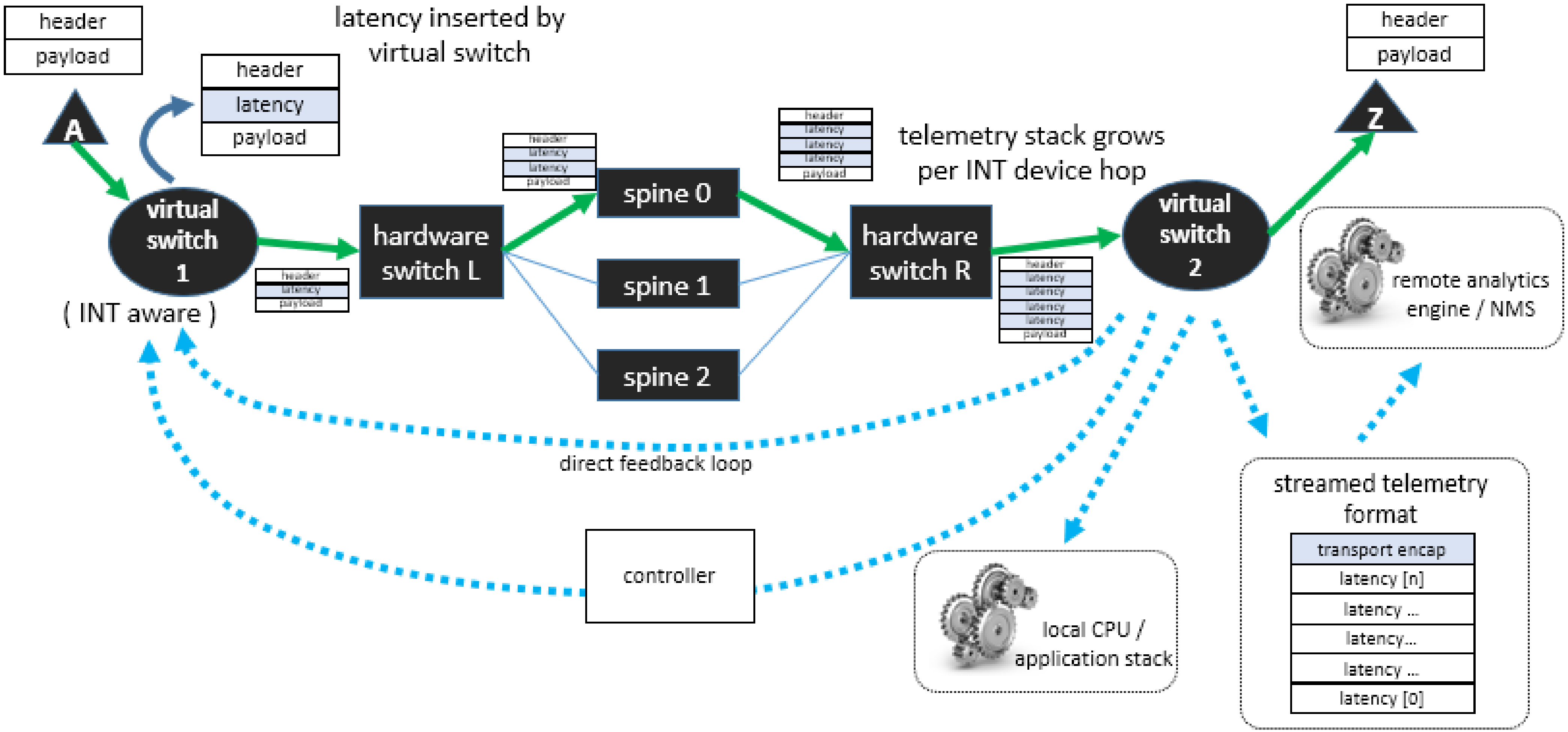
Data Plane Programmability and Telemetry

A "Passive Device" Latency Use Case based on INT

Overview – Telemetry from “Passive Devices”

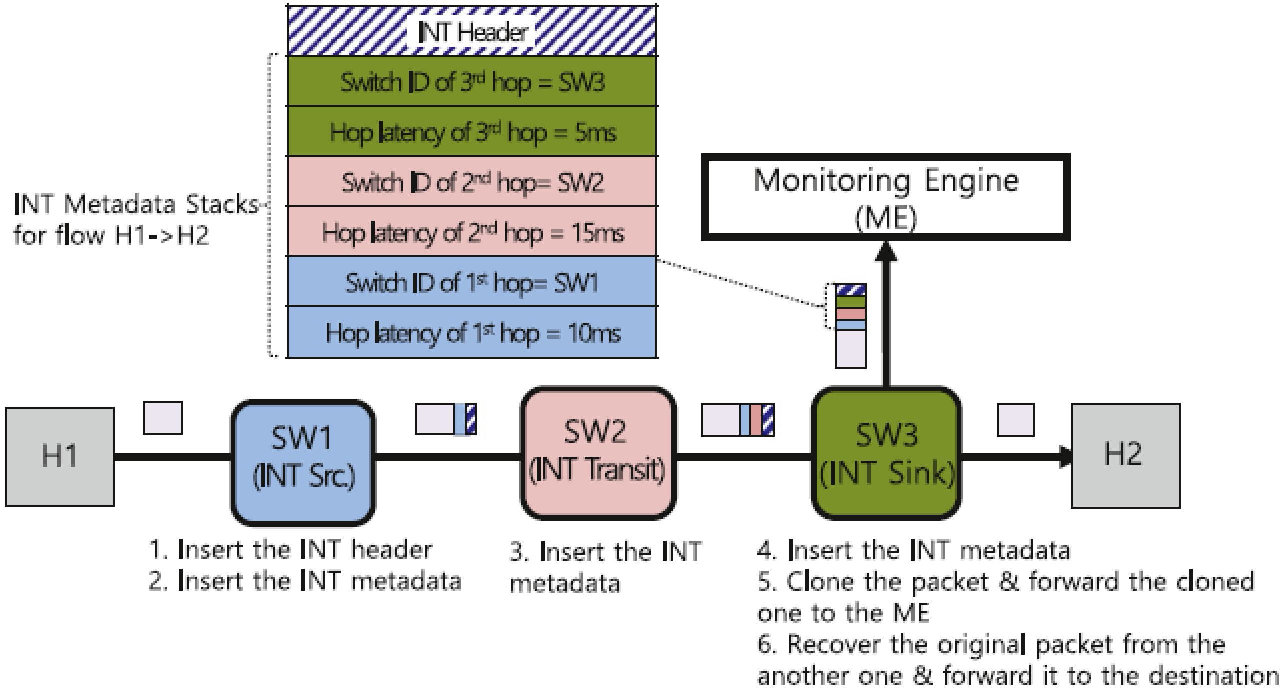
- Interesting Use Case suing Programable Pipeline and INT
- Latency from “Passive” Security Tools (not INT capable)
- Closed Loop INT environment
- The Tyranny on INT Data
- Data Reduction Strategy

"Active" Participants in Latency Telemetry



Packet View of Active Participants

The Devices under observation are INT capable participants



INT Header
Switch ID of 3rd hop = SW3
Hop latency of 3rd hop = 5ms
Switch ID of 2nd hop= SW2
Hop latency of 2nd hop = 15ms
Switch ID of 1st hop= SW1
Hop latency of 1st hop = 10ms
INT Metadata Stacks for flow H1->H2
Monitoring Engine (ME)
H1
SW1 (INT Src.)
SW2 (INT Transit)
SW3 (INT Sink)
H2

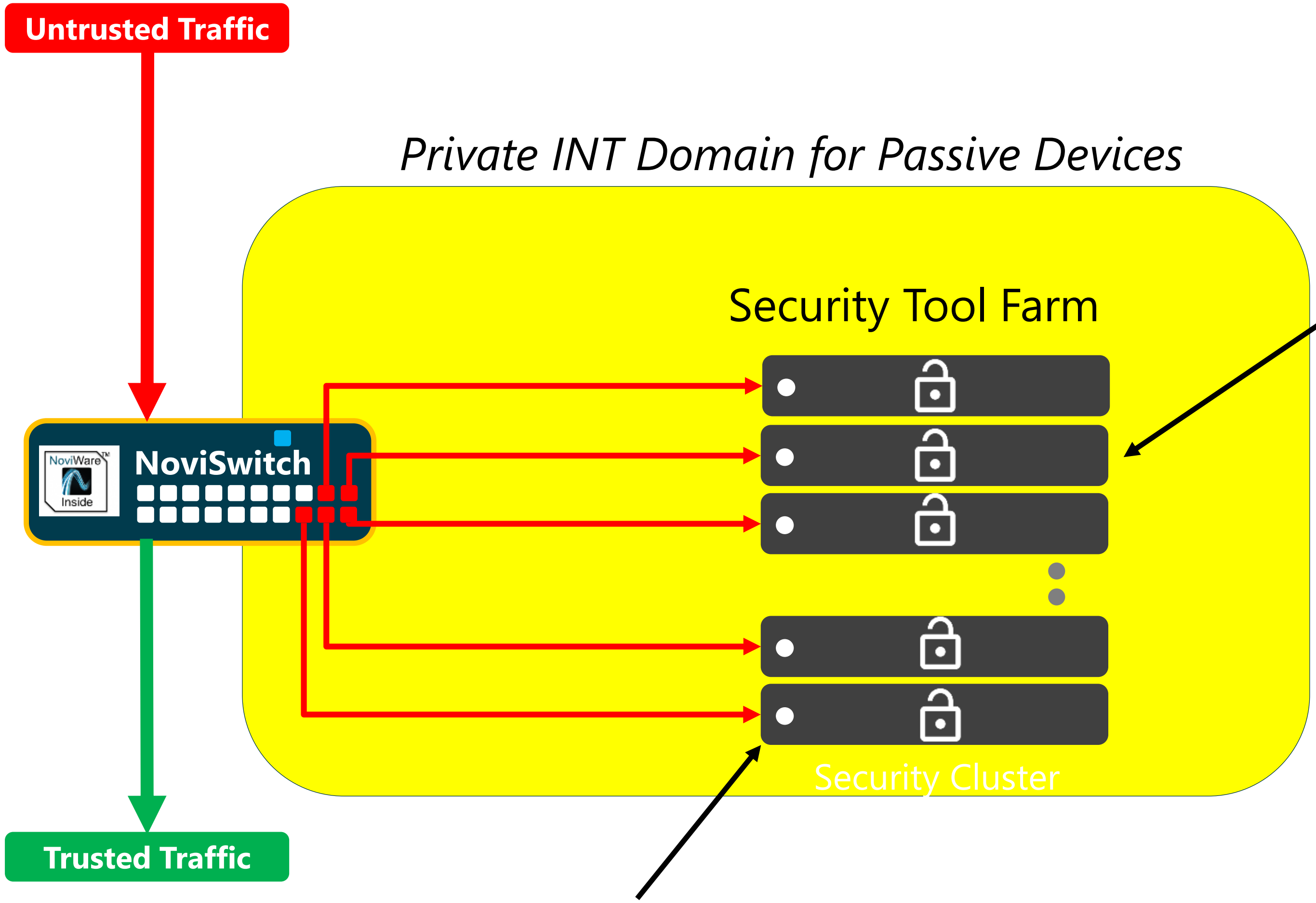
1. Insert the INT header
2. Insert the INT metadata

3. Insert the INT metadata

4. Insert the INT metadata
5. Clone the packet & forward the cloned one to the ME
6. Recover the original packet from the another one & forward it to the destination

NoviFlow
networks made programmable

New User Case - Private INT Domain / Passive Devices



Private INT Domain for Passive Devices

Security Tool Farm

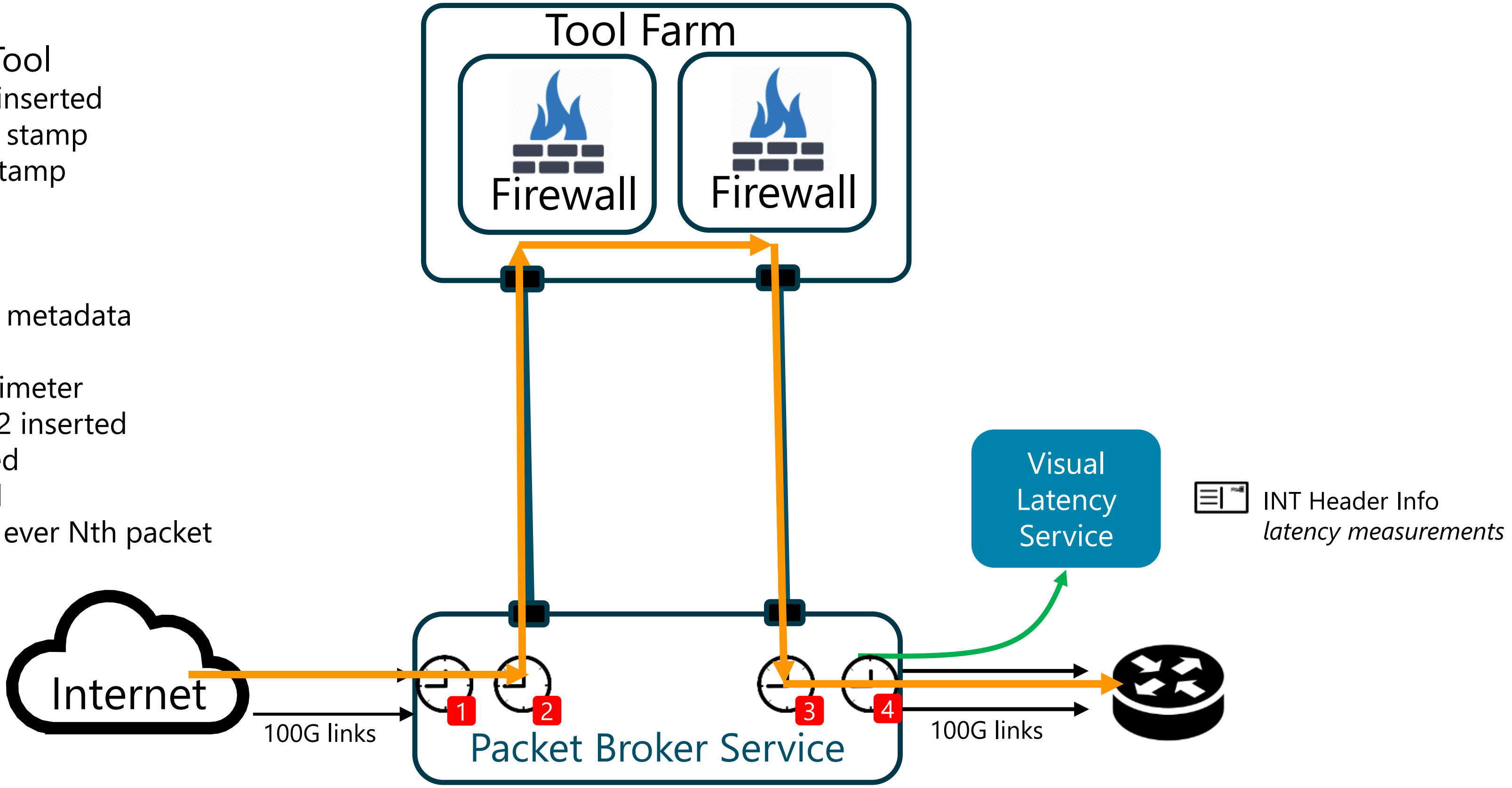
Problem:
Firewall devices not INT capable

Objective: Firewall Latency

NoviFlow
networks made programmable

INT Traverse of Tool Farm

1. Packet enters Security Perimeter
   - INT header inserted
   - Time captured to Metadata
2. Packet exits Port to Tool
   - INT Hop Header inserted
     - Entry time stamp
     - Exit time stamp
     - Ports
3. Packet re-enters switch
   - Time captured to metadata
4. Packet exits Security Perimeter
   - INT Hop Header 2 inserted
   - INT Header POPed
   - Packet forwarded
   - INT Data sent on ever Nth packet



The Tyranny of INT Data

- Log Data is Meta Information on a flow (Web Session)
- INT Data is Telemetry on packets within a flow – ORDERS OF MAGNITUDE MORE DATA
  - But less Information in each unit

100G Security Flow Model

- *1,400 Bytes - Ave packet size*
- *9 Million Packets per second (pps)*

Reduce **Data** while maintaining **Information**

1st Data Reduction Strategy - Sample

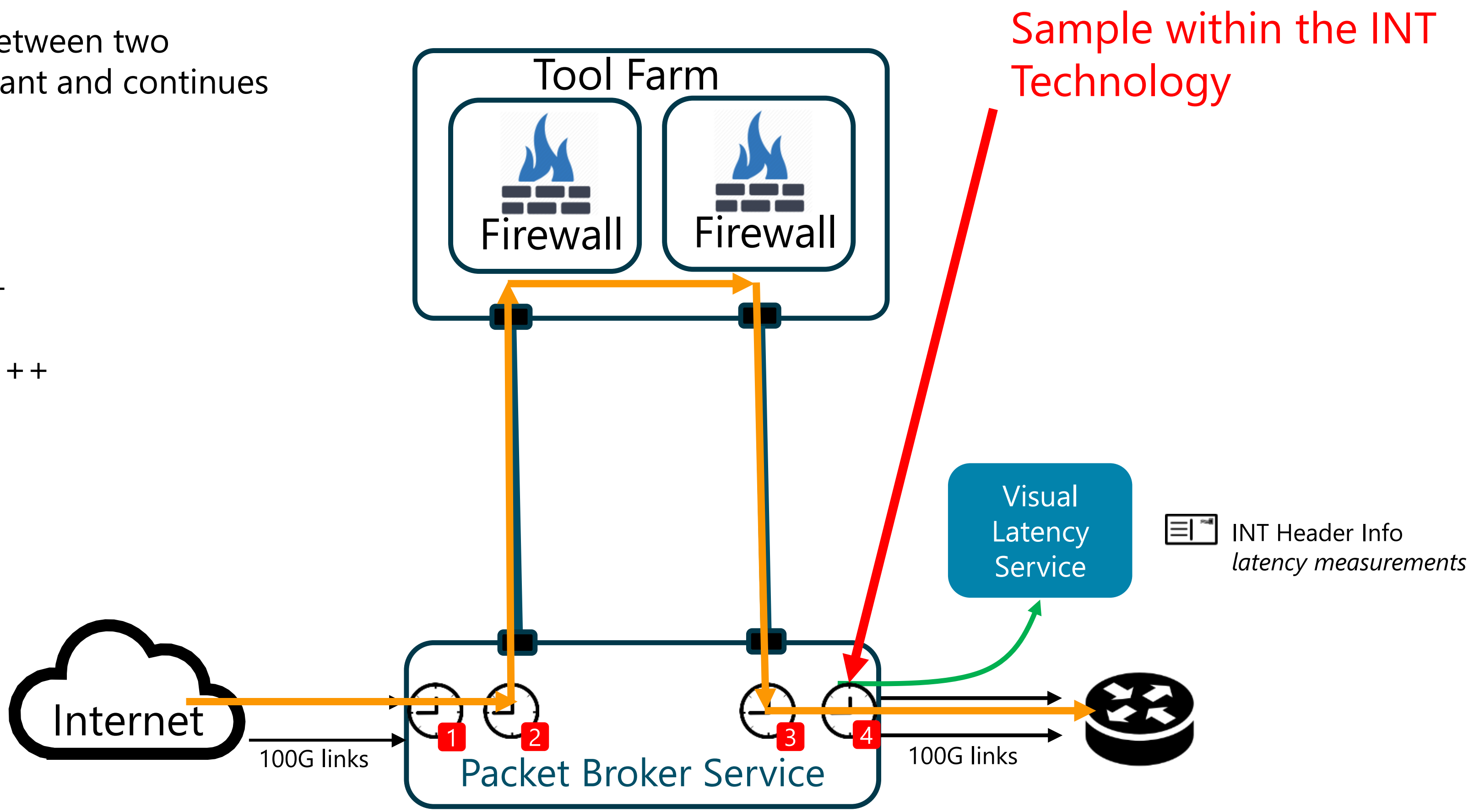
Key Observation

The latency information between two packets is close to redundant and continues little Information

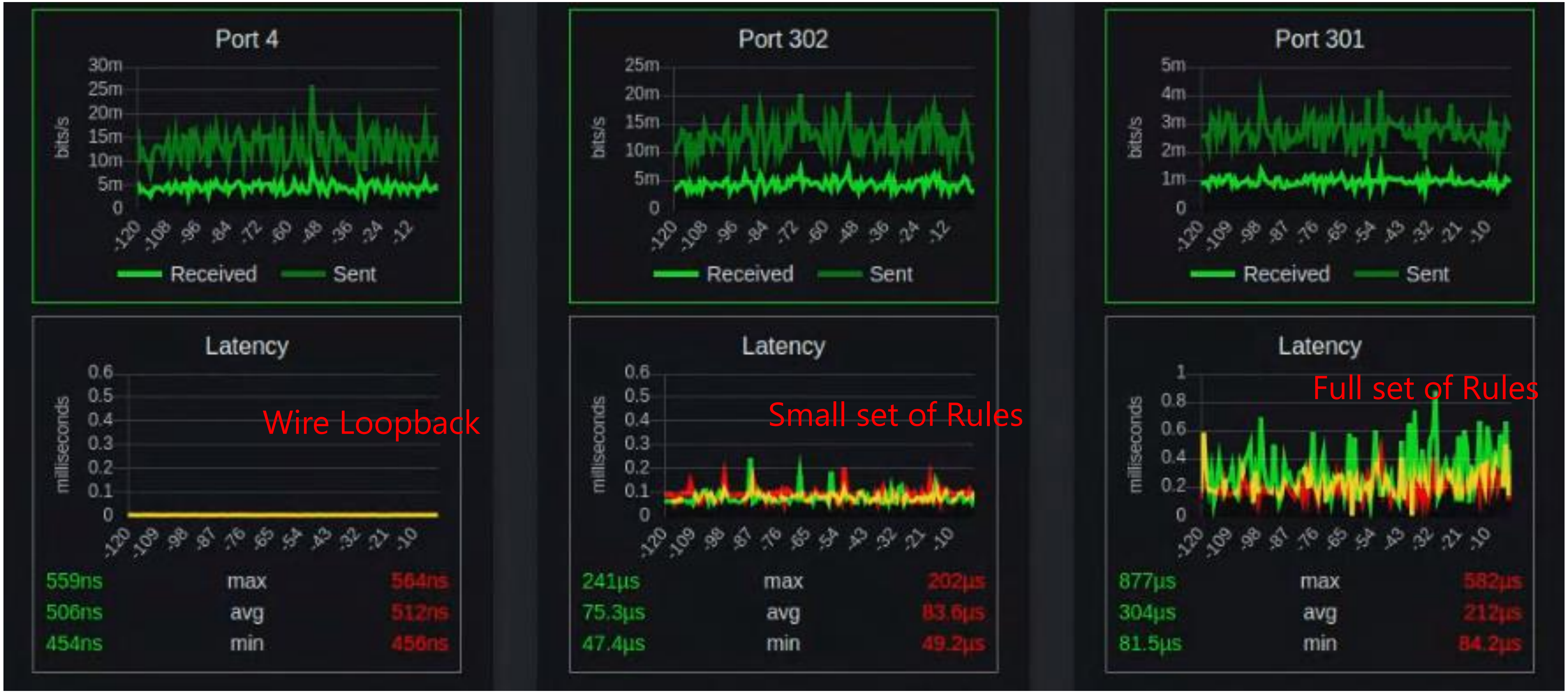
Information p1,p2 is ~0

Information p1,p1000 is +

Information p1,p10000 is ++



Dashboard Look at Latency in Tool Cluster



Wire Loopback

559ns	max	564ns
506ns	avg	512ns
454ns	min	456ns

Small set of Rules

241µs	max	202µs
75.3µs	avg	83.6µs
47.4µs	min	49.2µs

Full set of Rules

877µs	max	582µs
304µs	avg	212µs
81.5µs	min	84.2µs