ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Managed Networks for ISPs and MSPs

Multi-organisation operations, SLA reporting and service-desk integration on one platform

ISPs · MSPs · MSSPs

Document reference	Version	Date	Published by
CN/SDW/AN/MSP/v1.0	1.0	November 2026	ChiefNET Private Limited

Contents

1. Overview
2. The Challenge
3. The ChiefNET Solution
4. Reference Architecture
5. Key Benefits
6. Capability Map
7. Deployment Summary
8. Conclusion

Also available online at chiefnet.io/use-cases/sd-wan/msp-isp-managed-networks/

Overview

Internet service providers, managed service providers (MSPs) and managed security service providers (MSSPs) increasingly offer networking as a service: they deliver, operate and support connectivity for many customers at once, under contractual service levels. To do that efficiently, they need a platform that separates customers cleanly, measures service levels accurately, and fits into the tools their operations centres already use.

This application note describes the ChiefNET SD-WAN features designed for service providers: multi-organisation administration, SLA monitoring and reporting, configurable data retention, export to logging and service-management systems, and graded customer access.

The Challenge

Consider an MSP operating networks for 40 business customers with a combined 1,500 sites. Its operations team deals with the following:

- **Many customers, many consoles.** Switching between separate accounts or tools for each customer slows down the operations centre.
- **SLA disputes.** When a site goes offline, the cause may be the CPE, a local power cut or the ISP's access network. Without clear evidence, the provider absorbs penalties it does not owe, or customers lose trust.
- **Alert overload.** Raw alerts arrive by email from many systems and are hard to route to the right engineer.
- **Disconnected tools.** Monitoring data must reach the provider's log servers, dashboards and ticketing system, not stay in a separate portal.
- **Customer visibility.** Customers want to see their own network, and some want to make changes, without seeing anyone else's devices.
- **Site visits.** Every technician visit for installation or replacement adds cost and delay.

The ChiefNET Solution

ChiefNET runs every customer network from a single ChiefNET Orchestrator, with the tools a provider needs to separate customers, prove service levels and work within its existing operations centre.

Multi-organisation administration

Each customer is a separate organisation in the ChiefNET Orchestrator. Traffic and management data are isolated per customer, and each customer sees only its own devices. Provider staff with multi-organisation administrator rights can manage many organisations from a single account, so the operations centre works in one place.

Access is controlled through several login levels:

- **Full administrator**, who can change configuration and manage users for an organisation.
- **Read-only administrator** and **read-only limited user**, for customer staff or provider engineers who need visibility without change rights.
- **Multi-organisation administrator**, for provider staff responsible for several customers.

All Orchestrator access uses HTTPS with two-factor authentication.

SLA monitoring and reporting

Every ChiefNET CPE monitors itself and its WAN links continuously. WAN ports and tunnels are probed for packet loss, latency and jitter, and system health such as CPU temperature, CPU load and disk usage is tracked.

The SLA reporting system draws a clear distinction between three causes of downtime:

- **Device availability**: whether the ChiefNET CPE itself was operating.
- **Power outages** at the site.
- **ISP link availability**: whether the service provider's access network was delivering service, including next-hop equipment outside ChiefNET's control.

Reports are available for daily, monthly or custom periods, per WAN link and per ISP, along with WAN and device availability reports. Providers can reconcile contractual SLAs with measured availability, and customers can use the same reports to hold their own ISPs to account.

Data retention

Monitoring data is stored in a time-series database that supports graphing, querying, filtering and report generation. The retention period is configurable, so providers can keep data for as long as their contracts or policies require. Alerts on the Orchestrator WebUI are retained for 30 days and can be exported as CSV.

Events, alerts and notifications

ChiefNET raises events for network conditions (WAN port down, link quality, WAN failover, tunnel status and latency, bandwidth utilisation), system conditions (CPU, temperature, disk) and security conditions (configuration changes, new device provisioning, user logins and logouts). Thresholds are configurable.

Notifications can be delivered by email and to Telegram groups, so an on-call team can follow a customer's alerts in a shared channel.

Integration with provider tools

- **Splunk and syslog.** Events can be exported in real time to external Splunk or syslog servers for central logging and correlation.

- **Zoho ServiceDesk and OpManager.** ChiefNET integrates with Zoho ServiceDesk and OpManager, so that ChiefNET devices and events can be handled within existing service-desk and monitoring workflows. A built-in customer issue management system is also available.
- **Grafana dashboards.** A Grafana-based portal provides customisable dashboards, alerts and data collection, hosted in the cloud or installed on the provider's own servers.
- **SNMP v2.** Read-only SNMP v2 access, restricted to defined OIDs, lets existing network management systems poll ChiefNET devices.

Visibility into customer LANs

Beyond WAN health, ChiefNET provides LAN device activity monitoring, including usage and top talkers, and IP-level interface statistics. When a customer reports a slow network, engineers can see quickly whether a single host or application is consuming the link.

Fewer site visits

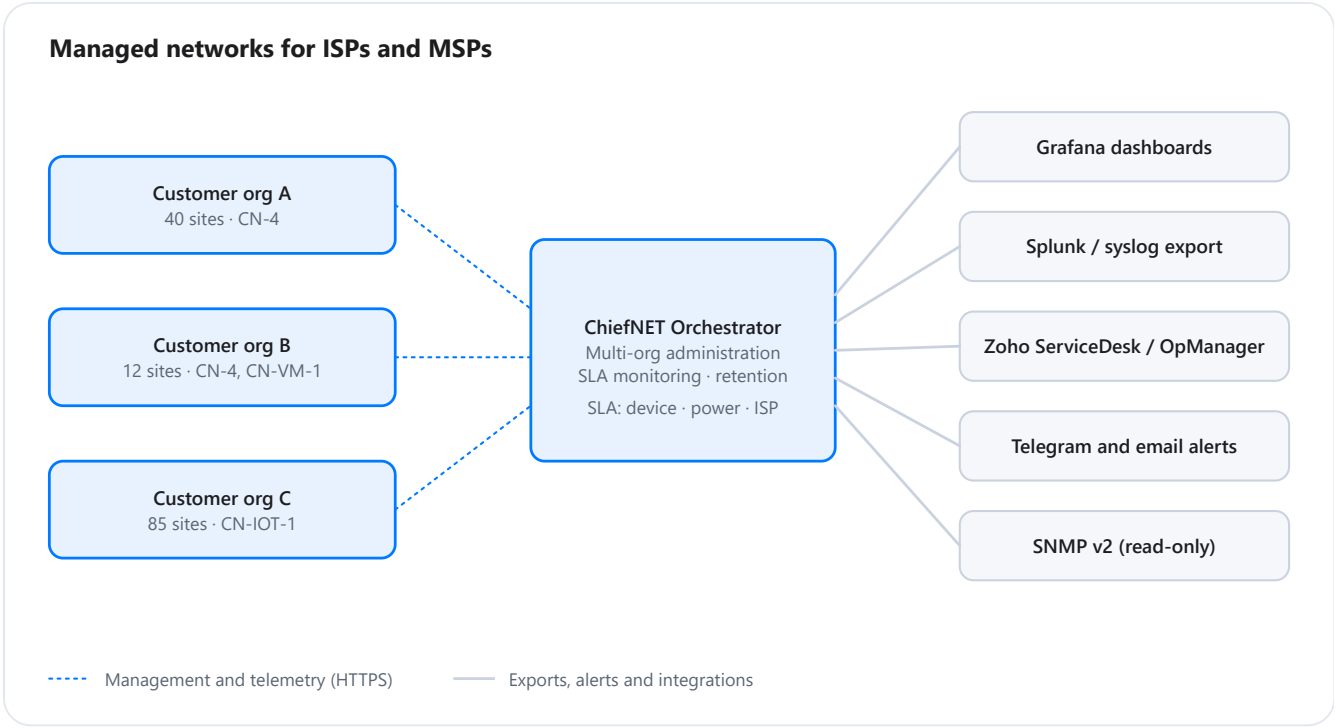
Devices are pre-provisioned before they ship and need only power and cables on site. Software is updated remotely from the Orchestrator. If a device must be replaced, the full configuration is held centrally, so the replacement can be configured identically to the original. Where a USB cellular interface is fitted, it provides an additional path for remote management.

Flexible hosting

The Orchestrator and gateways can run on ChiefNET's cloud, on the provider's own infrastructure, or in a hybrid model, with high availability for the Orchestrator, gateways and CPEs. This lets a provider host the platform in its own data centres where regulation or customer contracts require it.

Reference Architecture

The diagram shows three customer organisations, each with its own set of ChiefNET CPEs, reporting to a single multi-organisation ChiefNET Orchestrator. The Orchestrator provides SLA monitoring that separates device, power and ISP availability, and feeds Grafana dashboards, Splunk or syslog servers, Zoho ServiceDesk and OpManager, Telegram and email notifications, and SNMP v2 polling.



Customer organisations report to a multi-organisation ChiefNET Orchestrator, which feeds dashboards, log servers, service-desk tools, alerts and SNMP.

Key Benefits

- **One console for every customer.** Multi-organisation administration with strict per-customer isolation.
- **Defensible SLAs.** Reports separate device, power and ISP downtime, reducing disputes.
- **Fits the existing NOC.** Splunk, syslog, Zoho, Grafana and SNMP integration keep data in familiar tools.
- **Faster response.** Telegram and email notifications reach on-call engineers directly.
- **Right-sized customer access.** Full, read-only and limited roles let customers see their own network safely.
- **Lower field costs.** Zero-touch installation, remote software updates and centrally stored configurations reduce site visits.

Capability Map

ChiefNET capability	How it is used here
Multi-organisation administration	Manages all customer organisations from one provider account
SLA monitoring and reports	Separates device, power and ISP link availability over daily, monthly or custom periods

ChiefNET capability	How it is used here
Configurable data retention	Keeps monitoring data for the period required by contracts
Splunk and syslog export	Sends events in real time to the provider's logging platform
Telegram and email notifications	Alerts on-call teams to failovers, outages and configuration changes
Zoho ServiceDesk and OpManager integration	Feeds network events into existing ticketing and monitoring
Grafana dashboards and SNMP v2	Provides custom dashboards and polling by existing management systems
Customer access levels with two-factor login	Gives each customer the right level of visibility and control

Deployment Summary

1. Choose cloud, on-premises or hybrid hosting for the Orchestrator and gateways.
2. Create an organisation for each customer and assign provider and customer roles.
3. Configure notification channels, Splunk or syslog export, Zoho integration, Grafana dashboards and SNMP access.
4. Set data retention and SLA report schedules to match customer contracts.
5. Pre-provision and ship CPEs; confirm devices come online and appear in reports.

Conclusion

Service providers need more than a reliable edge device: they need to run many customer networks efficiently and prove the service they deliver. ChiefNET SD-WAN combines multi-organisation management, SLA reporting that separates device, power and ISP outages, and integration with the logging, dashboard and service-desk tools that operations centres already use.

ChiefNET

About ChiefNET Private Limited

ChiefNET Private Limited, founded in 2020 and headquartered in Coimbatore, India, builds secure networking products for enterprises and critical infrastructure: ChiefNET SD-WAN, a cloud-managed network platform for multi-site organisations, and ChiefNET OT Shield, a hardware-enforced data diode for operational technology.

---

contact@chiefnet.io · chiefnet.io
DVP Building, First Floor, No. 4, Kalapatti Main Road, Civil Aerodrome Post, Nehru Nagar West, Coimbatore, Tamil Nadu 641014, India