Module 3: Monitoring Portal Access & Walkthrough

Transitioning to proactive VLL managment

comBOX Certified Partner Program (CCPP)

Proactive Monitoring and Operational Control

Reactive IT

- Waiting for customer complaints to identify outages.
- High Mean Time to Repair (MTTR).
- High risk of SLA financial penalties.

Proactive NOC Operations



Centralized, single-pane-of-glass visibility across all deployments.



Instant identification of failing underlying ISPs before the customer notices.



Protected profit margins through significantly reduced support hours.

Enterprise Zabbix Architecture & Multi-Tenancy



comBOX Core

Enterprise-grade Zabbix monitoring engine providing centralized, real-time telemetry and automated email alerts for all active comBOX VLL services.

Partner Master Access

Single set of portal credentials.

Streamlined access for comprehensive management of all client environments.

Global visibility across all deployed comBOX VLLs under the partner account.

Real-time, aggregated view of performance and health metrics for every deployed service.

Full diagnostic drill-down capabilities.

Granular access to deep-dive data, logs, and historical performance trends for troubleshooting.

End-User Segregation

Optional, highly restricted login credentials.

Controlled entry with limited permissions for specific user roles.

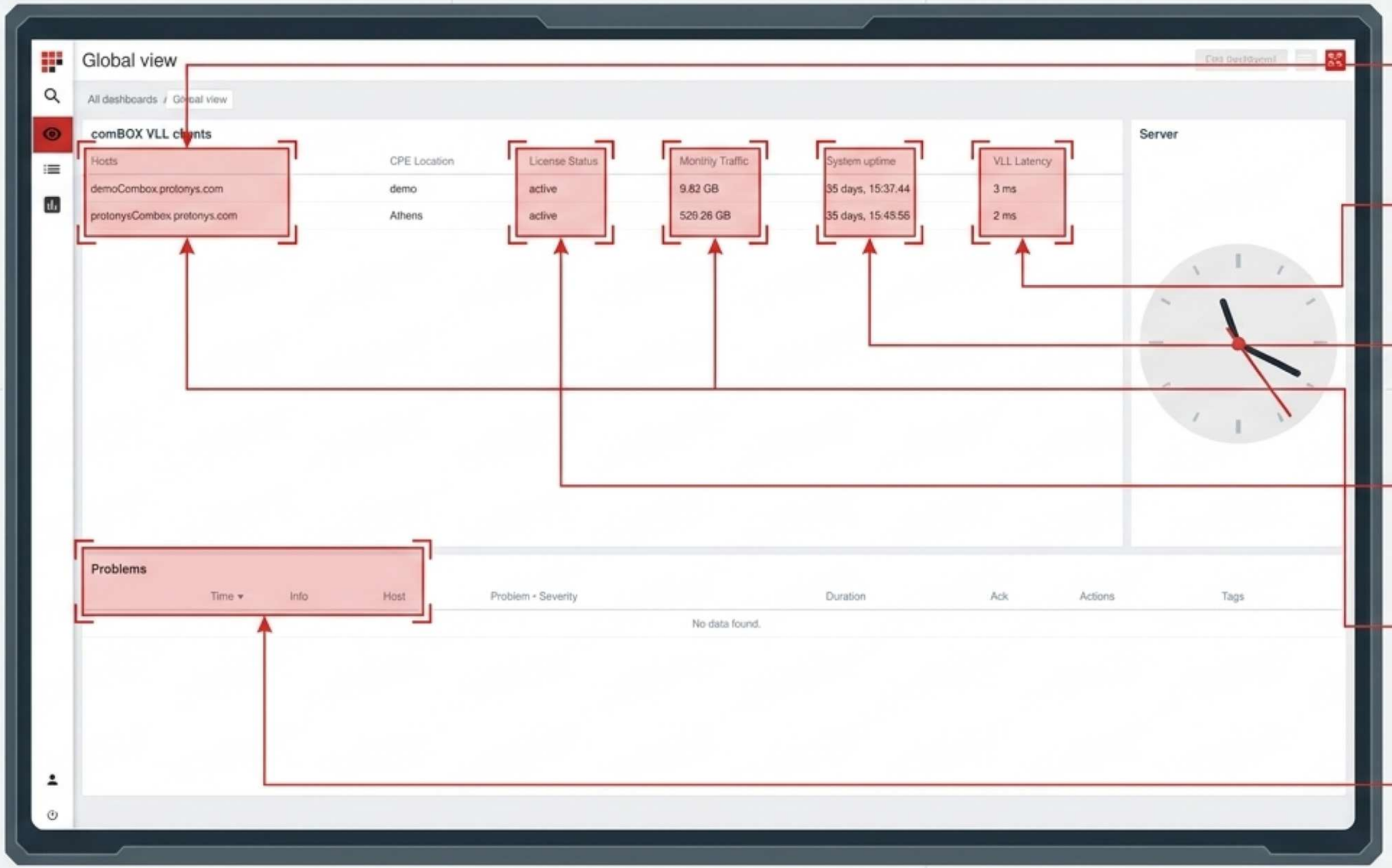
Strictly isolated view: Customers can only monitor their specific services.

Secure environment where users view only data relevant to their own deployments.

Builds customer trust through transparency without exposing your wider fleet or administrative controls.

Provides necessary insights while maintaining complete security and confidentiality of the partner's infrastructure.

The Global Dashboard: Fleet-Wide Visibility



Customer Hostname:
The unique identifier for the specific deployment.

License Status:
Verifies active service and billing state.

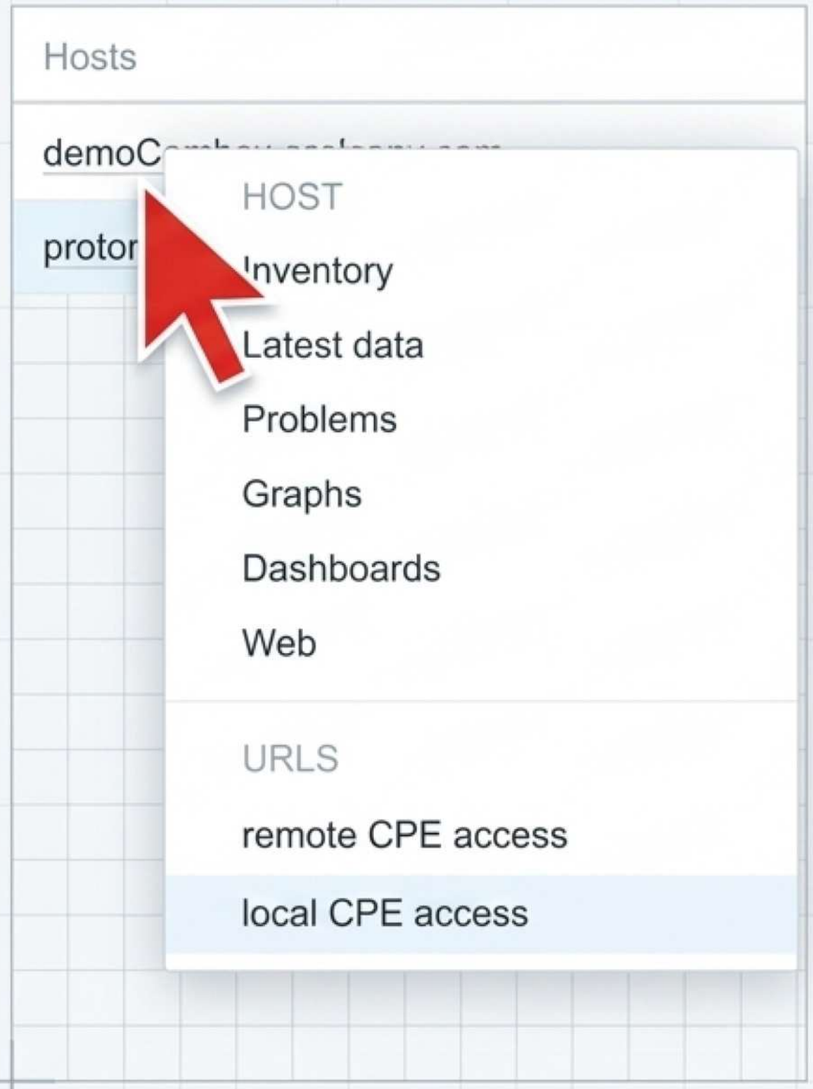
Monthly Traffic:
High-level bandwidth consumption metric.

System Uptime:
Continuous operation duration since last reboot.

VLL Latency:
Real-time indicator of the bonded tunnel's responsiveness.

Current Problems:
The immediate flag for active network alarms or localized hardware faults.

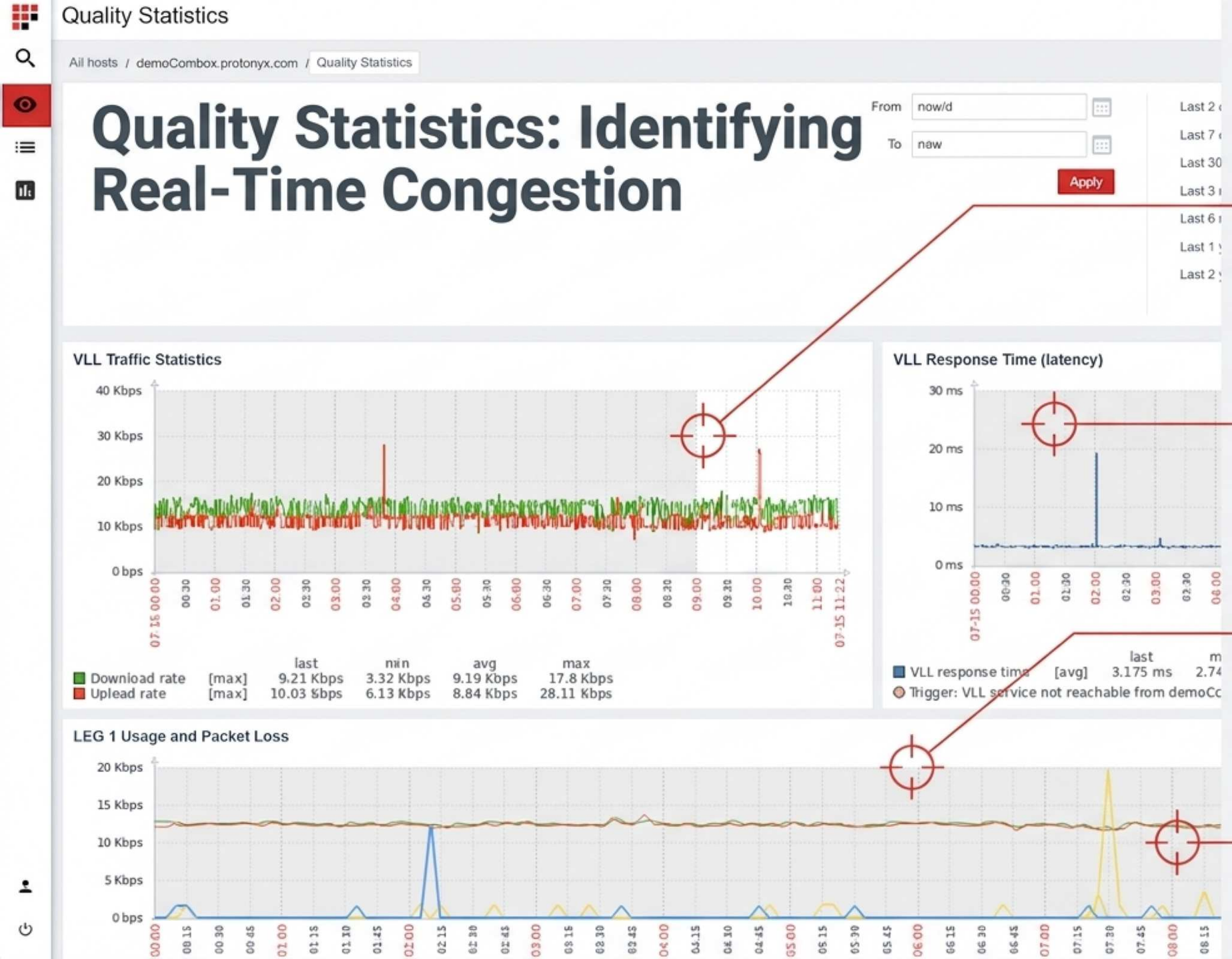
Host Navigation: Transitioning from Macro to Micro



Analytical Matrix

Phase 1: Diagnostics (Read-Only Telemetry)	
Inventory & Latest Data:	Raw system parameters and current polling data.
Problems:	Active and acknowledged system alarms.
Graphs & Dashboards:	Visual, historical, and real-time performance rendering.

Phase 2: Remediation (Active Management)	
Remote CPE Access:	Secure routing to the appliance GUI over the WAN/Internet.
Local CPE Access:	Direct access to the appliance GUI via the customer's local LAN.



Diagnostic Translation Matrix

VLL Traffic Statistics

Confirms active data flow; identifies if customer is maxing out their licensed bandwidth.

VLL Response Time (Latency)

Spikes indicate underlying ISP routing inefficiencies or severe link saturation.

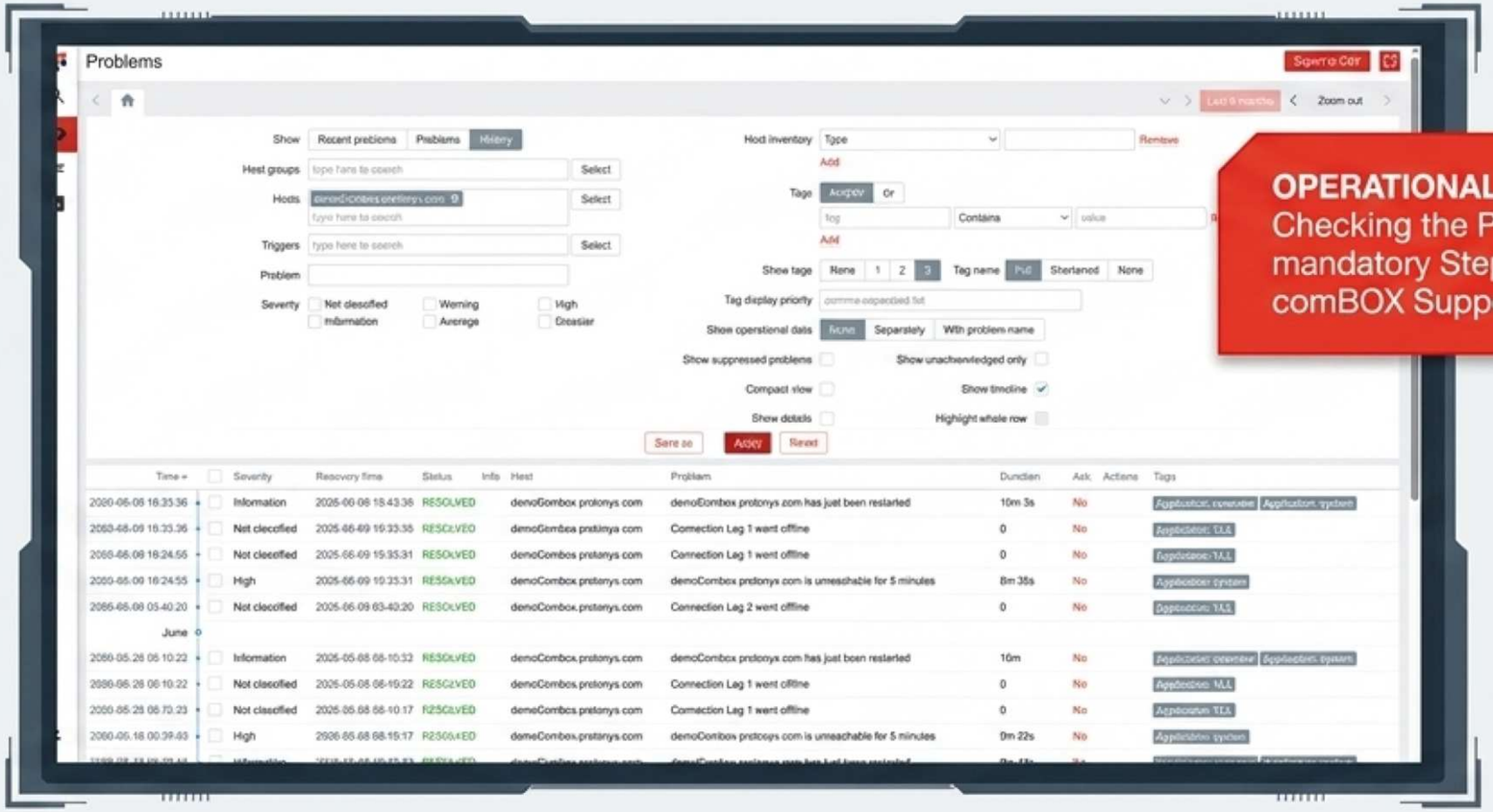
Individual WAN Leg Utilization

Exposes exactly which underlying ISP connection is underperforming or hoarding traffic.

Packet Loss

Identifies physical line degradation, poor 5G/LTE signal, or faulty ISP peering.

The Problems View: Tier 1 Incident Remediation



OPERATIONAL MANDATE:
Checking the Problems View is mandatory Step 1 before opening a comBOX Support Ticket.

Root Cause Analysis

Alarm: Connection Leg offline

Diagnosis: An underlying ISP link has failed.

Impact: The comBOX VLL absorbs the failure; customer stays online, but bandwidth is reduced.

Root Cause Analysis

Alarm: High Latency

Diagnosis: ISP routing congestion or saturation.

Root Cause Analysis

Alarm: Device Unreachable / Service Interruption

Diagnosis: Catastrophic failure.

Likely Cause: Site power outage, physical cable disconnection, or failure of all underlying WAN links simultaneously.

Performance Graphs: Forensics & Capacity Planning



AVAILABLE TELEMETRY: VLL TRAFFIC // LATENCY // CPU, RAM, HDD UTILIZATION // WAN LEG TRAFFIC // PACKET LOSS

Pillar 1: Retroactive Troubleshooting (Technical Forensics)

- **Investigating** intermittent issues reported after the fact (e.g., overnight drops).
- **Identifying** exact timestamps of ISP micro-outages.

Pillar 2: Capacity Planning (Commercial Upselling)

- **Monitoring** long-term VLL traffic trends to identify consistent bandwidth saturation.
- **Actionable Insight:** High resource utilization graphs provide data-driven evidence to upsell the client to a higher-tier service bundle (e.g., Silver to Gold).

Remediation Pathways: Remote vs. Local Access

Both methods provide direct access to the comBOX VLL Web Manager GUI for configuration and management—but the routing differs entirely.

Remote CPE Access

Pathway
Traverses the Internet/WAN via the bonded VLL tunnel.

Dependency
Requires the VLL service to be online and at least one WAN leg functioning.

Primary Use
Off-site configuration, daily monitoring, standard remote troubleshooting.

Local CPE Access

Pathway
Traverses the customer's internal LAN.

Dependency
Requires physical proximity or remote access to a local network device (e.g., jumpbox). Uses initial deployment credentials.

Primary Use
Initial hardware setup, or emergency fail-safe access when all WAN links are dead and device is isolated from the internet.

NOC Standard Operating Procedure & Live Demo

NOC Troubleshooting Flowchart



Trainer's Live Demo Checklist

- **Step 1:** Authenticate & verify Global View.
- **Step 2:** Open a customer's Quality Statistics.
- **Step 3:** Interpret a live or historical alarm in the Problems page.
- **Step 4:** Demonstrate graph utilization for capacity planning.
- **Step 5:** Launch Remote CPE Access to the appliance GUI.