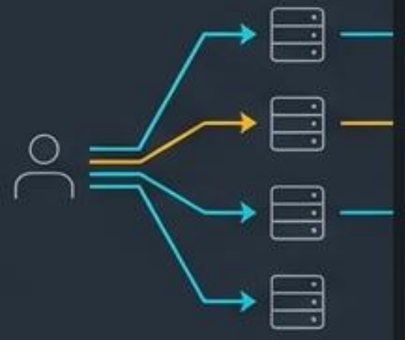
Network Telemetry & Operations



```
[SYS_INIT] Loading FCAPS Framework...
[MODULE_1] Fault Management & Root Cause Isolation
[MODULE_2] Performance Optimization & Capacity Planning
[STATUS] Operational
```

CPU 64%
Stability/Normal operations

CPU 100%
Vitality/Drop Operations

ALert 0.3%
Warning/Nominal operations

11.63
Healthy traffic

0.8 m.
Slight anme packet loss

CPU 36%
Memory 36%
Stable 20%
Storage 25%

CPU 18 MiB
Memory 16TB
Stable 19 MiB
Storage 68TB

Stab
Stability normal

0.5%
Slight packet loss

CPU 48 MiB
Memory 93 TB
Stable 62 TB
Storage 31 TB

Dropped
Critical fault

0/0
Dropped connection

NotebookLM

The Two **Pillars** of Network Telemetry

Pillar 1: Stability (Health)

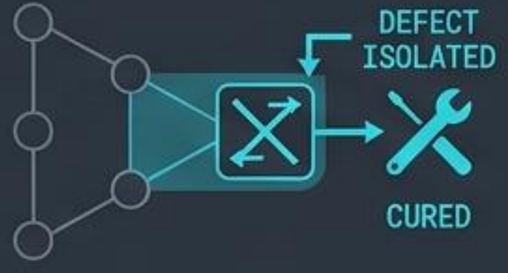
Metric Group: Fault Management

Objective: Keeping the network alive. Diagnosing disease, isolating defects, and curing root causes.

Key Focus: Reactive & Corrective (Preventing outages)

FAULT HISTORY (LAST 24H)

ROOT CAUSE ANALYSIS (RCA)



OUTAGE PREVENTION

Pillar 2: Vitality (Fitness)

Metric Group: Performance & Capacity

Objective: Keeping the network fast and efficient. Managing bandwidth diet, throughput, and responsiveness.

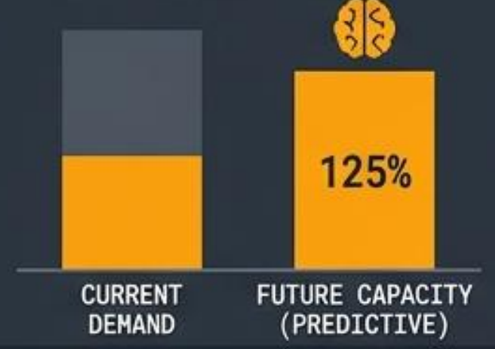
Key Focus: Proactive & Predictive (Optimizing user experience)

THROUGHPUT TREND (LAST 7 DAYS)

BANDWIDTH UTILIZATION MAP

RESPONSIVENESS SCORE

CAPACITY FORECAST



NotebookLM

The Anatomy of a Network Outage

Widget 1

1. The Fault (Defect)

Definition: The physical or logical defect residing in the system. The true root cause.

Telemetry: Severed fiber-optic cable or a dead redundant power supply.

Note: Can remain hidden and dormant if not actively in use.

Widget 2

2. The Error (Incorrect State)

Definition: The immediate manifestation of an activated fault within the system's internal logic.

Telemetry: An NMS log showing a router interface dropping from UP to DOWN.

Widget 3

3. The Failure (Observable Outage)

Definition: The external deviation from expected behavior. The disruption of service.

Telemetry: A database timeout. End-users cannot access the corporate intranet.

NotebookLM

The Avalanche Effect and Event Correlation

The Storm: 5,000 Symptomatic Events

Examples: Edge switch uplinks down, BGP adjacencies timed out, Wi-Fi controllers disconnected

The Correlation Engine

Rule:
IF [Core Switch A Fails]
AND [Edge Switch B is Topologically Downstream]
AND [Time Window < 30s]
THEN [Suppress Switch B Alerts]

Root Cause Identification

1 Actionable Trouble Report:
Core Switch A Hardware Power Supply Failure

NotebookLM

Strategic Entry Points for Hypothesis Testing

Top-Down

Verify end-user software, then check L4 transport firewall ports.

Best for single-user complaints regarding specific services.

Divide-and-Conquer

Execute an IP ping test. Instantly halves the problem space. If successful, L1-L3 are functionally sound. Best for rapid isolation.

Bottom-Up

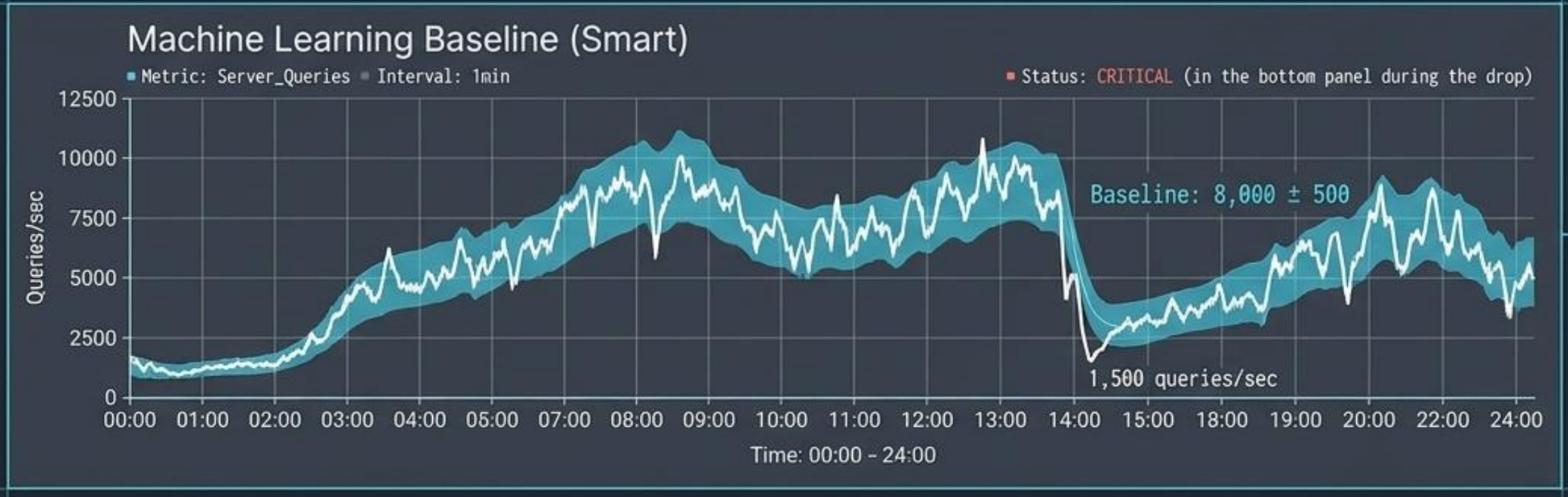
Verify physical cables, fiber optics, and link lights.

Best for localized hardware outages and physical CRC errors.

NotebookLM

Static Thresholds vs. Algorithmic Baselining

Insight: The static threshold is never crossed. No alarm sounds. The fault remains hidden.



⚠ **Insight:** Real-time traffic falls outside the historical envelope. The NMS instantly flags the deviation as a severe anomaly.

NotebookLM

The Subjectivity of Performance

> “A network that physically forwards packets but does so slowly that users cannot complete their tasks is, for all practical purposes, failing.”

Hardware survival is binary. Performance is contextual. We must translate subjective complaints into objective mathematical metrics of capacity, responsiveness, and reliability.

NotebookLM

The Holy Trinity of Telemetry Metrics

1. Throughput (The Pipe)

Definition: The actual, realized rate of successful data delivery over time (Mbps/Gbps).

Context: Distinct from physical bandwidth; always lower due to TCP/IP header overhead and line noise.

2. Delay / Latency (The Speed)

Definition: The total milliseconds required for a bit to travel from source to receiver.

Context: The ultimate metric for network responsiveness and application usability.

3. Jitter (The Reliability)

Definition: The variance in delay between sequential packets in a single data stream.

Context: If Packet A takes 20ms and Packet B takes 80ms, the jitter is 60ms. Devastating for real-time delivery.

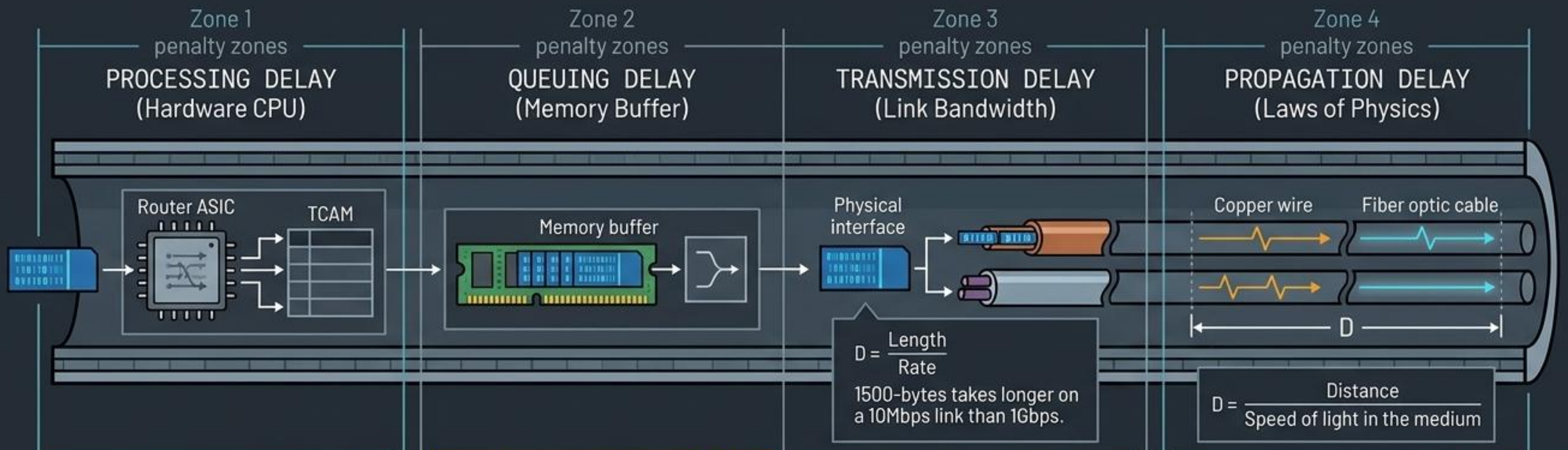
NotebookLM

Application Sensitivity Matrix

	Elastic Traffic	Inelastic Traffic (Real-Time)
Examples	FTP, HTTP, Database Backups	VoIP, Live Video, Industrial Control Systems
Throughput Sensitivity	HIGH (Demands maximum capacity)	LOW (Requires a small, fixed capacity)
Delay/Jitter Sensitivity	LOW (Data arrives perfectly intact, just slower. The application stretches.)	HIGH (Jitter > 30ms distorts audio. Delayed syllables are discarded entirely.)
Behavior Under Stress	Adapts	Breaks

NotebookLM

The Anatomy of Delay



Zone 1 ✓ µs

The microseconds a router ASIC takes to read the header and consult the TCAM routing table.

Zone 2

The highly variable time spent sitting in RAM waiting in line during congestion.

Zone 3 bit

The time to push bits onto the wire.

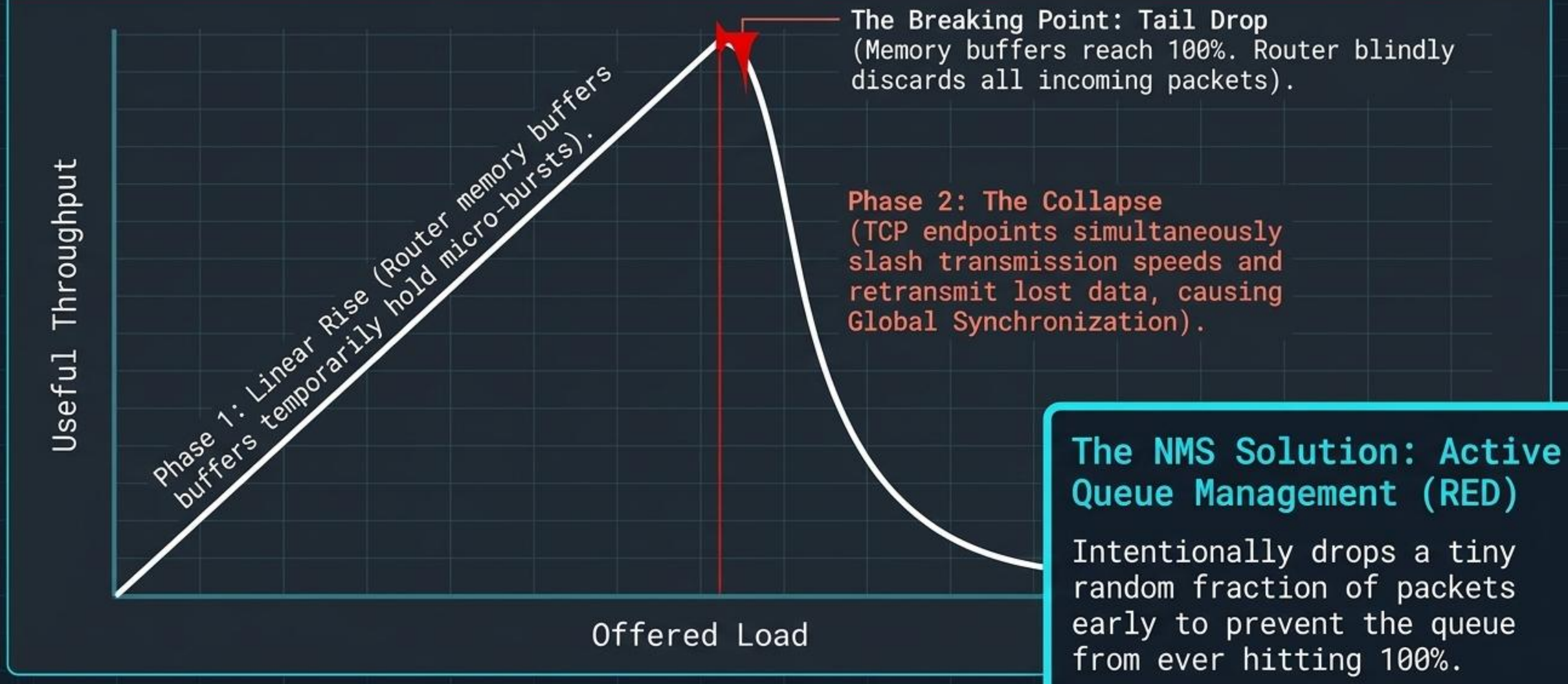
Zone 4

The physical transit time through copper or fiber.

NotebookLM

Congestion Collapse and Active Queue Management

The Congestion Collapse Curve



The NMS Solution: Active Queue Management (RED)

Intentionally drops a tiny random fraction of packets early to prevent the queue from ever hitting 100%.

NotebookLM

Modalities of Performance Measurement

Passive Observation (NetFlow / IPFIX)

Mechanism: Silently listening to authentic production traffic. Routers compile flow summaries based on the 5-tuple.

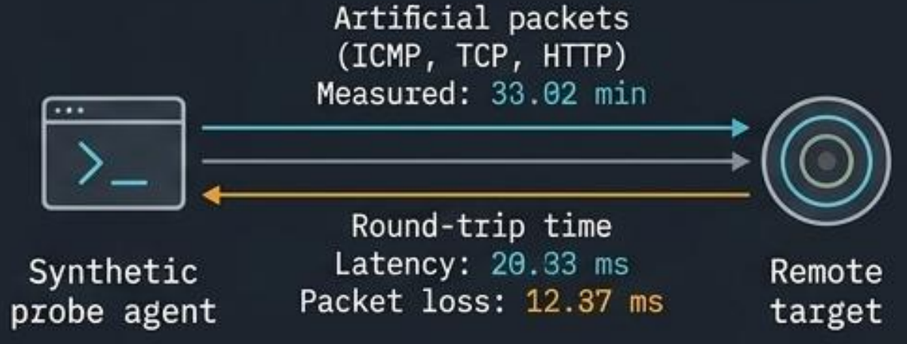
Best For: Capacity planning, traffic engineering, and identifying WHO is consuming bandwidth.

⚠ **Blind Spot:** Cannot measure performance on idle links with no active users.

Active Probing (Synthetic Monitoring)

Mechanism: Intentionally injecting artificial test traffic (ICMP pings, TCP handshakes, Layer 7 HTTP requests) and measuring the response.

Best For: SLA verification, continuous latency baselining, and detecting faults on idle backup links at 2:00 AM.

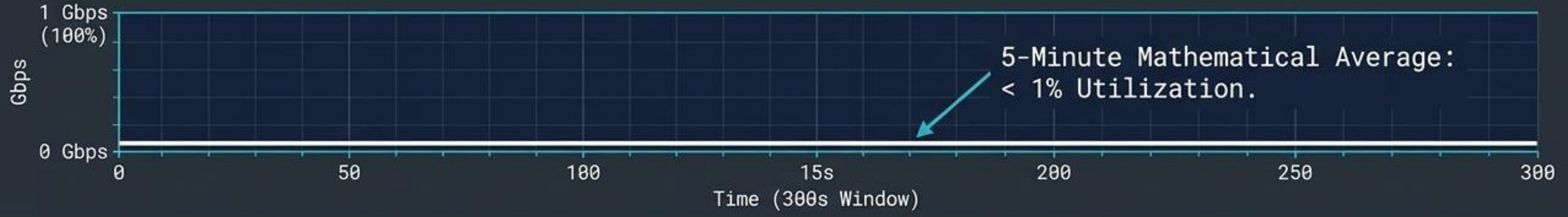


NotebookLM

Traffic Variance and the Monitoring Blind Spot

Actual Traffic on the Wire (Reality)

NMS Dashboard Reality (Standard Polling)



Key Takeaway: Low average utilization does not guarantee the absence of severe, instantaneous bottlenecks. Averages hide disasters. Advanced sub-second telemetry is required to capture true bursty variance.

NotebookLM

The 95th Percentile Reality Check

The Math (A 30-Day NMS Calculation)

1. **Sample:** Collect 8,640 data points (every 5 mins for a month).
2. **Sort:** Arrange from absolute highest traffic to lowest.
3. **Discard:** Delete the top 5% (the 432 absolute highest spikes, representing ~36 hours of micro-bursts).
4. **Select:** The 433rd sample becomes the mathematical truth for sustained network capacity.

The Synthesis

- Planning for the average masks congestion.
- Planning for the peak wastes budget on temporary anomalies.
- The 95th percentile acknowledges that temporary micro-bursts are safely absorbed by router memory queues, providing the exact high-water mark needed for ISP billing and physical scaling.

NotebookLM