NIAGARA NETWORKS

WHITE PAPER

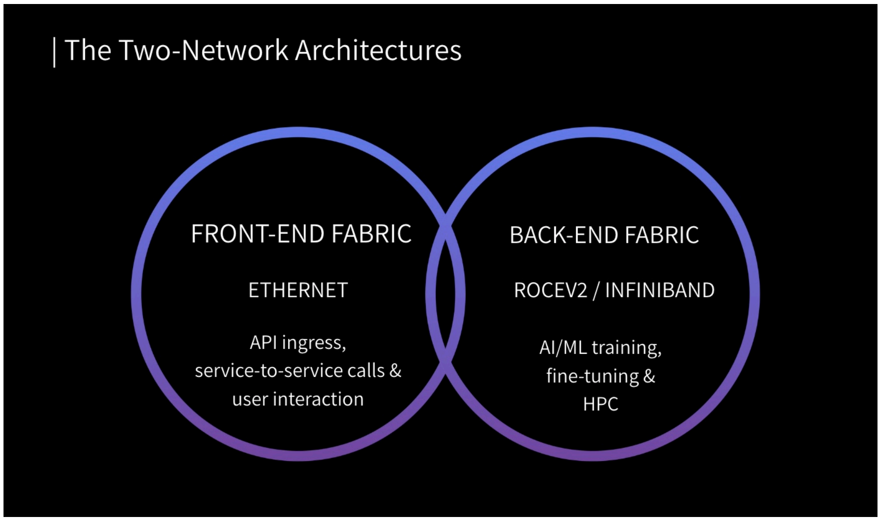
Eliminating the GPU Tax: Visibility Architecture for AI Data Centers

As nations battle for global AI leadership, investment in silicon is unprecedented. Yet a critical “Networking Wall” is emerging. In massive, distributed GPU clusters, the network is no longer a passive utility - it is the central nervous system.

AI data centers succeed when the network disappears as a bottleneck. In practice, it rarely does. Every duplicate packet we forward to tools, every unnecessary payload we ship to storage, and every microburst we fail to smooth steals time from GPUs and elongates Job Completion Time (JCT).

The Two-Network Architecture

Modern AI Data Centers do not run on a single network. They utilize a dual-fabric design that requires a specialized visibility approach. The front-end fabric is Ethernet-busy with API ingress, service-to-service calls, and user interaction. It tolerates modest latency and is where deep inspection, policy enforcement, and analytics live. The back-end fabric is a lossless high-bandwidth domain-RoCEv2 or InfiniBand-responsible for moving tensors, gradients, and checkpoints at 400/800 Gb/s. It is allergic to jitter. Any inline device that introduces queuing variance shows up immediately as GPU idle time. Visibility in this world must be surgical: passive and non-intrusive on the back-end, concise and deterministic on the front-end, and forensically defensible everywhere.



| The Two-Network Architectures

FRONT-END FABRIC

ETHERNET

API ingress,
service-to-service calls &
user interaction

BACK-END FABRIC

ROCEV2 / INFINIBAND

AI/ML training,
fine-tuning &
HPC

The Front-End Fabric (Standard Ethernet):

- Role: Connectivity for data ingestion, user APIs, and management.

- The Challenge: Massive North-South throughput (400G+) that overwhelms traditional security appliances. At these speeds, traditional security appliances collapse under buffer pressure, licensing constraints, or forced sampling - creating blind spots.

The Back-End Fabric (The "Compute" Cluster)

- Topology: Leaf-Spine (Fat-Tree). Every GPU is effectively one hop away from any other GPU to ensure "Any-to-Any" high-speed communication.
- Protocol: RoCEv2 (RDMA over Converged Ethernet). This is a "lossless" protocol that allows GPUs to bypass the CPU and write directly to each other's memory.
- The Problem: Even a 0.1% packet loss in this fabric can slash effective GPU utilization by over 15% due to "Synchronization Stalls" - observed in large-scale training clusters.

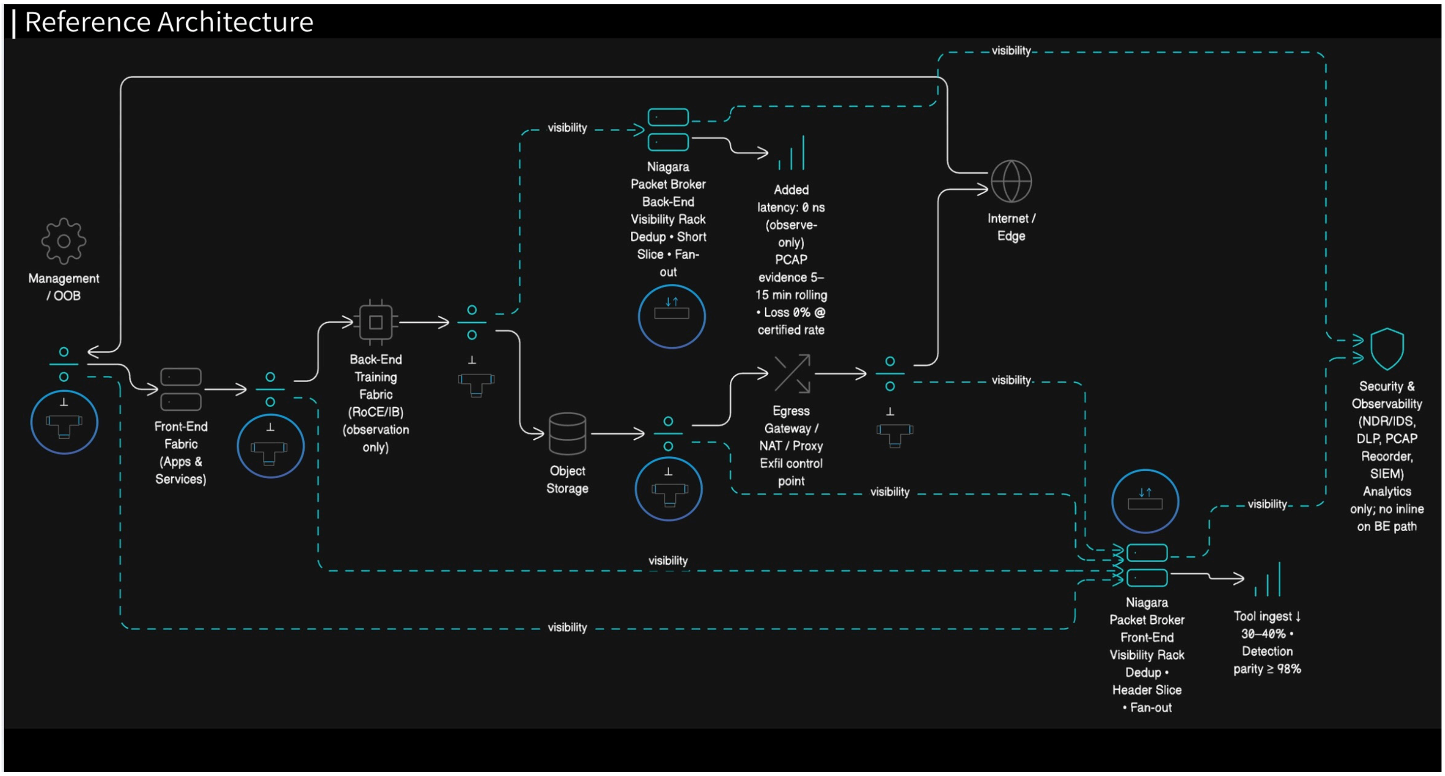
Visibility Led Design

Objective is not to build another analytics platform, but to engineer a clean, predictable data exhaust that downstream security and observability tools can consume without drowning. We do that by aggregating packet sources with passive optical taps, collapsing duplicates at ingress so tools see each conversation once, slicing payloads to the minimum each tool requires, and distributing traffic symmetrically across sensor farms. Where audits and incident response demand proof, we maintain rolling packet capture windows that can be produced on demand without instrumenting the training path.

Architectural Highlights

- Passive TAPs and High-Availability Bypass Switches at choke points (edge, leaf–spine, storage, egress).
- Deterministic de-duplication to cut 20–40% duplicate packets before tools.
- Header/byte slicing (e.g., 128–256 B) to preserve signal while lowering ingest.
- L2–L4 filtering and symmetric 5-tuple load balancing across sensor farms.
- Parallel feed to rolling PCAP recorders for defensible evidence.

| Reference Architecture


visibility
visibility
Niagara Packet Broker Back-End Visibility Rack Dedup • Short Slice • Fan-out
Added latency: 0 ns (observe-only) PCAP evidence 5–15 min rolling • Loss 0% @ certified rate
Internet / Edge
Management / OOB
Front-End Fabric (Apps & Services)
Back-End Training Fabric (RoCE/IB) (observation only)
Object Storage
Egress Gateway / NAT / Proxy Exfil control point
visibility
visibility
Security & Observability (NDR/IDS, DLP, PCAP Recorder, SIEM) Analytics only; no inline on BE path
visibility
visibility
visibility
Niagara Packet Broker Front-End Visibility Rack Dedup • Header Slice • Fan-out
Tool ingest ↓ 30–40% • Detection parity ≥ 98%

Reference Architecture - Solution Elements Placement

- TAPs: On Edge-FE uplinks, FE leaf-spine, storage north–south, egress links, and back-end pod edges.
- Front-End Broker: Inline or out-of-band; deduplication, 128–256B slice , L2–L4 filtering, and load balancing to NDR/IDS, DLP, PCAP & SIEM.
- Back-End Broker: deduplication, short slice, header-only monitoring profiles; never inline.

Niagara does not compete with tools - it enables them:
Niagara provides a clean, deterministic feed to security and observability-out of band. Passive TAPs and packet brokers aggregate links, remove duplicates, slice payloads to headers, and fan-out to tools. On the training fabric we observe only-no inline devices.

Use Cases

- Traffic Sanitization: AI training is repetitive. Sending 100% of raw 400G traffic to a security tool is an expensive waste of power and licenses.
- The Solution: Niagara's e-Packetron performs line-rate Deduplication and Packet Slicing. We strip payloads where inspection is not required, forwarding only the relevant headers to your NDR or IDS.
- The Impact: A security tool licensed for 100G can now monitor a 400G cluster. This eliminates the "GPU Tax" by ensuring the network remains clean and congestion-free.
- Zero-Latency Visibility (Intelligent Bypass): In a RoCEv2 fabric, you cannot place security tools "inline" without introducing latency that kills JCT.
- Solution: Niagara provides High-Availability Bypass Switches and Passive TAPs. We "observe" the compute fabric without adding a single nanosecond of delay - no queuing, no buffering, no retransmission impact.
- Impact: Full visibility into the "East-West" GPU communication for performance monitoring and security, with zero impact on training speed.

Conclusion: Architecture Over Brute Force

The race for AI dominance will be won by those who build the most efficient infrastructure. By moving from "dumb" packet delivery to an Intelligent Visibility Layer, AI operators can:

- Reduce OpEx: Lower security tool costs by up to 60%.
- Accelerate JCT: Ensure GPUs are always compute-bound, never network-bound.
- Ensure Sovereignty: Verify that every bit of national data stays where it belongs.

In doing so, network visibility stops taxing GPUs,and starts protecting their value.

| Visit www.niagaranetworks.com to learn more about our network visibility solutions.

About Niagara Networks

Niagara Networks™ delivers all the essential building blocks for high-performance visibility and network intelligence across physical and virtual network infrastructures. Our comprehensive portfolio includes Network Packet Brokers, Bypass Switches, Network TAPs, and a unified orchestration layer for seamless visibility and control. We design, develop, and manufacture our products in Silicon Valley, USA. Thanks to these integrated in-house capabilities, Niagara Networks is agile in responding to market trends and meeting the customized needs of service providers, enterprises, data centers, and government agencies. www.niagaranetworks.com.