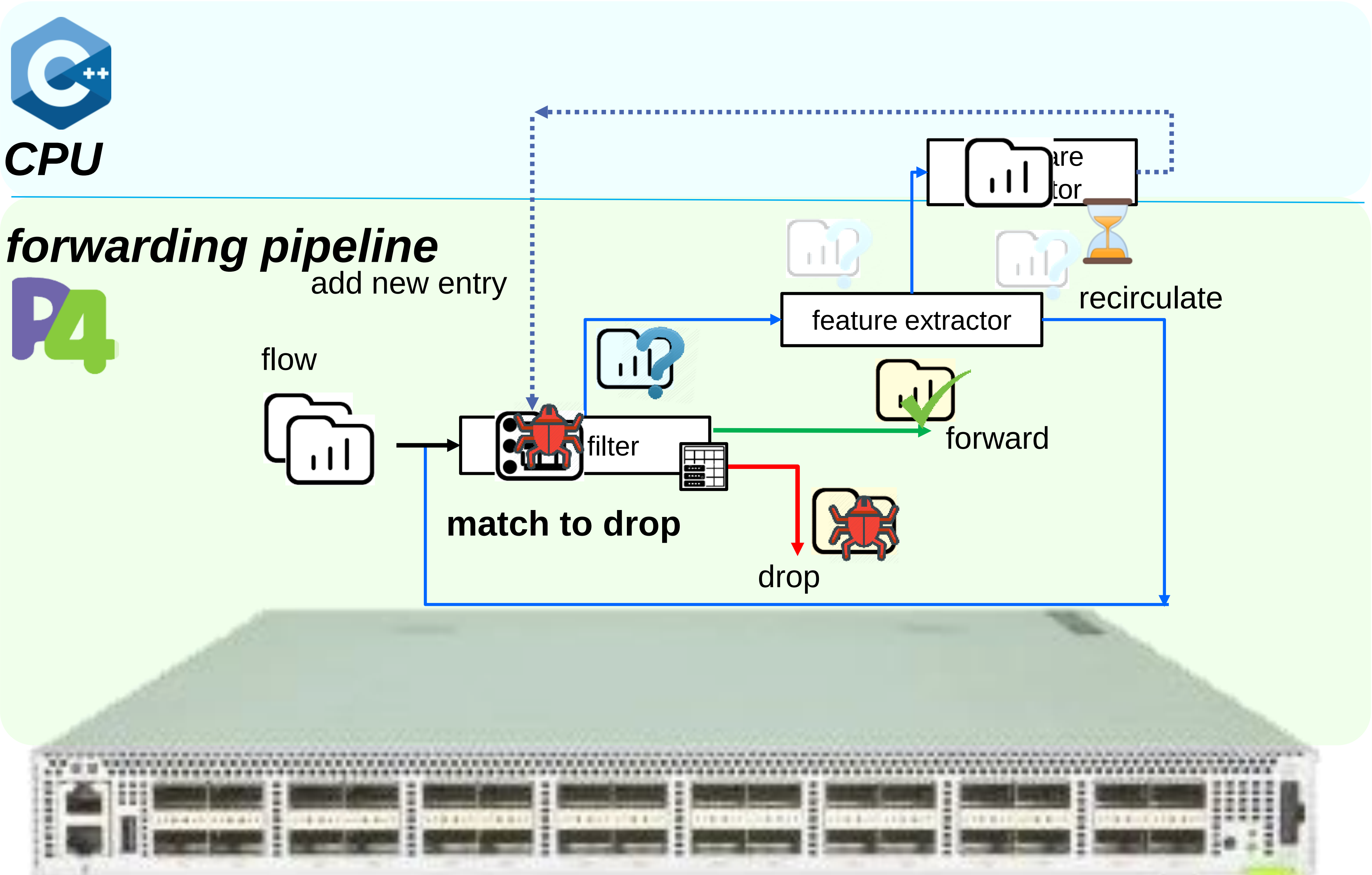
Overview of P4-IPS



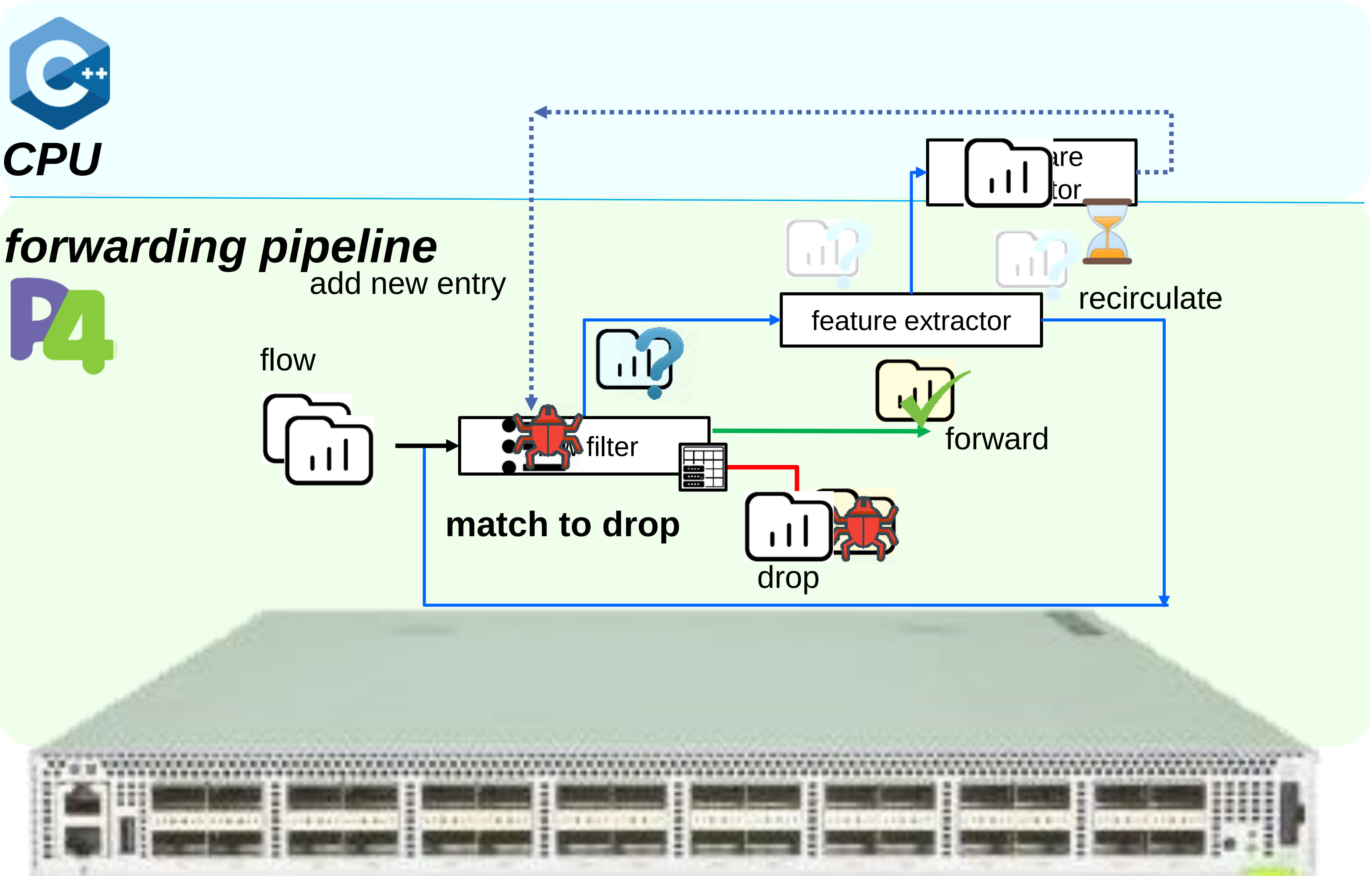
Overview of P4-IPS



Overview of P4-IPS



Overview of P4-IPS



CPU

forwarding pipeline

add new entry

flow

filter

match to drop

feature extractor

are
tor

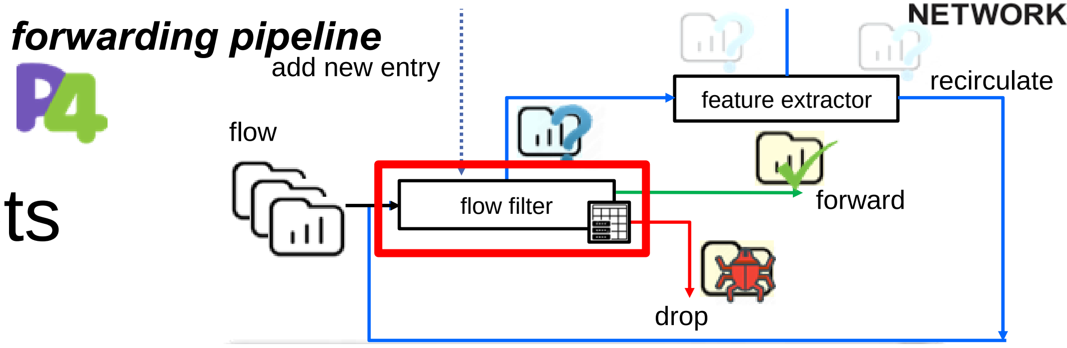
recirculate

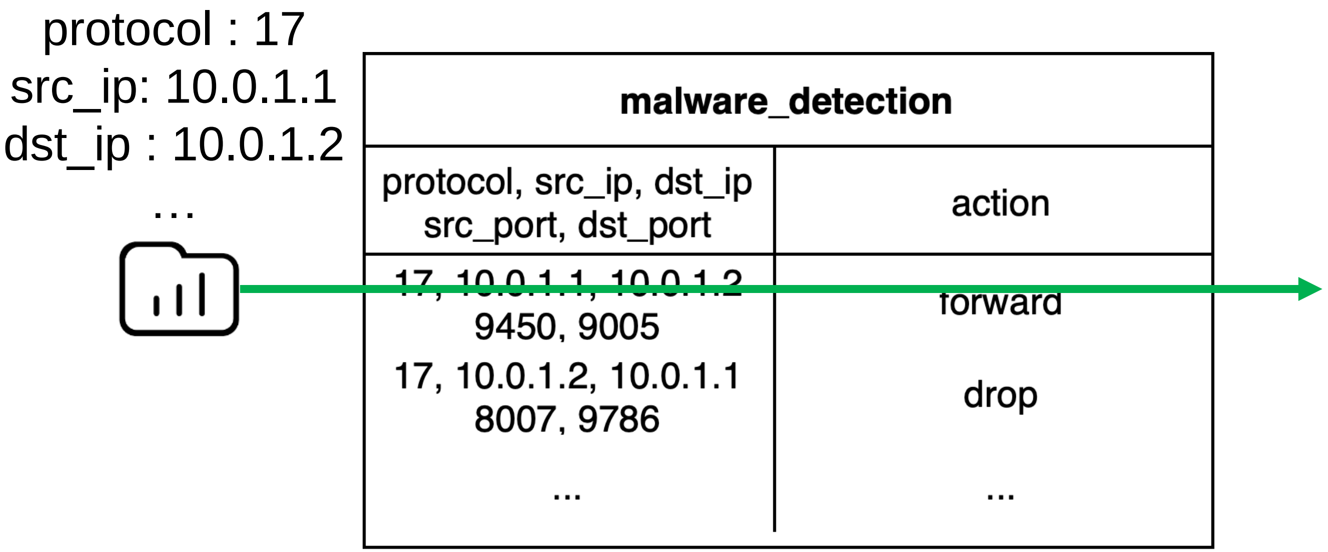
forward

drop

Flow Filtering

- Malware Detection Table
  - determine to drop/forward packets
  - key: five tuple
  - action : **forward** or drop

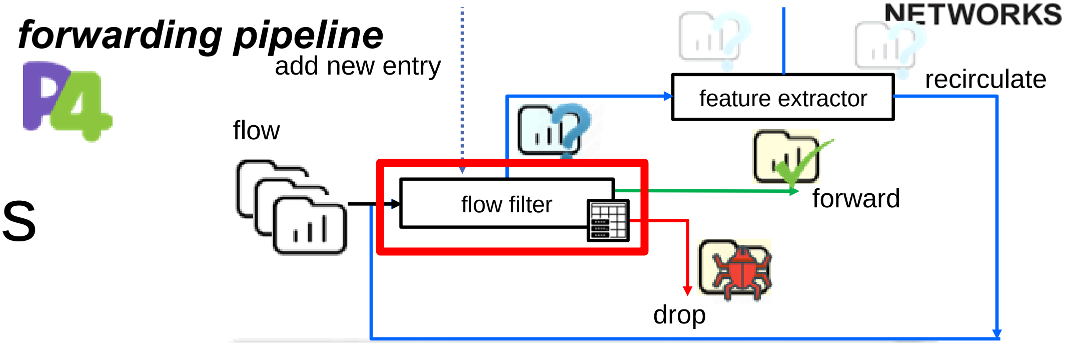


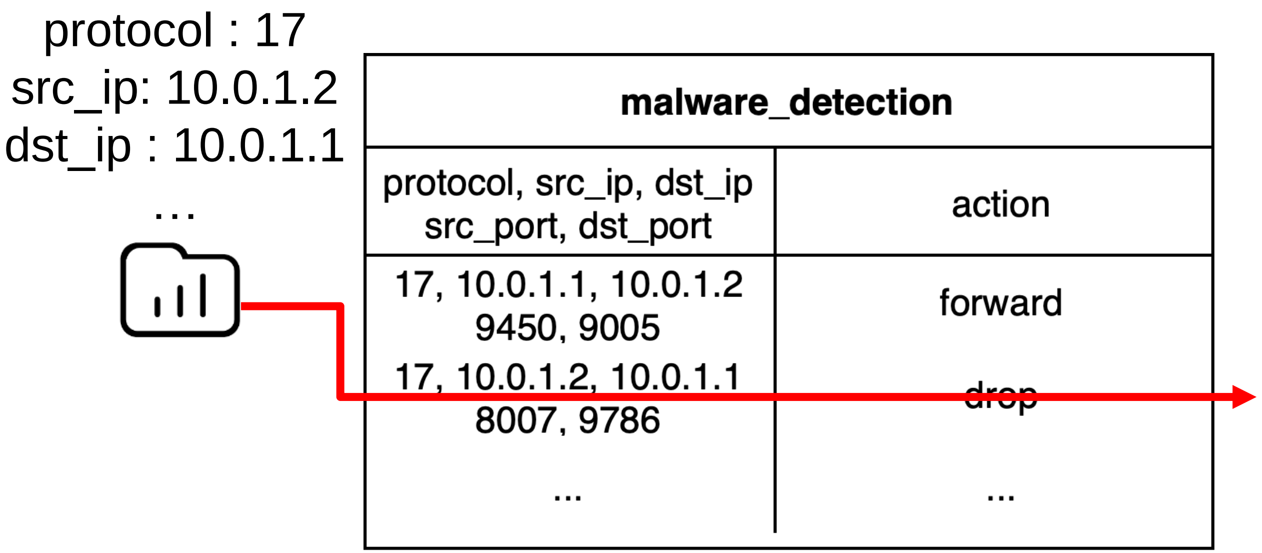


malware_detection	
protocol, src_ip, dst_ip src_port, dst_port	action
17, 10.0.1.1, 10.0.1.2 9450, 9005	forward
17, 10.0.1.2, 10.0.1.1 8007, 9786	drop
...	...

Flow Filtering

- Malware Detection Table
  - determine to drop/forward packets
  - key: five tuple
  - action : forward or **drop**

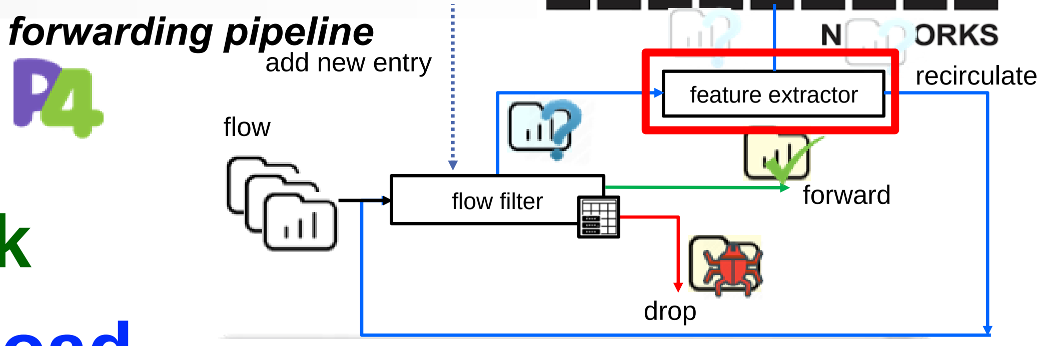


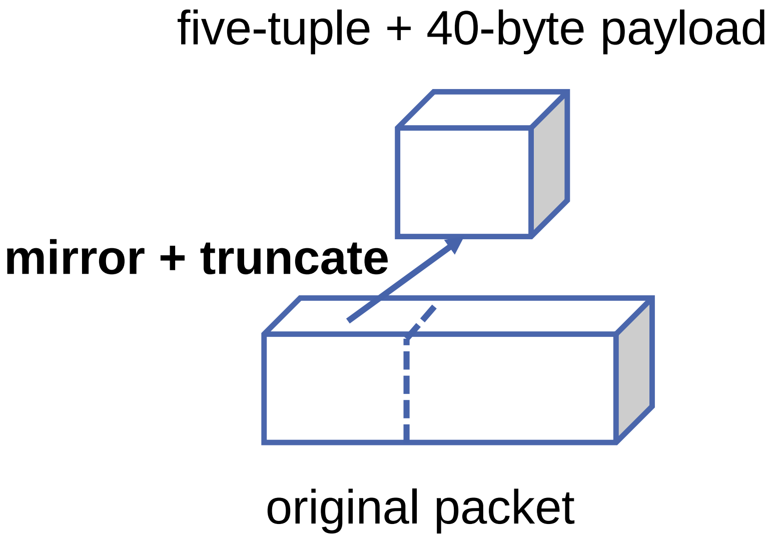


malware_detection	
protocol, src_ip, dst_ip src_port, dst_port	action
17, 10.0.1.1, 10.0.1.2 9450, 9005	forward
17, 10.0.1.2, 10.0.1.1 8007, 9786	drop
...	...

Feature Extractor

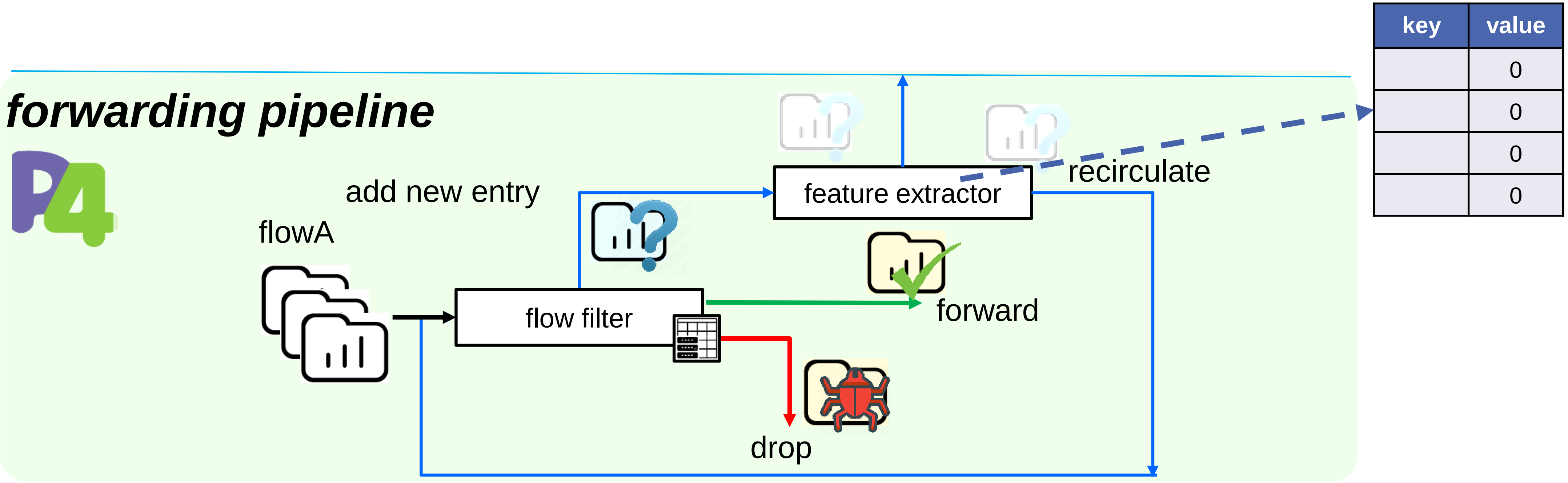
- Mirror function
  - extract features for **Neural Network**
  - features: **five-tuple** + **40-byte payload**
  - processed by **P4 forwarding pipeline**





Feature Extractor

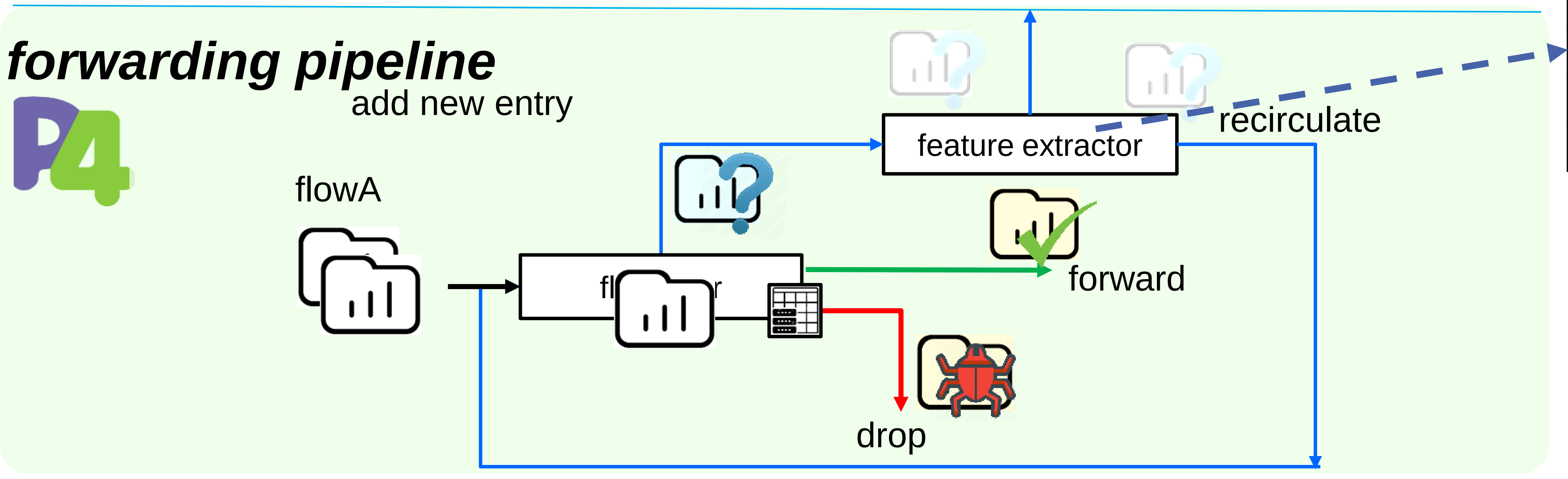
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
	0
	0
	0
	0

Feature Extractor

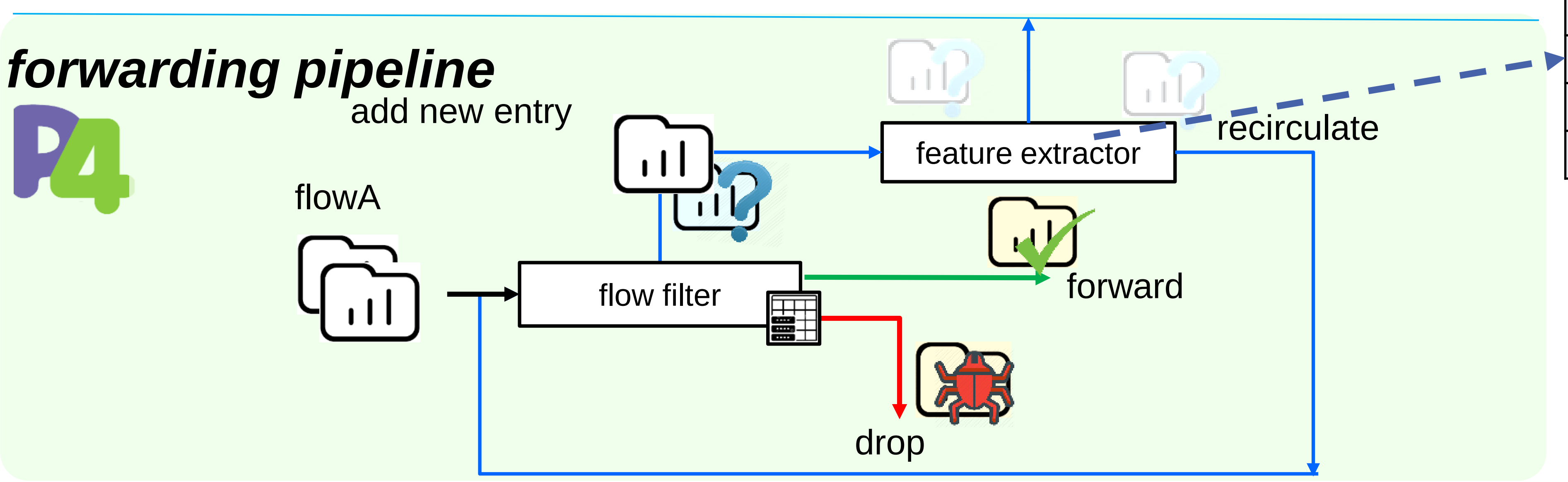
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
	0
	0
	0
	0

Feature Extractor

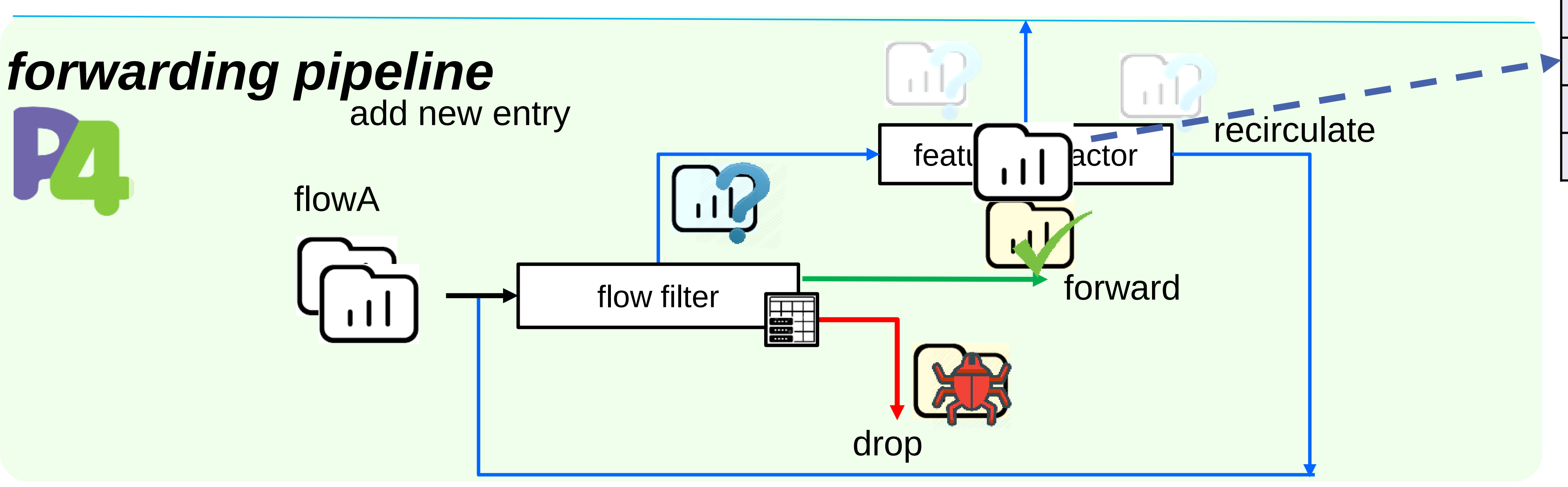
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
	0
	0
	0
	0

Feature Extractor

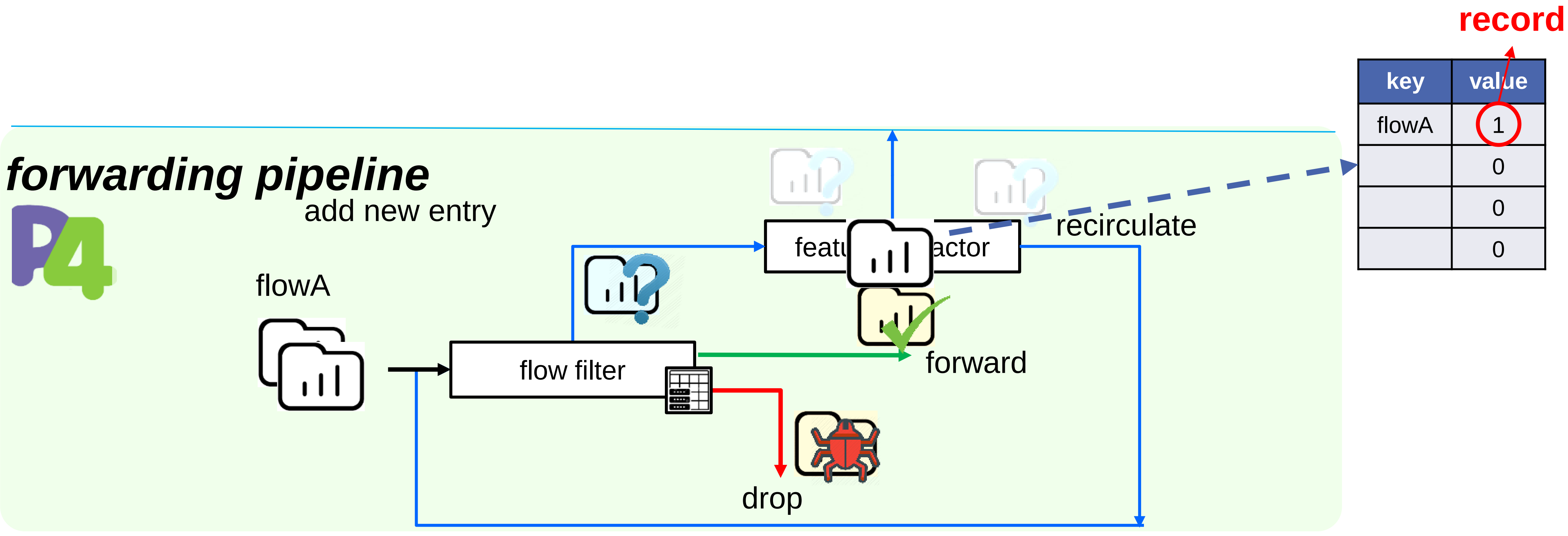
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
	0
	0
	0
	0

Feature Extractor

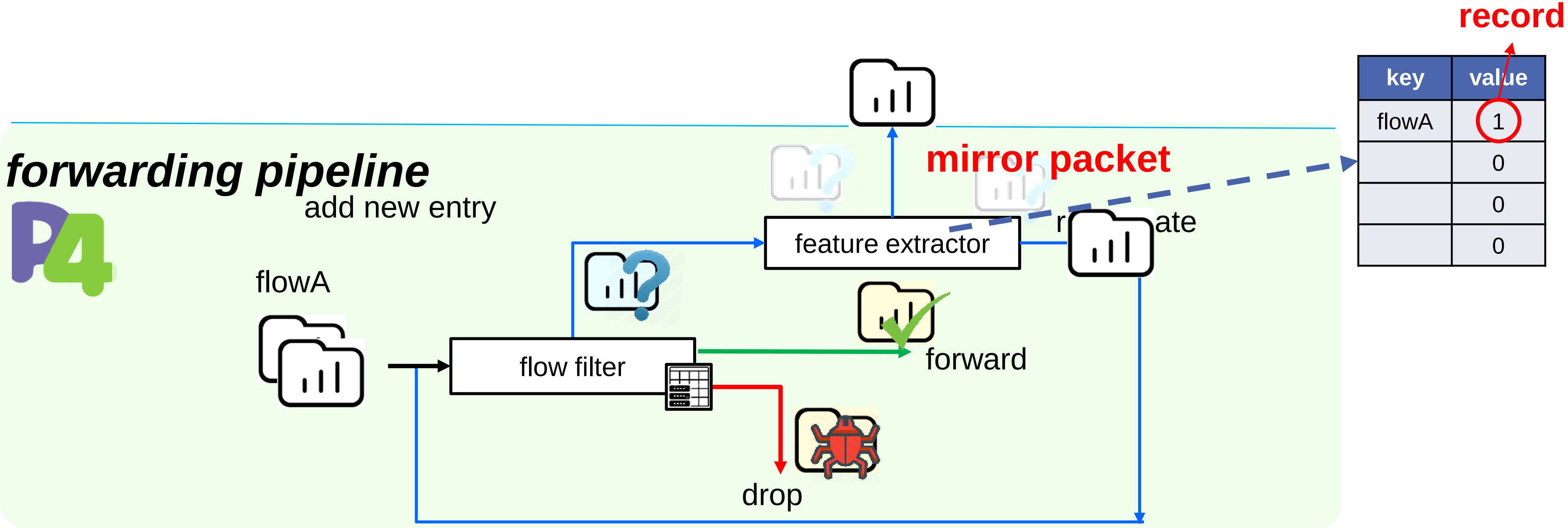
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

Feature Extractor

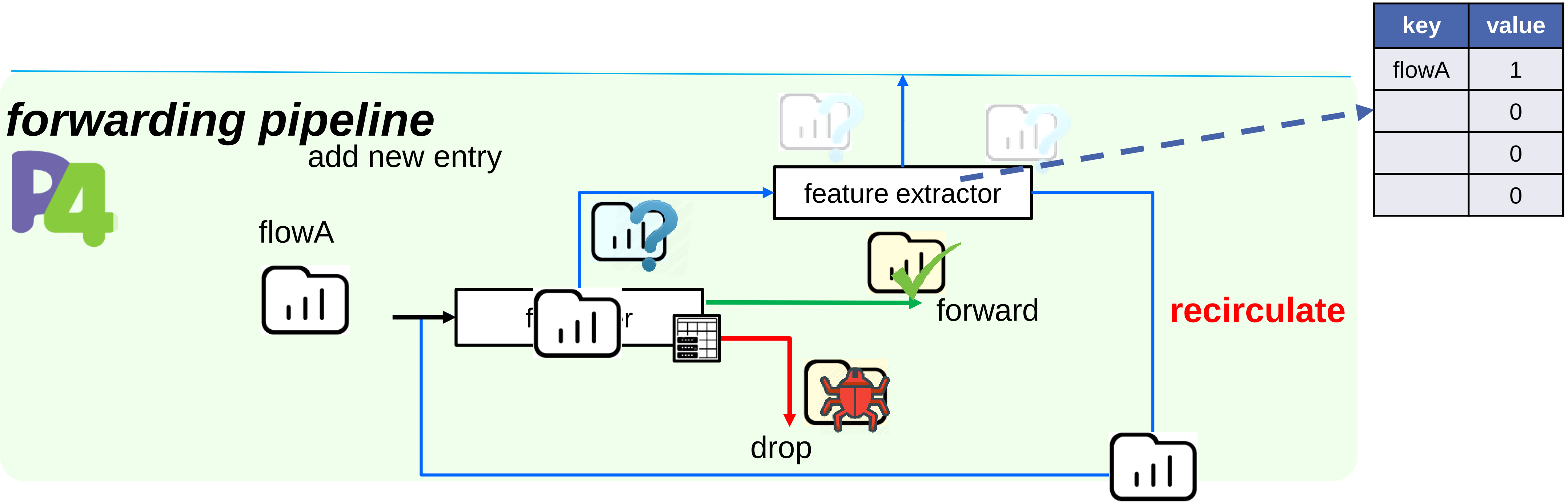
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

Feature Extractor

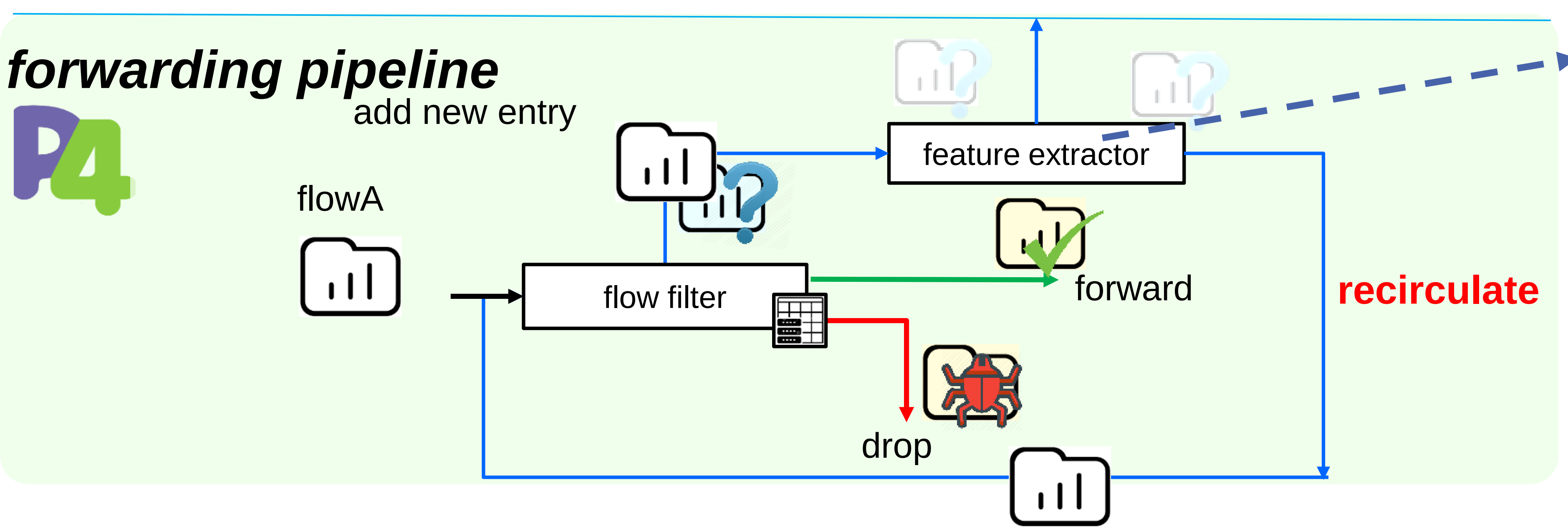
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

Feature Extractor

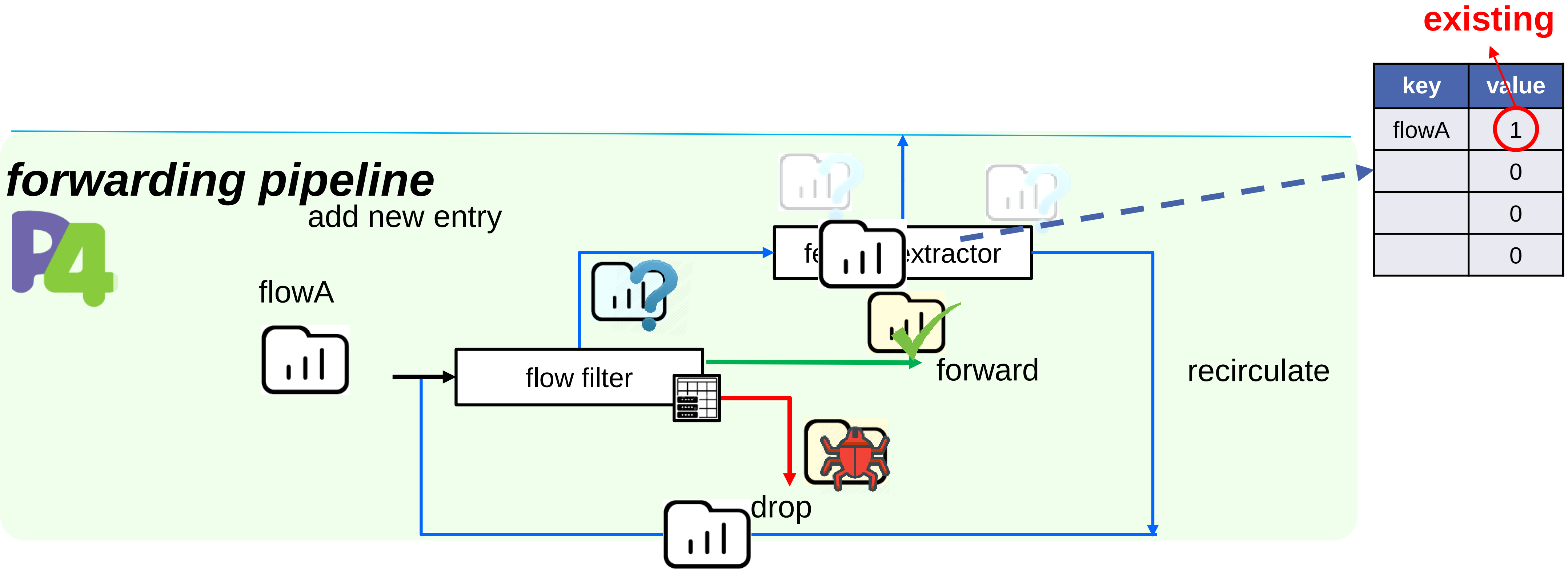
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

Feature Extractor

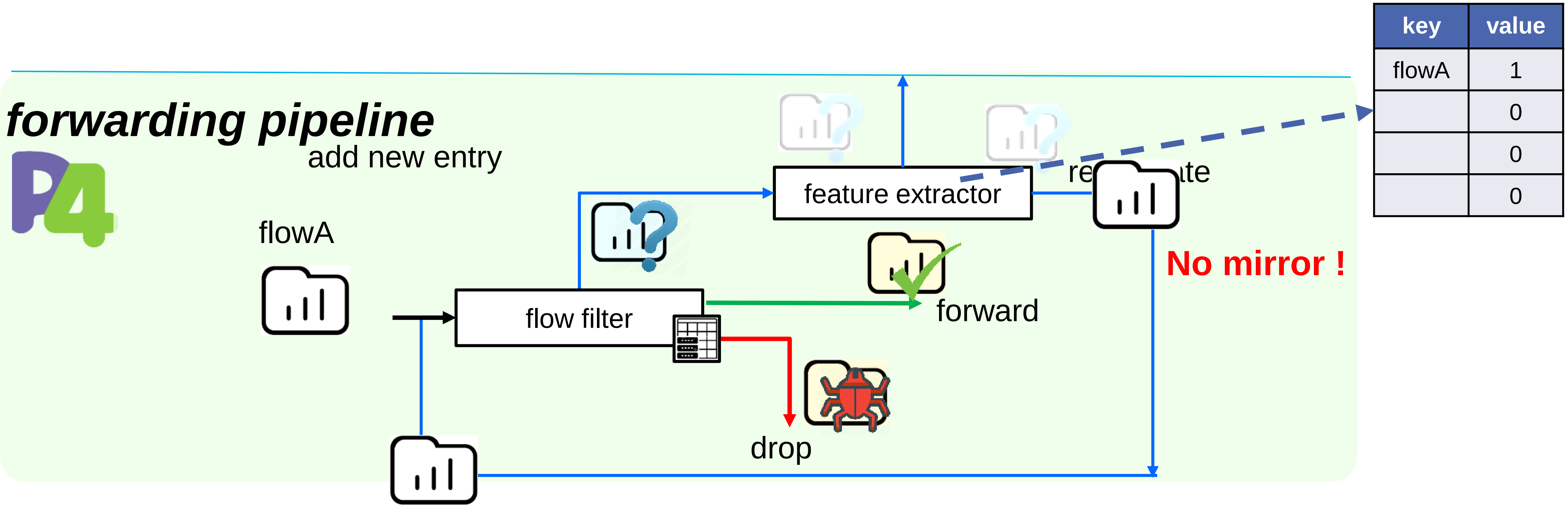
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

Feature Extractor

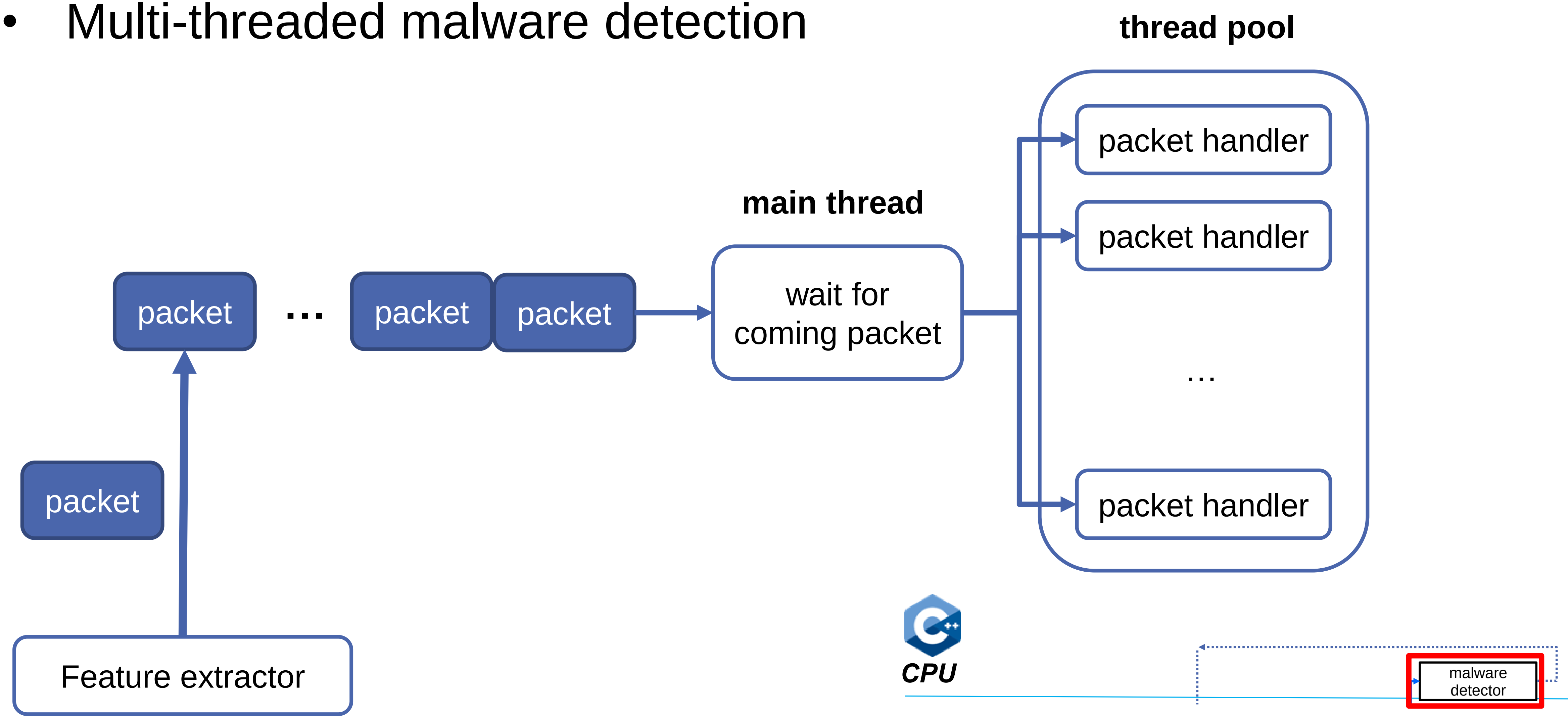
- Prevent **multiple run** of malware detection for one flow
  - extract/send features from the first packet



key	value
flowA	1
	0
	0
	0

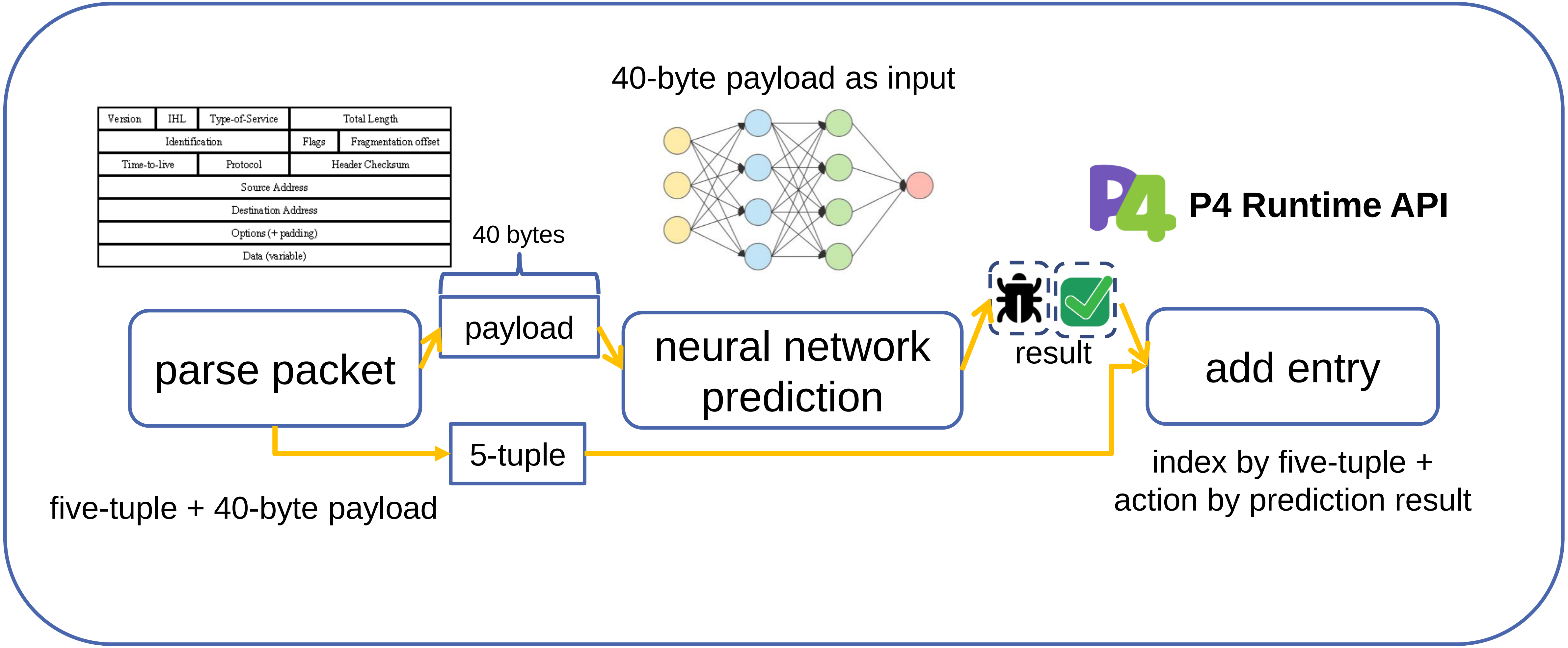
Malware Detector

- Multi-threaded malware detection



Packet Handler

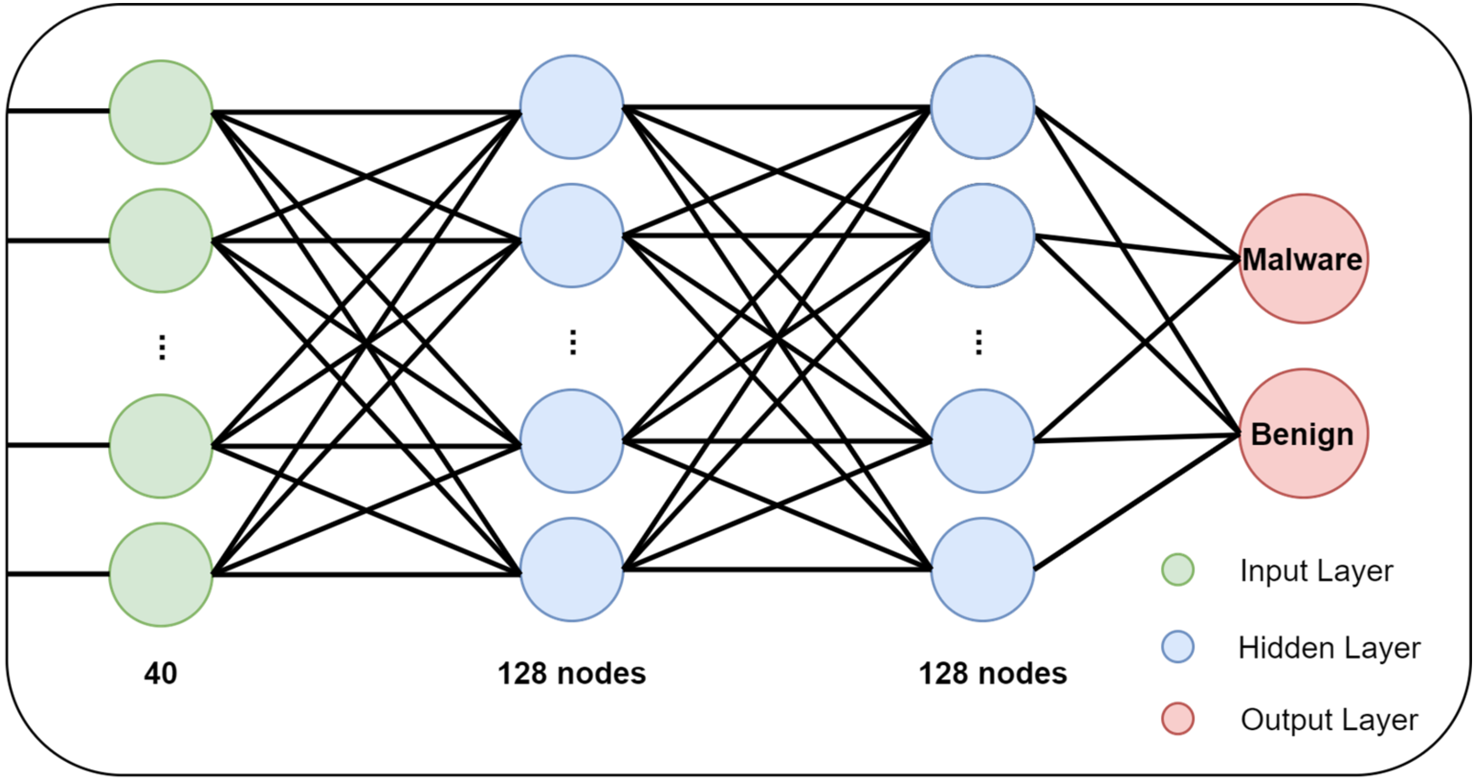
Packet handler



Version	IHL	Type-of-Service	Total Length	
Identification			Flags	Fragmentation offset
Time-to-live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options (+ padding)				
Data (variable)				

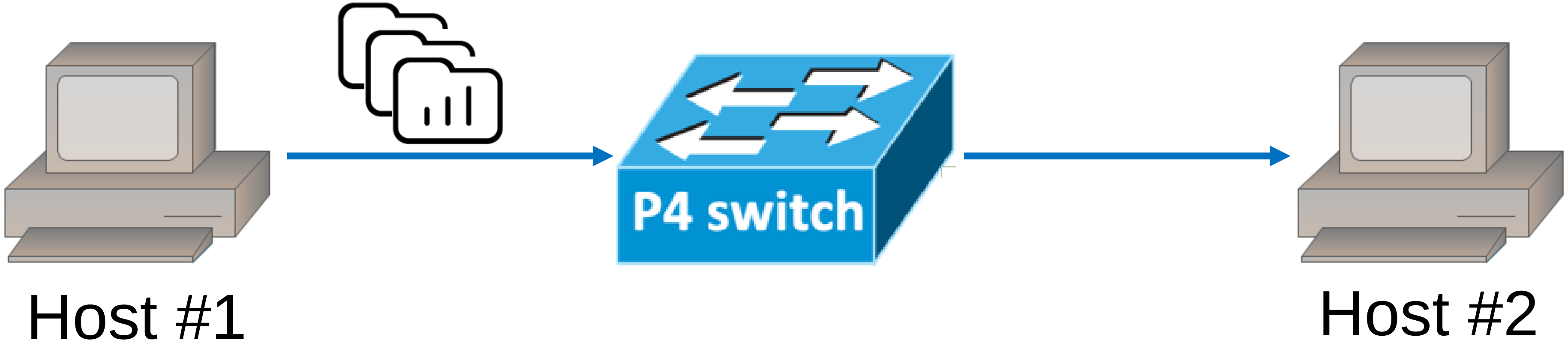
Neural Network Model

- Two hidden layers + 128 nodes per layer
- **resource optimized** + **fast computing**



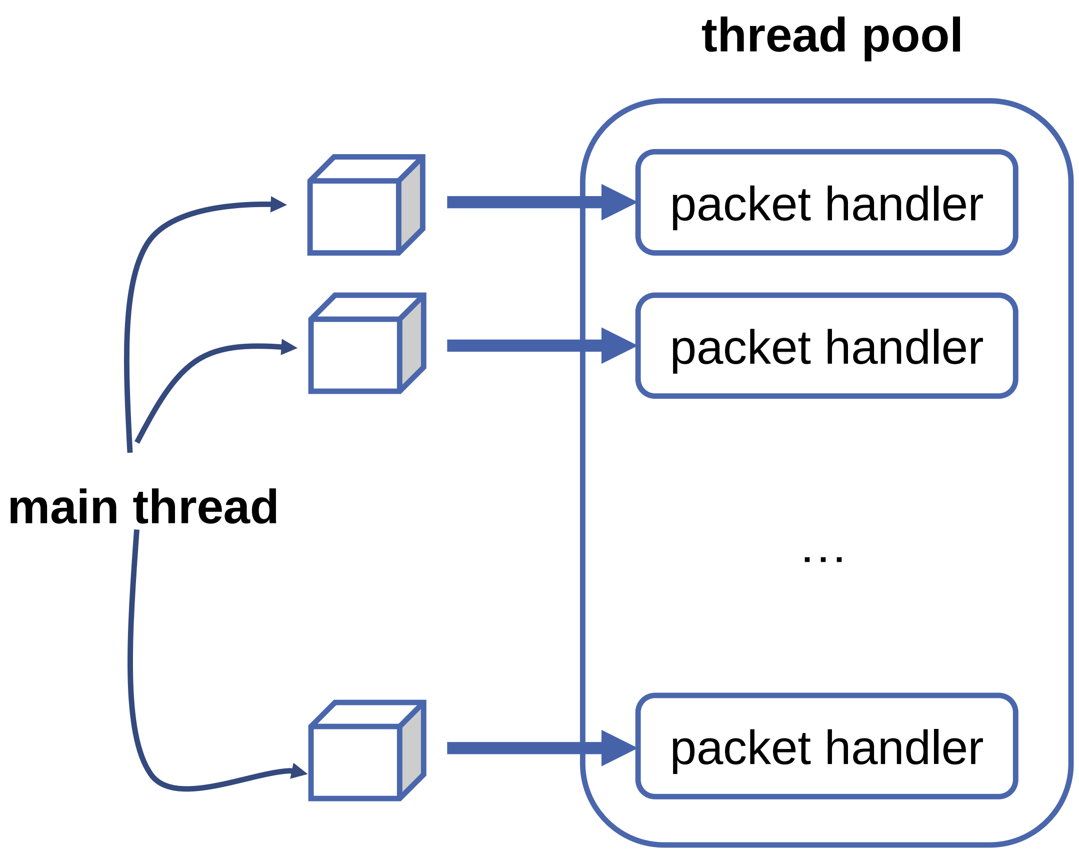
Evaluation Setting

- Host #1 works as sender
  - ”tcpreplay” sends flows from pcap



Evaluation Result

- P4 Switch CPU with 4 cores (2 threads per core)
- 3.17X faster than single thread

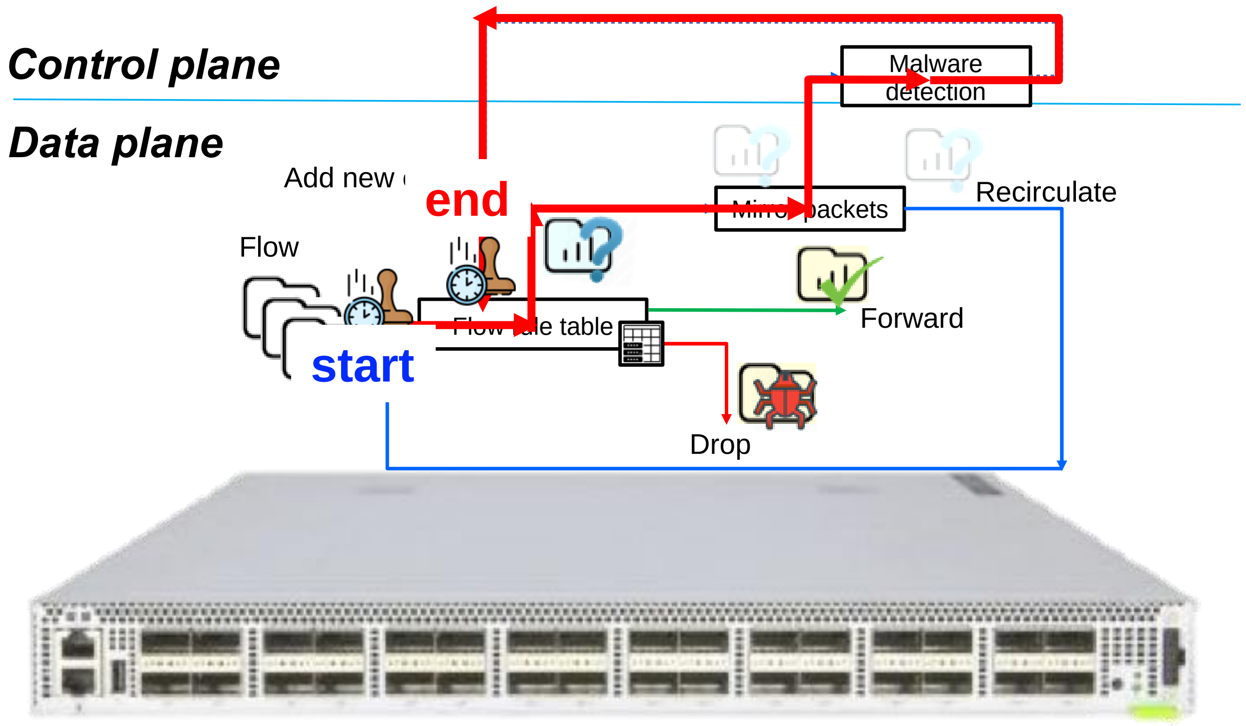


thread	flow/s
1	2950
2	2975
3	5649
4	7353
5	7752
6	8196
7	8849
8	9345

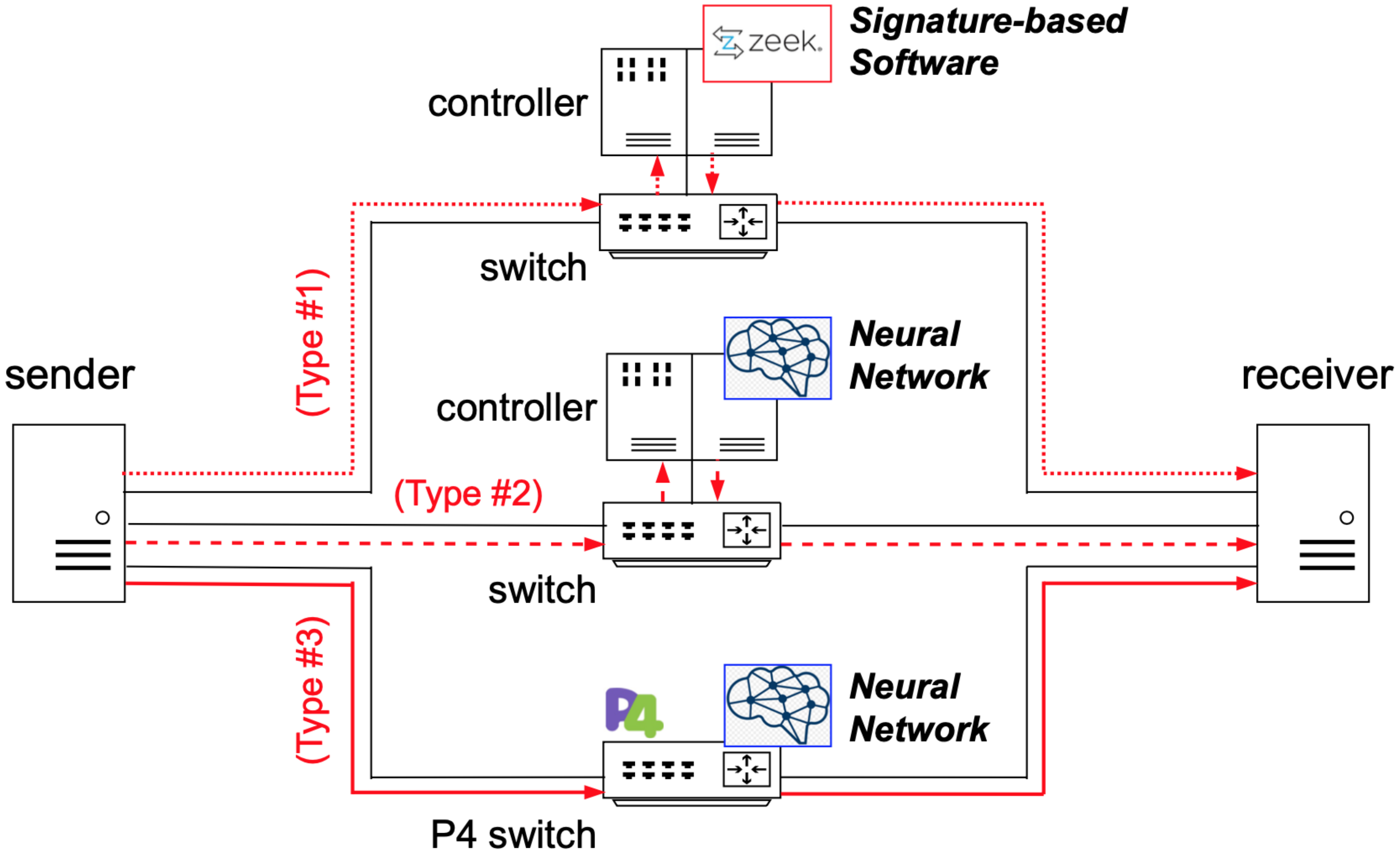
3.17x

Evaluation Setting

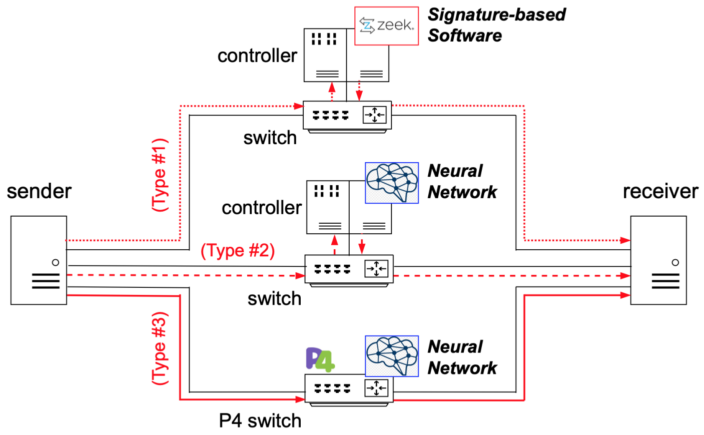
- Measure response time
  - **start** from packet coming into P4 switch
  - **end** as determining packet action (forward or drop)



Comparison of 3 IPS



Evaluation Result



Type #1: Signature-based IPS on external server
Type #2: SDN-based ML-IPS on external server
Type #3: ML-IPS on P4 switch (P4-IPS)

	Type #1	Type #2	P4-IPS
response time (ms)	119.63	51.19	0.34 (single thread)
processing capability (flow/s)	2	17	9345 (8 threads)

Conclusion

- P4 switch provides **in-switch computing** to overcome disadvantages of traditional software-based IDS, meanwhile reducing **communication overhead** to external server

- Evaluation results
  - response time: **353X** faster than other solutions
  - processing capability: **4672X** better than other solutions