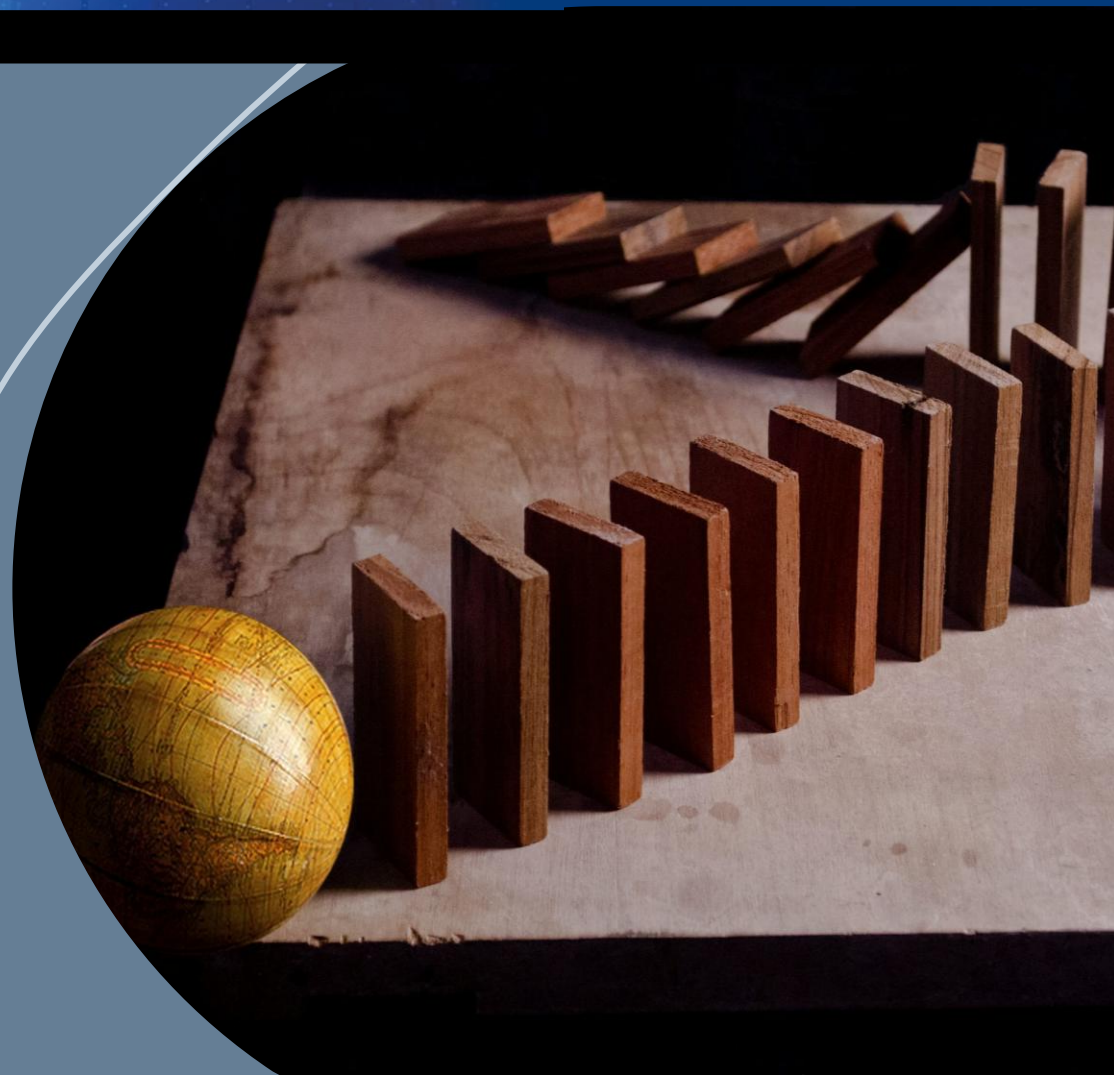
Understanding Per-Stream Filtering and Policing

- Configuration, Capabilities, and Limitations

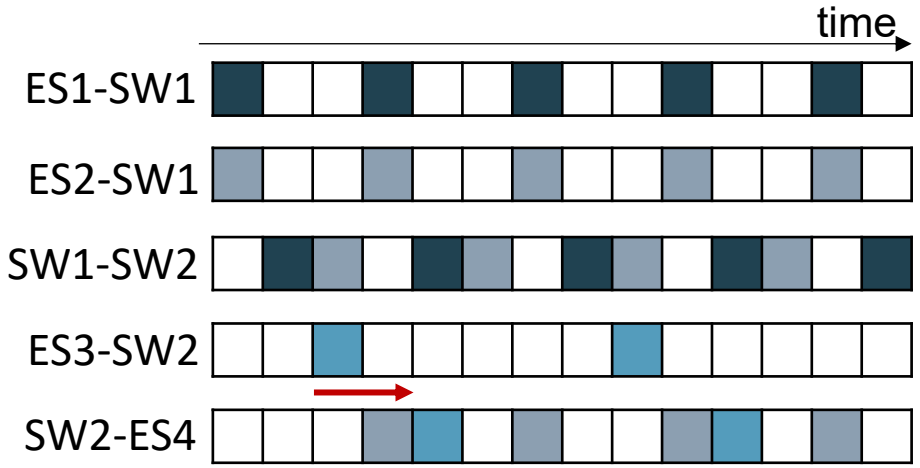
Prof. Dr. Lisa Maile, Technische Universiteit Eindhoven (Speaker)
Prof. Dr. Nicolas Navet, Uni. Luxembourg & Cognifyer (Speaker)
Dr. Marc Boyer, ONERA
Leo Séguin, RealTime-at-Work (RTaW)



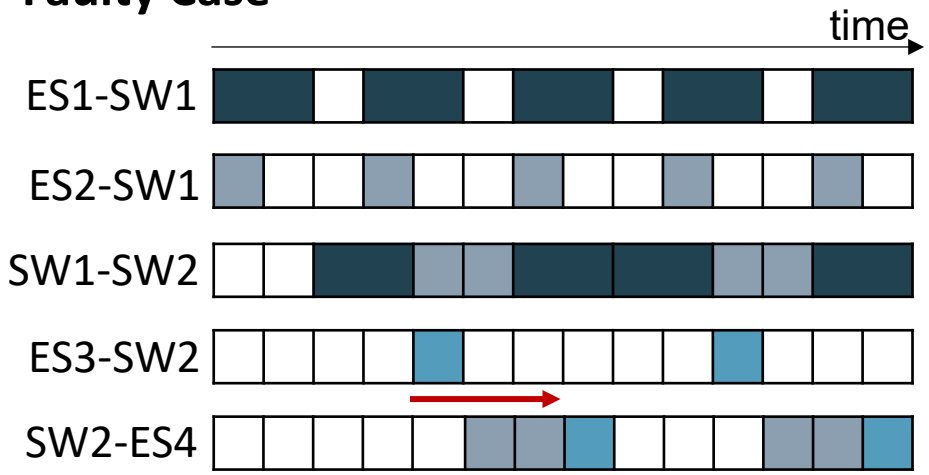
Introduction

Why Per-Stream Filtering and Policing (PSFP)?

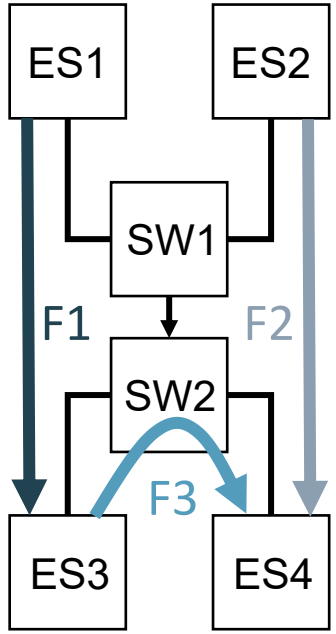
Nominal Case



Faulty Case



Prio: F1 > F2 > F3



TSN guarantees are **conditional**:
only if talkers respect traffic contracts (TSpec)

Reality: clock drift, bugs, misconfiguration, "babbling idiot", attackers

Faults propagate in network ("**domino effect**")

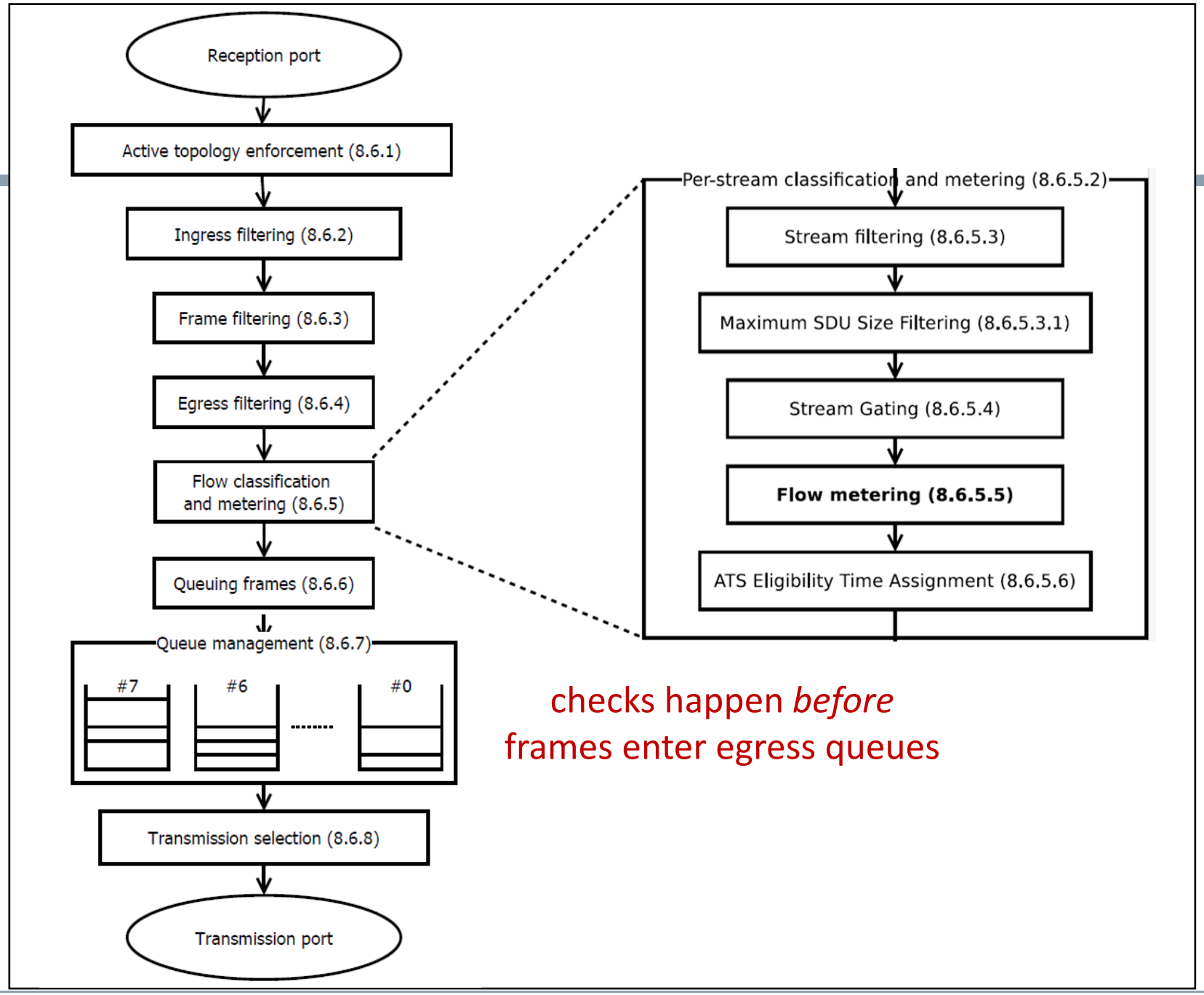
PSFP: contain faults locally (**fault containment**)

F3 latency affected, even without direct interference with faulty F1.

PSFP Introduction

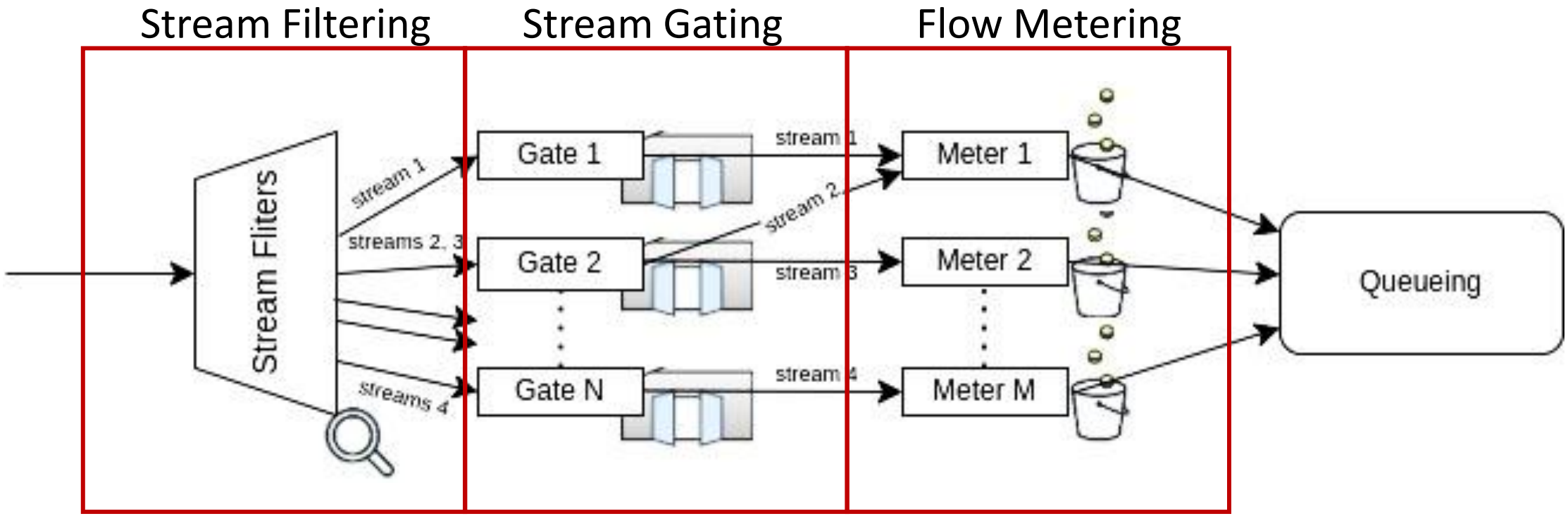
Architecture

- Pre-TSN:
  based on routing/VLAN
- TSN add:
  Per Stream Filtering and Policing (PSFP)
- To tag/drop out of contract frames
- May prevent
  - Queue overflow
  - Deadline miss



PSFP Introduction

Architecture

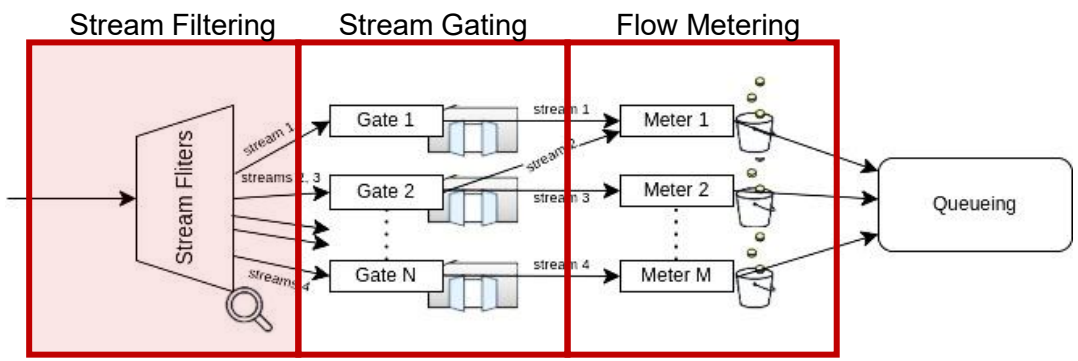


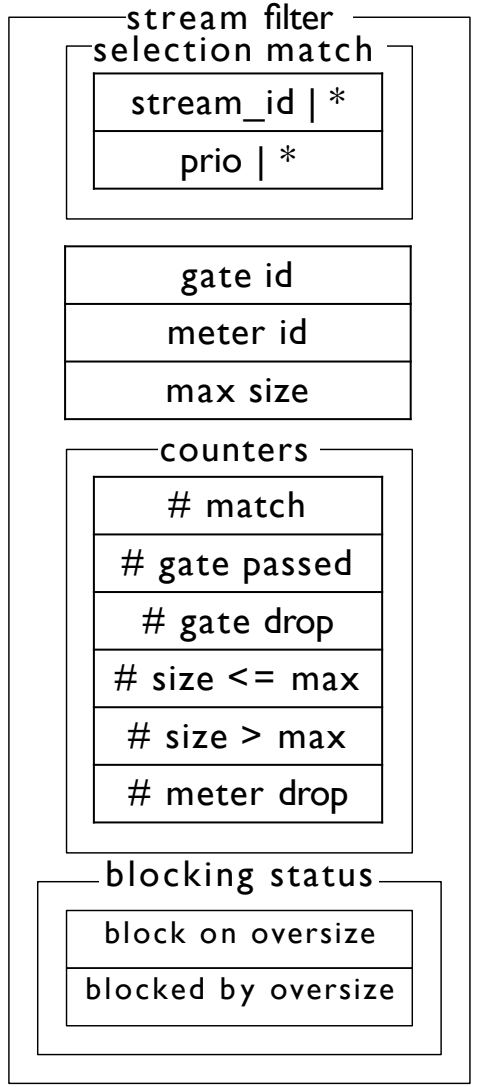
PSFP Introduction

Stream Filtering

Stream ID Function	Examines
Null Stream	dest_addr, vlan_id
MAC and VLAN Stream	src_addr, vlan-id
IP Stream	IP_src_addr, IP_dst_addr, IP_protocol, src_port, dst_port, …

1. Scan the list of filters
2. Select the first one matching pair: (*stream-id, priority);* * = wildcard*
3. A selected filter defines
   a) Check the frame size (wrt *maxSDUsize*)
   b) Define a path through Gate and Meter
   c) Update a few counters



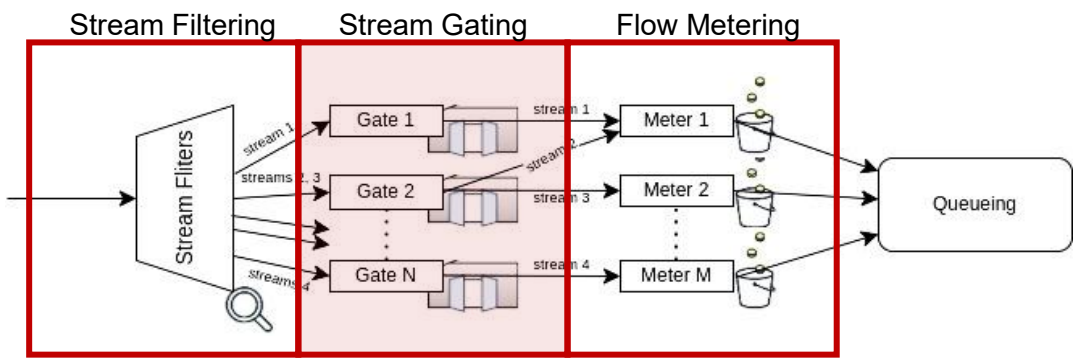


PSFP Introduction

Stream Gating

Stream Control List (≠ Gate Control List)

1. A (cyclic) time-driven list
2. Gate is open / closed: closed = dropped
3. IPV can change the priority of a frame
4. Max. no. of bytes



stream gate

stream gate control list

TimeInterval (duration)	State (open/closed)	IPV	#Octet Max
20µs	open	2	64
200µs	closed	-	-
40µs	open	3	128
...	...	...	...

closed status

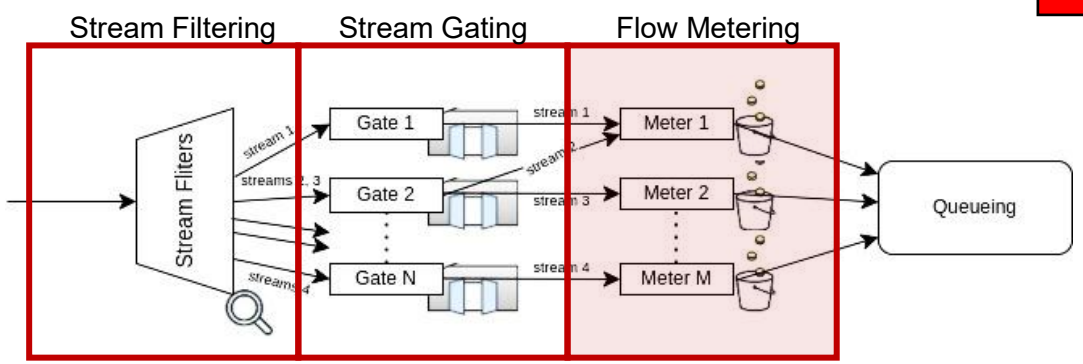
close on invalid Rx
closed by invalid Rx
close on exceed Rx
closed by exceed Rx

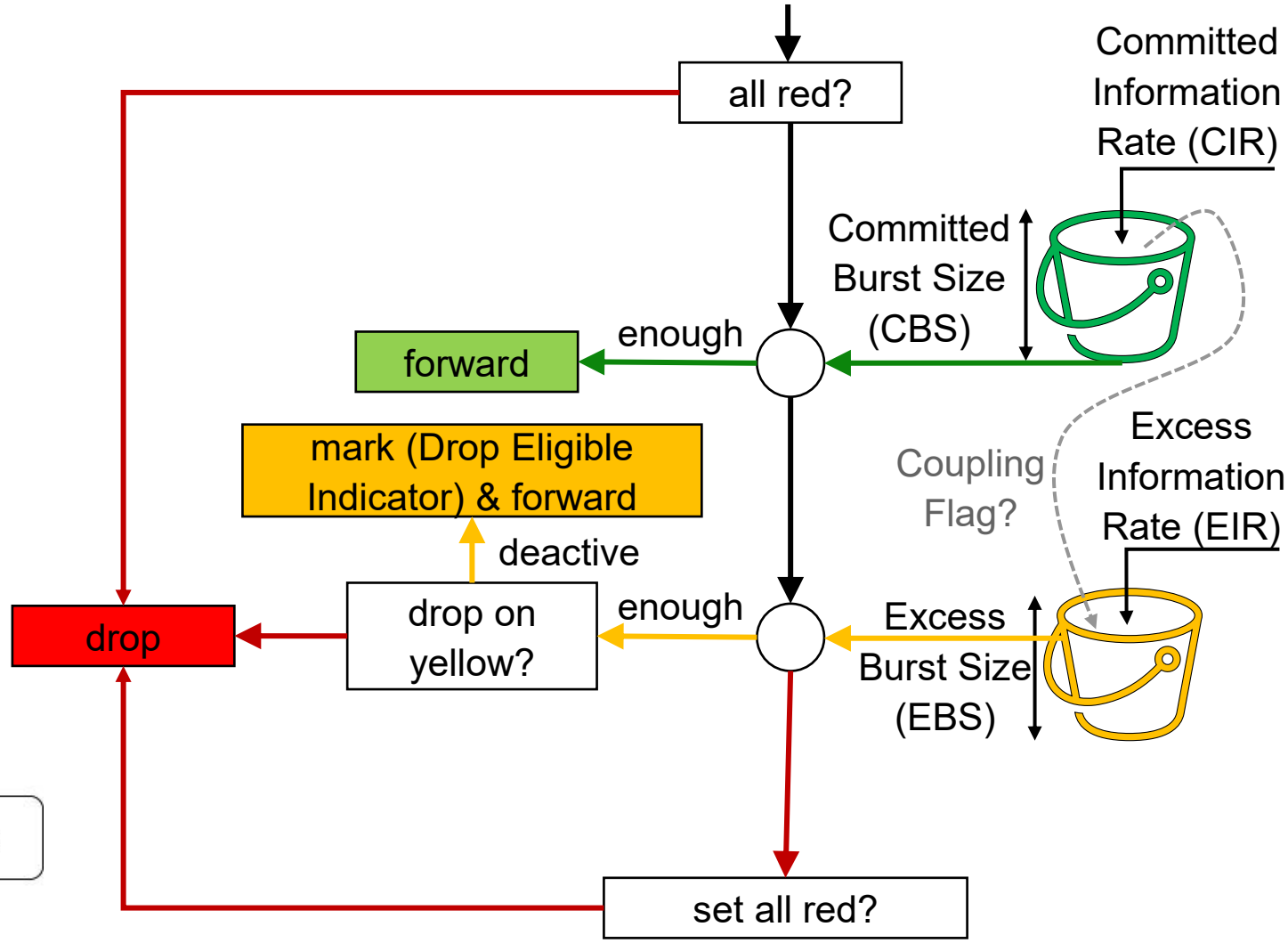
PSFP Introduction

Stream Metering

A double token-bucket:

- Green: conformant
- Yellow: excess
- Red: violation





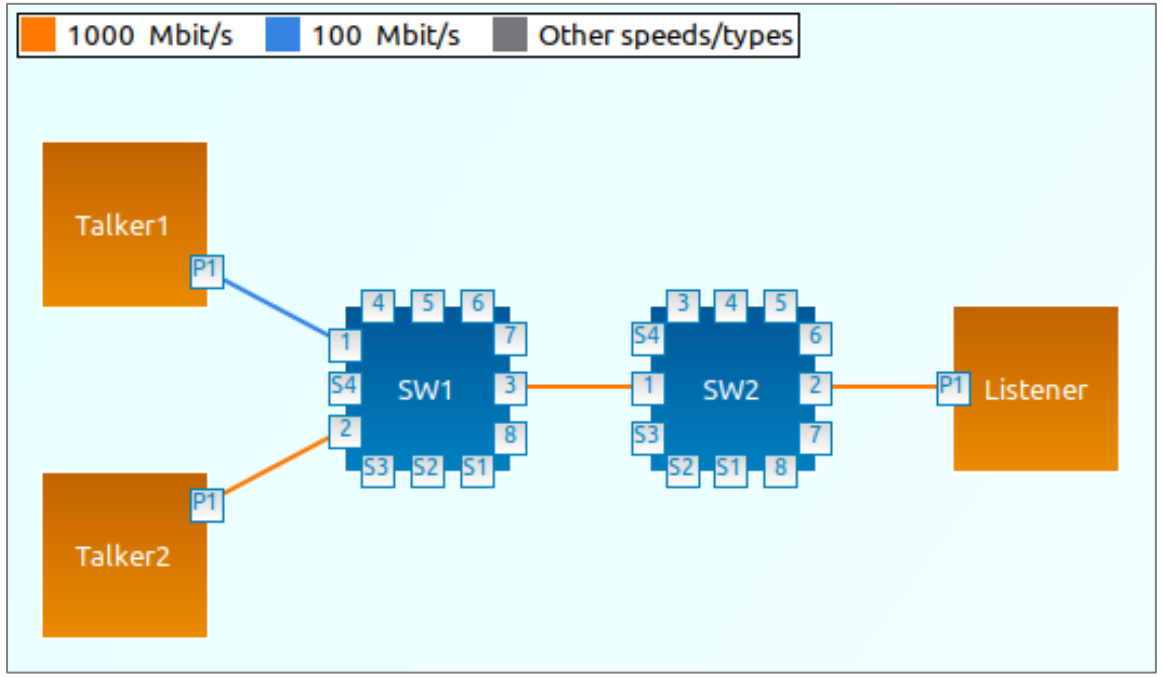
PSFP Demonstration

Experimental setup and traffic definitions

Objective: Evaluate how PSFP flow-meter configuration affects fault containment and the forwarding of valid traffic, in both simulation and hardware experiments.

Experimental platform:

- RTaW-Pegase for modeling, simulation and trace analysis
- 2 x RELY-TSN12 switches
- 1 x RELY-TSN-REC for trace recording on SW1-SW2 link



Traffic:

- F1 (critical, deadline 0.9 ms)
- F2 (interference, faulty in Experiment 1)

Flow	Path	PCP	Arrival model
F1	Talker1 → Listener	5	1,000 B every 250 µs
F2 (nominal)	Talker2 → Listener	6	64 × 1,500 B every 8 ms
F2 (faulty)	Talker2 → Listener	6	100 × 1,500 B every 2 ms

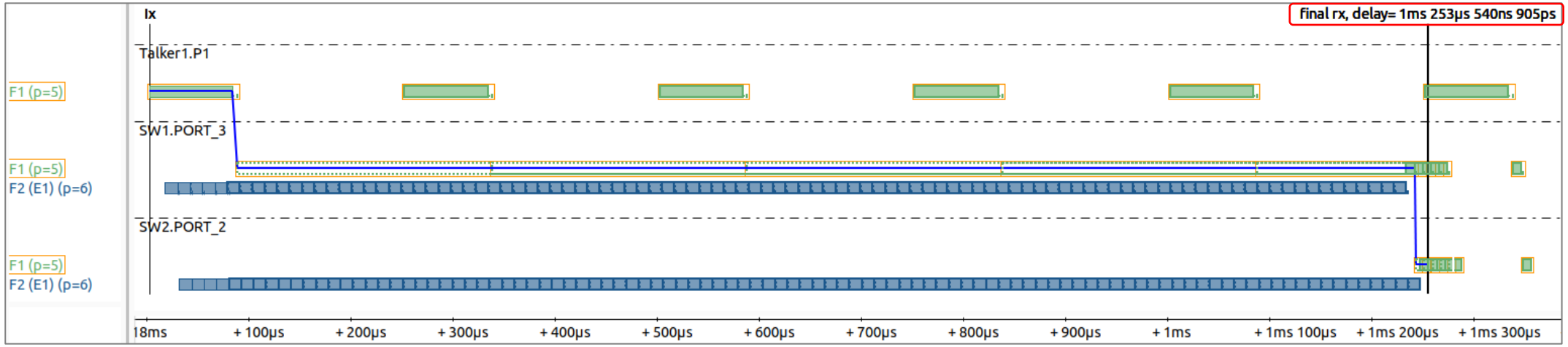
PSFP experiments

Faulty F2 stream policed on SW1; oversized CIR or no flow metering

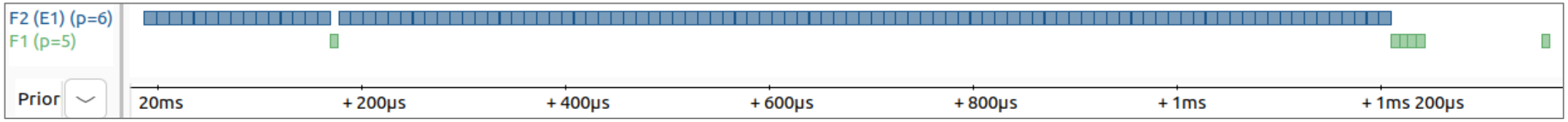
“Too loose” PSFP → no protection from faulty traffic (F2)

Faulty F2 increases F1 end-to-end delay up to 1.25 ms

RTaW-Pegase simulation trace (F1 end-to-end)



Hardware setup recorded trace (SW1-SW2 link)



Observed behavior:

- Here the oversized CIR admits all faulty F2 traffic, producing essentially the same result as no flow metering.
- No F2 packets are dropped, and F1 packets experience excessive end-to-end delays.

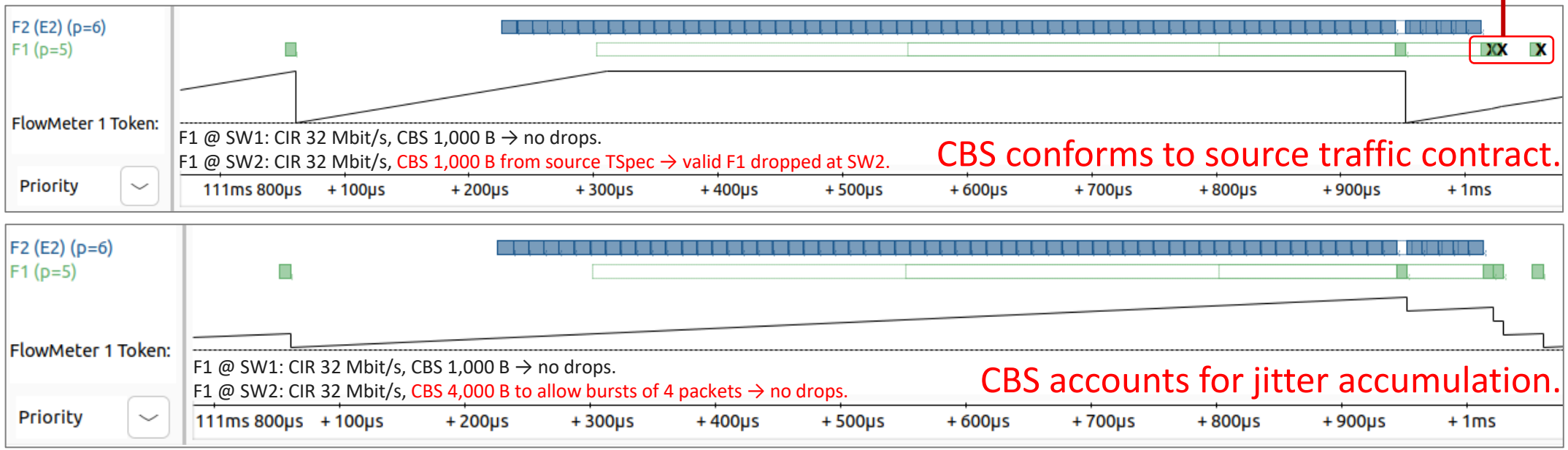
PSFP experiments

None of the flows misbehaves ; F1 policed on SW1 and SW2
Downstream CBS must account for jitter accumulation along the path

⚠ no guidance in the standard

"Too strict" PSFP → drops nominal traffic (F1)

RTaW-Pegase simulation traces (SW1-SW2 link)



Observed behavior / takeaway:

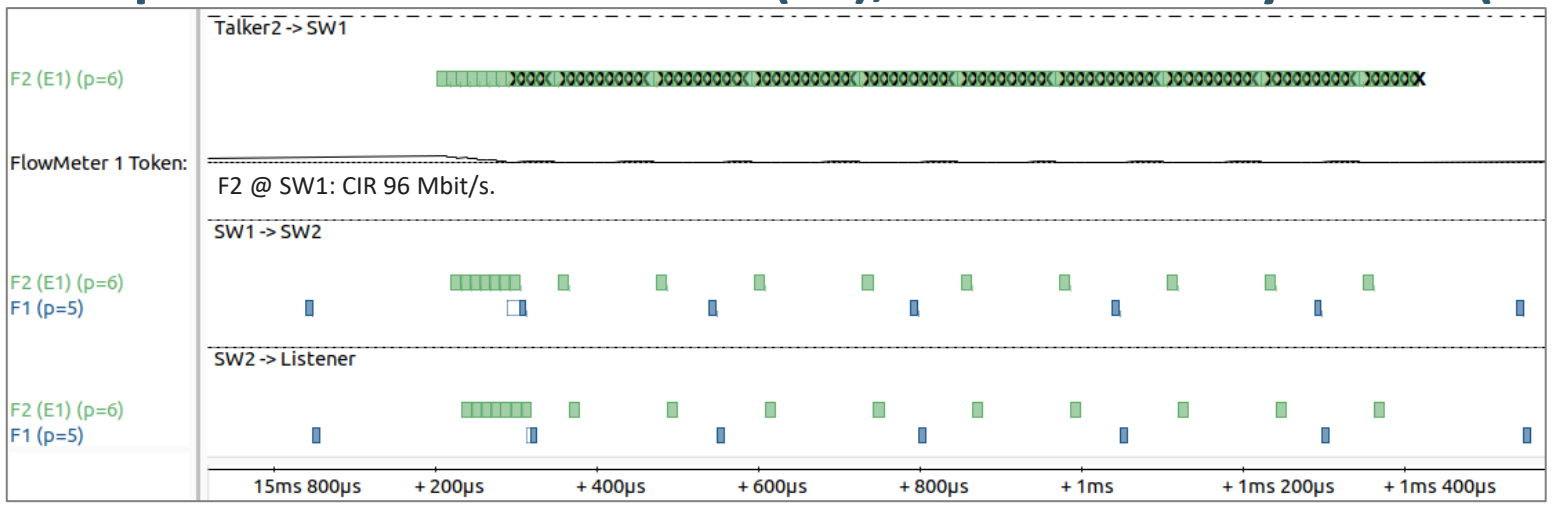
- Valid F1 packets are dropped because the CBS does not account for bursts created by jitter accumulation.
- Schedulability analysis provides an upper bound on the maximum number of packets that can accumulate before transmission, from which a safe downstream CBS can be derived.

PSFP experiments

Faulty F2 stream policed on SW1; correct PSFP configuration

Correct PSFP → protects nominal traffic (F1), discards faulty traffic (F2)

RTaW-Pegase simulation trace (F2 end-to-end)



Black crosses indicate dropped packets. F2 packets are filtered out at SW1 not to exceed the traffic specification.

Packet drops in simulation

PortOwner	Port	Destination	Flow	Cause	Drop Rate	Drops	Arrivals
Talker2	P1	SW1	F2 (E1)	PSFP_FLOW_METER_FILTER	8.39*10^-1	41944	50000

Packet drops on hardware

Filter ID	Matching frames	Gate passing frames	Gate not passing frames	SDU passing frames	SDU not passing Frames	Red frames
Default	4000	4000	0	4000	0	0
1	50000	50000	0	50000	0	41944

Observed behavior / takeaway:

- Correct CIR definition matches F2's nominal rate (96 Mbit/s)
- F2 drops prevent faulty traffic from delaying F1. Max end-to-end delay is approximately halved and below the deadline.

Recommendations for Configuration…

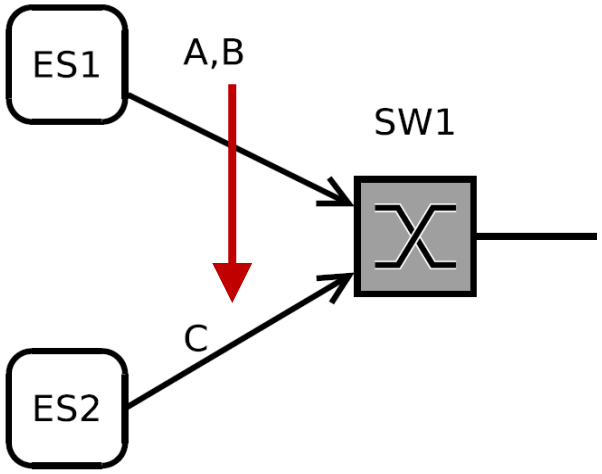


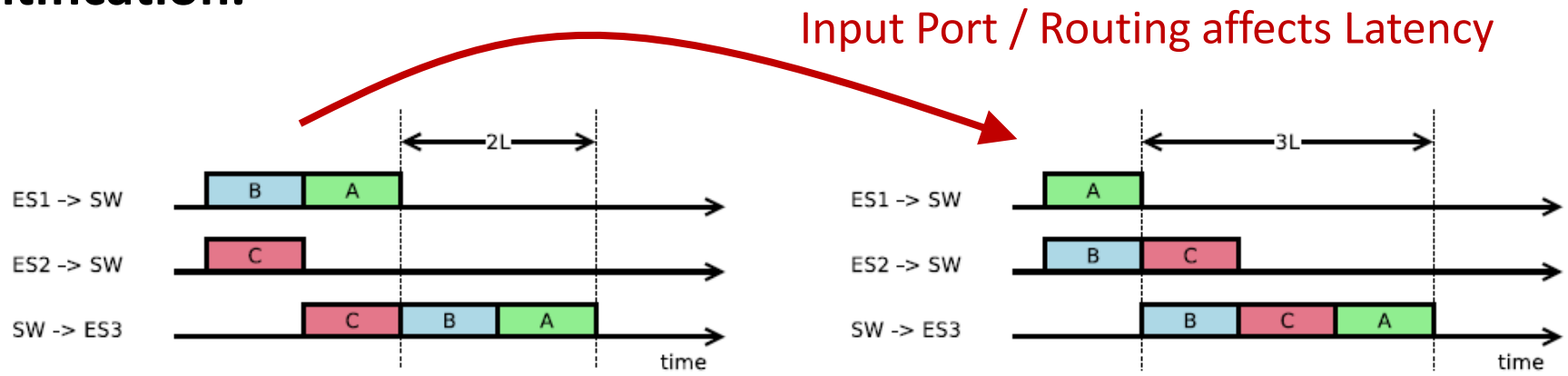
Configuration Guideline

Misrouting

[RTS'26] Maile, Boyer, "Guidance on the Configuration of Per-Stream Filtering and Policing in Time-Sensitive Networking", Real-Time Systems, The International Journal of Time-Critical Computing Systems, Springer, under Minor Revision, forthcoming. **Will be free open access.**

Ingress port in stream identification.





Configuration Guideline

✓ **Stream-handle matching**

Ingress port is implicitly considered → **protects against misrouting**

✗ **Wildcard matching (*, p)**

Ingress port may be ignored → **no protection against misrouting**

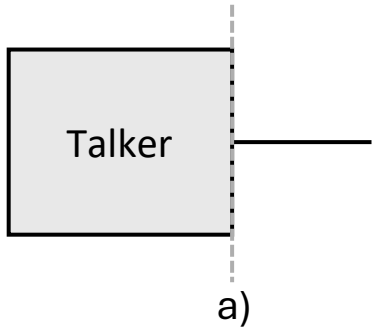
Always include the ingress port in the stream_id to match filters for flows that require performance guarantees.

Configuration Guideline

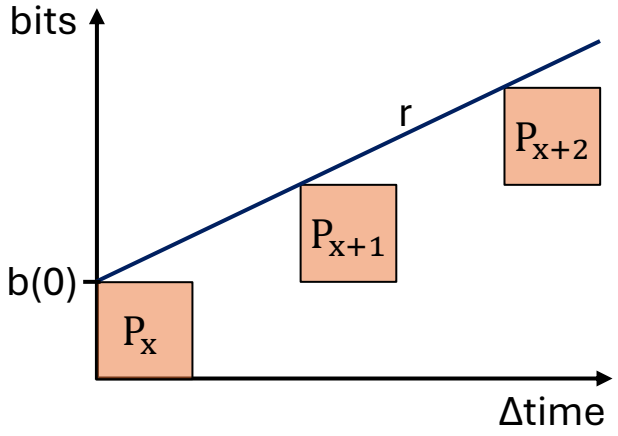
Non-Time-Triggered Forwarding

[RTS'26] Maile, Boyer, "Guidance on the Configuration of Per-Stream Filtering and Policing in Time-Sensitive Networking", Real-Time Systems, The International Journal of Time-Critical Computing Systems, Springer, under Minor Revision, forthcoming. **Will be free open access.**

Example: Strict Priority



a) traffic according to TSpec



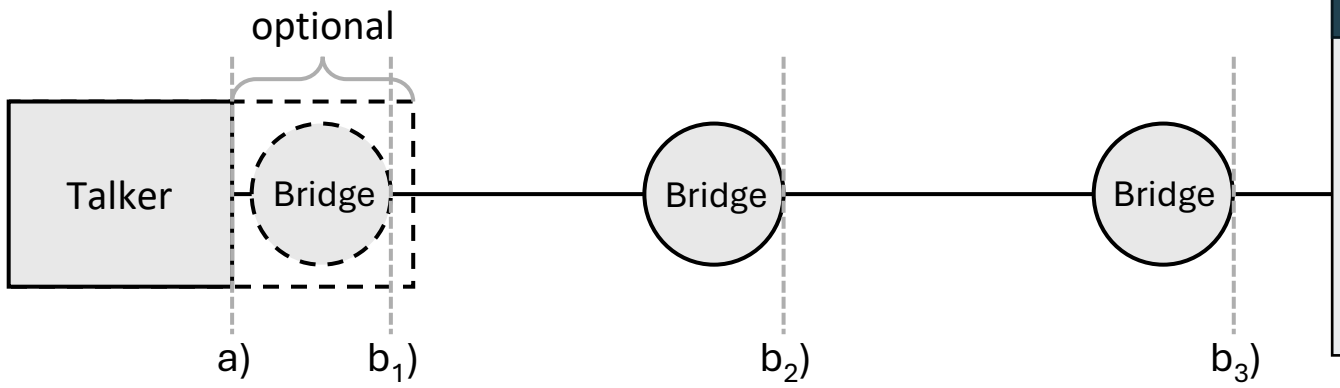
TSpec Parameters		Token-Bucket Parameters
Stream Reservation Protocol		
MaxFramesPerInterval	MFI	$r = \frac{m}{I}$
MaxFrameSize	MFS	$b(0) = \begin{cases} 2m - [r \cdot (I - \text{LTO} + \text{ETO})] & \text{if TTA} = \text{true} \\ m & \text{otherwise} \end{cases}$
Interval	I	
TSpecTimeAware	TTA	$b(J) = b(0) + r \cdot J$
if TSpecTimeAware = true **then**		
EarliestTransmitOffset	ETO	
LatestTransmitOffset	LTO	
Resource Allocation Protocol		
CommittedInformationRate	CIR	$r = \text{CIR}$
CommittedBurstSize	cbs	$b(0) = \text{cbs}$
MaxTransmittedFrameLength		$b(J) = b(0) + r \cdot J$
MinTransmittedFrameLength		

Configuration Guideline

Non-Time-Triggered Forwarding

[RTS'26] Maile, Boyer, "Guidance on the Configuration of Per-Stream Filtering and Policing in Time-Sensitive Networking", Real-Time Systems, The International Journal of Time-Critical Computing Systems, Springer, under Minor Revision, forthcoming. **Will be free open access.**

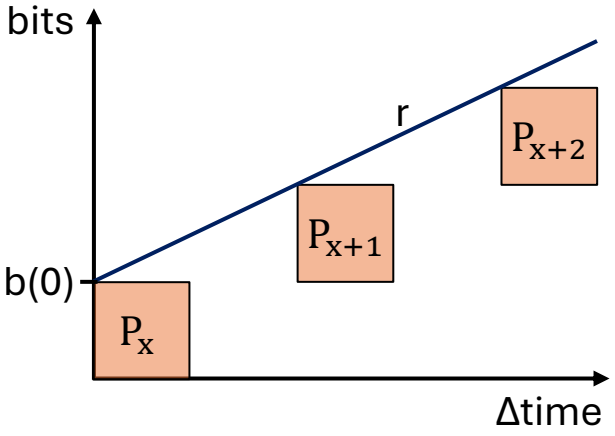
Example: Strict Priority



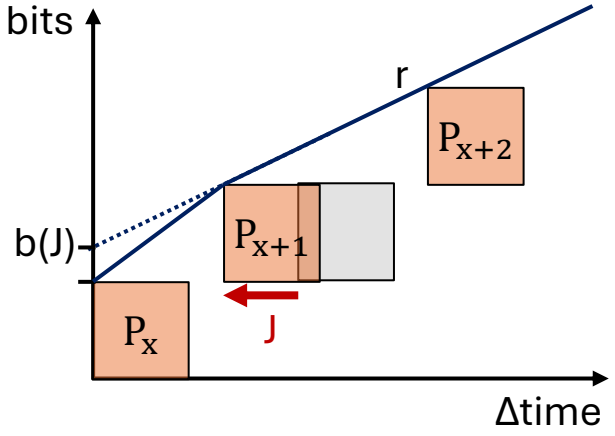
Configuration Guideline

Filter: One per stream.
Gate: Not required.
Meter: One per stream with **CIR = r** and **CBS = b(J).**
b(J) from TSpec + worst-case analysis of path jitter, e.g., using Network Calculus.

a) traffic according to TSpec



b_*) traffic change after forwarding



Here: Jitter J = Difference between min. & max. possible delay on a path incl. clock inaccuracy, hardware jitter, traffic inference, …

Limitations even when configured correctly …

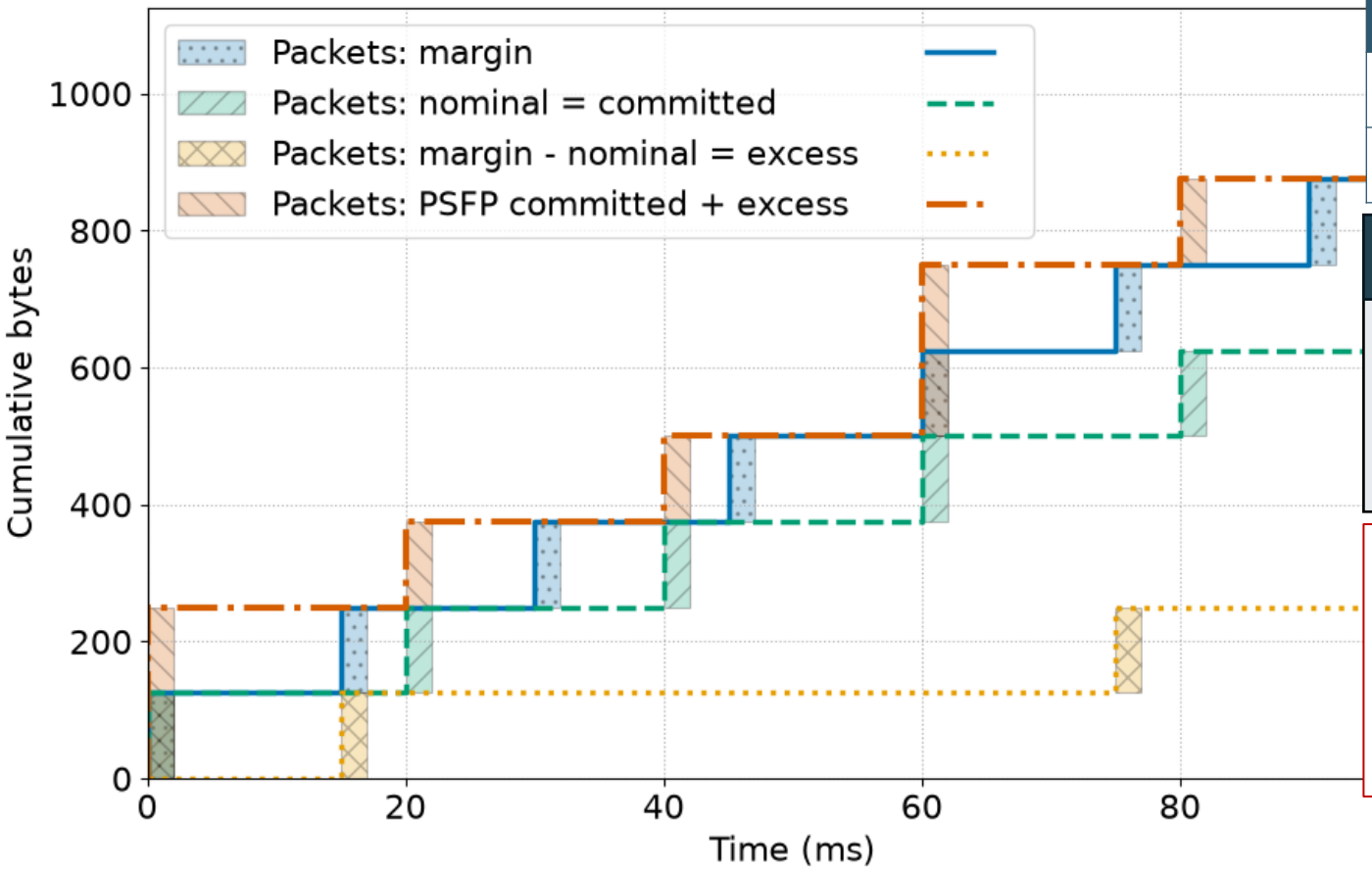


Configuration Guideline

Monitoring with excess meter

[RTS'26] Maile, Boyer, "Guidance on the Configuration of Per-Stream Filtering and Policing in Time-Sensitive Networking", Real-Time Systems, The International Journal of Time-Critical Computing Systems, Springer, under Minor Revision, forthcoming. **Will be free open access.**

Committed vs. excess meter: Tokens consumed separately



Flow	Arrival model	Rate
F1 (nominal)	125 B every 20 ms	50 Kbit/s
F1 (margin)	125 B every 15 ms	66.6 Kbit/s

Configuration Guideline

✓ **Committed meter for complete behavior.**

✗ **Use excess meter for safety margings.**

Consider additional pessimism in guarantees.

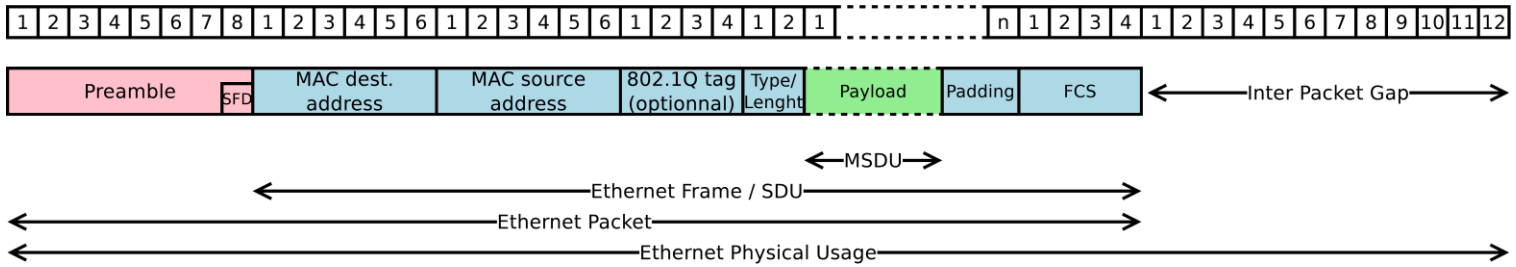
Alternatively adapt standard:

(as in RFC 2698)

1. bucket = margin, every frame consumes tokens.
2. bucket = nominal, determines color.

Limitations

Per-frame overhead (preamble + IPG) is not counted by a flow meter, unlike in the Credit-Based Shaper's idleSlope



The flow meter counts only SDU bytes
SDU = MAC dest → FCS. The wire adds **8 B preamble + 12 B inter-packet gap** to every frame — not counted by the flow meter.

- The wire transmits and CBS idleSlope reserves **SDU + 20 B** per frame. The 20 B overhead is not counted by the flow meter.
- Smaller frames at the same SDU rate → more overhead: **the meter discards no packets while the link bandwidth exceeds the contract** (e.g., a CBS idleSlope).
- Worst case (64 B frames, meter sized for 1522 B): up to **≈ +30% wire bandwidth over contract** [ERTS'26].

Example of a babbling idiot the meter cannot see

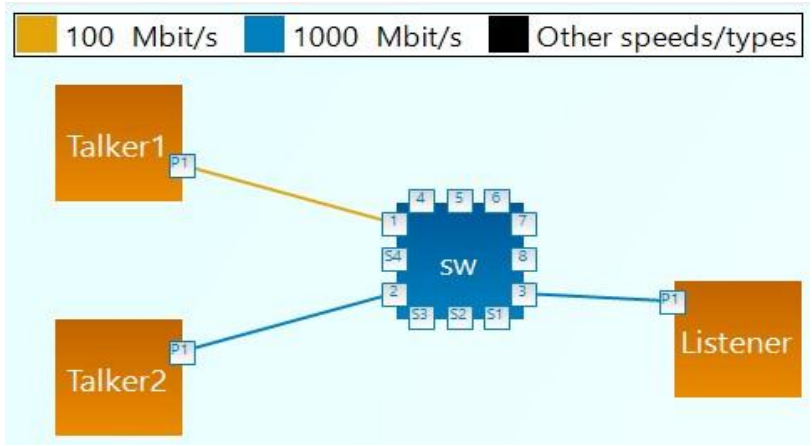
- F1 nominal — 1500 B every 1 ms → SDU rate 12.00 / wire 12.16 Mb/s
- F1'' faulty — 64 B every 43 µs → SDU rate 11.91 Mb/s ✓ **passes**, wire 15.63 Mb/s ✗ **+29% over contract**

[ERTS'26] Ladeira, Boyer, Navet, Séguin, "PSFP in TSN Networks: Insights into Some Practical Limitations", ERTS 2026

Limitations

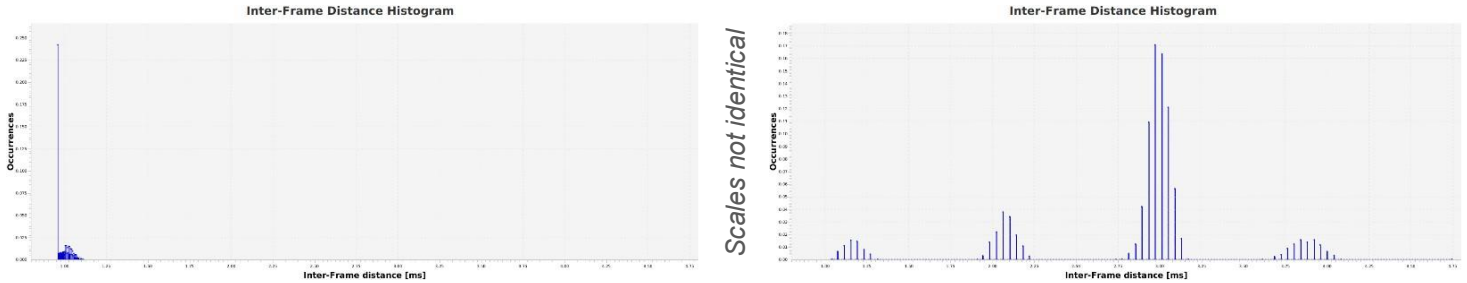
Observing packet losses in simulation and on hardware

Setup

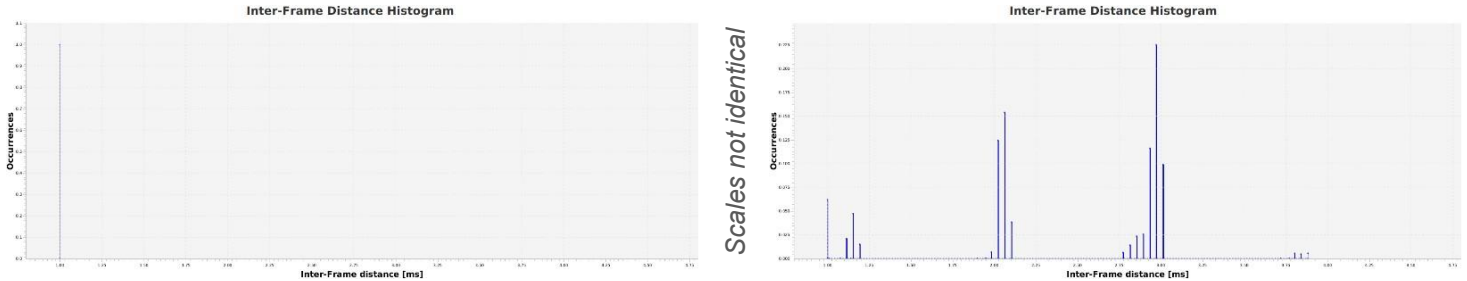


- HW: RELY-TSN12 switch, capture at the Listener
- Simulation: RTaW-Pegase
- **Switch → Listener: F1 and F2 share one CBS queue, idleSlope = 17 Mbit/s**
- F2 (victim, Talker2): 500 B every 1ms, 4.16 Mbit/s on the wire
- F1 (nominal, Talker1): 1,500 B every 1ms, 12.16 Mbit/s on the wire
- **F1″ (faulty, Talker1): 64 B every 43µs — passes the meter (11.91 < CIR 12.16 Mbit/s), 15.63 Mbit/s on the wire**

F2 nominal | **F2 with faulty F1″**



RTaW-Pegase simulation — inter-frame distances of F2 at the Listener



Hardware capture — inter-frame distances of F2 at the Listener

Although F1″ conforms to its flow meter, the shared CBS queue overflows. F2 loses up to 3 consecutive frames / observed both in simulation and on hardware (spikes at 2×, 3×, 4× the period)

[ERTS'26] Ladeira, Boyer, Navet, Séguin, "PSFP in TSN Networks: Insights into Some Practical Limitations", ERTS 2026

Solutions

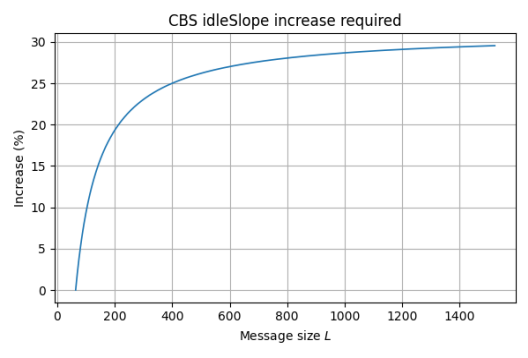
Metered bytes vs on-wire bytes: what can be done today, what the standard could change

- **Tightening the meter is not a solution:** a CIR set low enough to keep small-frame traffic within the stream's reserved link bandwidth may also discard up to 23% of the valid traffic sent with large frames [ERTS'26].

Workaround possible today

Over-provision the CBS idleSlope downstream of the flow meter to absorb the excess the meter lets through and no innocent frame is lost.

Requires increasing the idleSlope by up to 30% [ERTS'26].



Enhancement requires 802.1Q change or vendor extension

1) minSDUSize check in the stream filter (as in AFDX)

Caps the wire bandwidth at the contract when a minimum frame size can be enforced, but not applicable to streams with no guaranteed minimum size (e.g., fragmented data). Proposed in IEEE 802.1: draft PAR P802.1Qek (Sept. 2026).

2) Count on-wire bytes (SDU + 20 B) for metering

Meter, wire and CBS idleSlope then count the same bytes. The device already counts the overhead elsewhere (CBS at egress, ATS eligibility time).

Note on ATS: per-flow ATS may be less exposed, as its eligibility time includes the media overhead and MaxResidenceTime discards over-delayed frames, but the level of protection achieved remains to be studied in detail.

[ERTS'26] Ladeira, Boyer, Navet, Séguin, "PSFP in TSN Networks: Insights into Some Practical Limitations", ERTS 2026

Limitation & Solutions

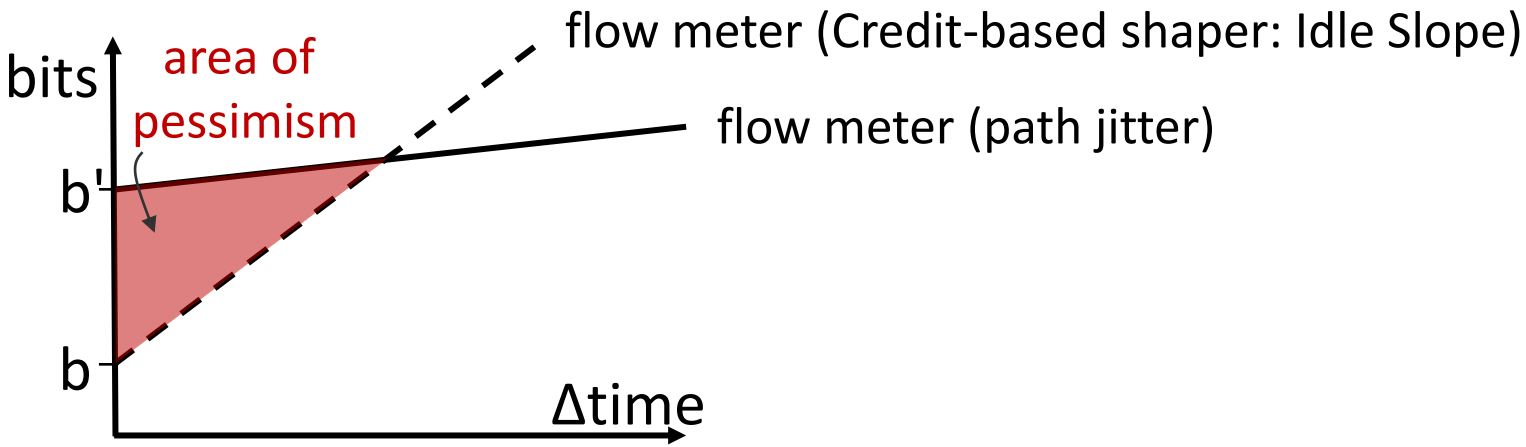
Short Overview

[RTS'26] Maile, Boyer, "Guidance on the Configuration of Per-Stream Filtering and Policing in Time-Sensitive Networking", Real-Time Systems, The International Journal of Time-Critical Computing Systems, Springer, under Minor Revision, forthcoming. **Will be free open access.**

Some more aspects…

PSFP cannot **validate the functionality** of all **shapers**. For example:

– Credit-Based Shaper output is bounded by two envelopes, but PSFP can enforce only one.



– Asychronous Traffic Shaper "shaping for free property" cannot be verified (previous hop).

Mitigation is limited: Excess packets only dropped (potentially dropping valid frames only interfering with faulty flows). Instead, Internal Priority Value adjustment desirable.

… complete configuration guidelines and limitations can be found in [RTS'26]

Overview

Understanding PSFP



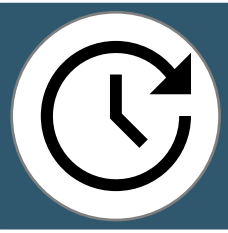
PSFP offers protection for ultra-critical systems



Avoid too loose and too strict configurations.
Our configuration guidelines fill this gap.



Current standardization has limitations.



New configuration guidelines („default rules“)
+ small changes in standardization
= improved usability of PSFP in the future

Questions?

Lisa Maile
- l.t.maile@tue.nl

Nicolas Navet
- nicolas.navet@uni.lu

Marc Boyer
- marc.boyer@onera.fr

Leo Séguin
- leo.seguin@realtimeatwork.com

Thank you!