ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Branch Resilience with Multiple WAN Links

Dual ISPs, 4G/5G backup, quality-based failover and hot-standby CPEs

Retail · Financial services · Distributed enterprises

Document reference	Version	Date	Published by
CN/SDW/AN/RESIL/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/branch-resilience-multi-wan/

Overview

For most distributed organisations, a branch without a network is a branch that cannot trade. Point-of-sale systems stop, ERP screens freeze, calls drop and staff wait. Yet branch connectivity usually depends on local ISPs whose service quality varies by location and by hour, and on a single router that is a single point of failure.

This application note describes how ChiefNET SD-WAN keeps branches running through link degradation, ISP outages and equipment failure, using multiple WAN links, continuous quality measurement, policy-based failover and load balancing, and redundant CPEs. It also shows how to use a metered 4G/5G link as a backup without letting it be consumed by non-essential traffic.

The Challenge

Consider an organisation with 200 branches. Each has a fixed broadband or fibre connection, and many have a 4G or 5G connection as backup. The operations team reports recurring issues:

- **Links that are up but unusable.** An ISP link can stay “up” while losing packets or adding seconds of delay. Simple up/down failover does not react, and users suffer.
- **Idle backup capacity.** The second link sits unused until the primary fails completely.
- **Expensive backup links drained.** When failover happens, everything moves to the 4G link, including video streaming and software updates, and the data allowance is quickly used up.
- **Single points of failure.** A failed router or power supply takes the entire branch offline until a replacement arrives.
- **Dependence on central systems.** If the management platform is unreachable, some solutions cannot keep branches working normally.
- **Disputes with ISPs.** Without independent measurements, it is hard to hold ISPs to their service levels.

The ChiefNET Solution

ChiefNET places a pre-provisioned CPE at each branch, connects it to the ChiefNET Cloud WAN over every available link, and manages it from the ChiefNET Orchestrator.

Continuous link-quality monitoring

Every ChiefNET CPE continuously probes each WAN link and each SD-WAN tunnel, measuring packet loss, round-trip latency and jitter. These measurements drive automatic decisions rather than just status displays:

- A link with packet loss above 11% is reported as unstable; above 90% it is treated as unusable. A link that does not answer probes for 30 seconds is declared down.

- Thresholds for switchover and switchback are configurable, globally and per application.
- Tunnel latency is monitored, with an alert raised above a configurable threshold (three seconds by default).

Even with no explicit policy configured, a CPE with several WAN links monitors them for Internet access and moves traffic to a working link.

Policy-based failover

ChiefNET Traffic Policy lets administrators define classes of traffic by subnet, port, protocol, application or domain, and decide how each class uses the available links:

- **Primary and backup.** Each class can have its own primary and secondary WAN port. Payment traffic might prefer WAN 1, while voice prefers WAN 2.
- **Quality-based selection.** A class can require a maximum latency, jitter or loss; the CPE places it on whichever link currently meets that requirement and keeps a backup assigned.
- **Tunnel failover.** Enterprise tunnels move to the best available ISP automatically, and multiple tunnels can run simultaneously.

Failover and load balancing can be applied at the same time, so traffic uses all healthy links in normal operation and concentrates on the remaining links during a fault.

Weighted load balancing

Where two links are healthy, ChiefNET can load-balance selected traffic across both, with weights that control the share each link carries. Balancing is done per flow rather than per packet, which avoids out-of-order delivery that would harm application performance. This turns the backup link into useful capacity instead of idle insurance.

Protecting metered 4G/5G links

The 4G/5G link is often the most expensive per gigabyte. ChiefNET's exclusive WAN port selection and sensitive-traffic exclusive forwarding let administrators specify that certain classes of traffic may use only particular links. For example, streaming, social media and bulk updates can be limited to the fixed line; if that line fails, this traffic is dropped rather than moved to LTE. Point-of-sale, ERP and voice traffic keeps primary and backup paths at all times.

Combined with QoS, which sets minimum and maximum bandwidth per class, this ensures that a branch running on its backup link still serves its critical applications properly.

The CN-4 supports an optional built-in LTE/5G interface, and qualified USB LTE or 5G modems can be added as another WAN connection.

Hot-standby CPE with VRRP

For branches that cannot tolerate a device failure, two CN-4 appliances can be installed as a VRRP-based Edge Device HA pair. Each device monitors the other. If the active device fails, including through a local power fault, or if one of its network interfaces fails, the standby takes over the

gateway role and all services. A standby device can be added later to a site that started with a single CPE.

If a CPE is damaged, the full configuration is held centrally, so a replacement device can be configured identically to the original.

Autonomous operation

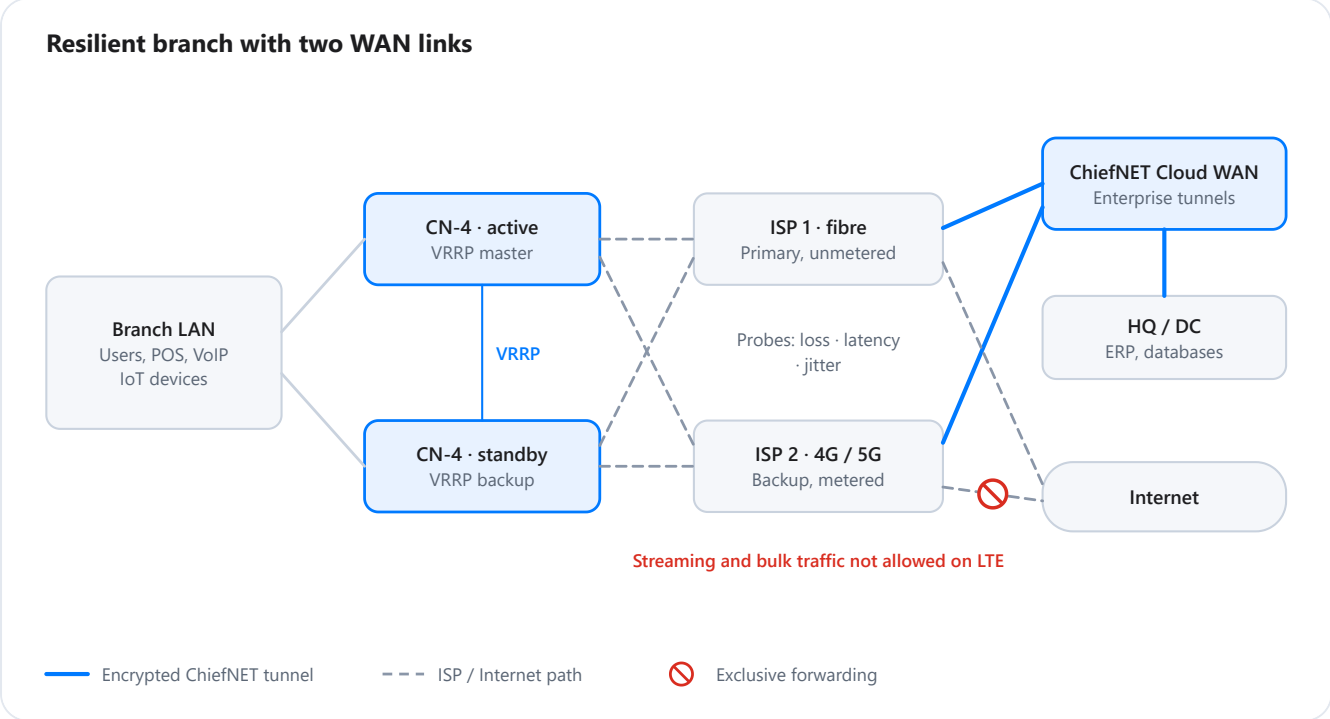
ChiefNET CPEs do not need constant contact with the Orchestrator. If the management plane is unreachable, each branch continues to operate on its own with its configured policies.

Visibility and ISP accountability

The Orchestrator shows the status and quality of every port and tunnel. Events such as WAN failover, tunnel WAN change and WAN IP change are logged and can be sent by email or Telegram. ISP SLA reports separate downtime caused by the ISP from power outages at the site and from downtime of the ChiefNET device, giving the organisation evidence for discussions with its providers.

Reference Architecture

The diagram shows a branch LAN served by two CN-4 CPEs in a VRRP active/standby pair. Both CPEs connect to a fibre link and to a metered 4G/5G link. Encrypted tunnels to the ChiefNET Cloud WAN run over both links, reaching HQ and data-centre applications. Internet-bound traffic uses local breakout on the fibre link, while streaming and bulk traffic is not allowed on the LTE link.



A VRRP pair of CN-4 CPEs uses a fibre link and a metered 4G/5G link, failing over on loss, latency or jitter while keeping non-critical traffic off LTE.

Key Benefits

- **Faster reaction to poor links.** Failover is triggered by loss, latency and jitter, not only by a link going down.
- **More usable bandwidth.** Weighted, per-flow load balancing puts both links to work.
- **Controlled backup costs.** Exclusive forwarding keeps metered 4G/5G capacity for critical applications.
- **No single device failure.** VRRP hot-standby CPEs protect the branch gateway.
- **Resilient when isolated.** Branches keep operating without contact with the Orchestrator.
- **Evidence for ISP SLAs.** Reports separate ISP downtime from power outages and device downtime.

Capability Map

ChiefNET capability	How it is used here
WAN and tunnel link-quality monitoring	Measures loss, latency and jitter continuously on every link and tunnel
Quality-based failover with configurable thresholds	Moves each traffic class to a link that meets its requirements
Weighted, per-flow load balancing	Uses both links in normal operation without packet reordering
Exclusive WAN port selection	Keeps non-critical traffic off metered 4G/5G backup links
Hierarchical QoS	Maintains service for critical applications on reduced capacity
Edge Device HA (VRRP)	Provides a hot-standby CPE that takes over on device or interface failure
Autonomous offline mode	Keeps branches running without the Orchestrator
ISP SLA reports and alerts	Documents ISP performance and notifies staff of failover events

Deployment Summary

1. Classify branch traffic into critical, normal and non-essential classes, and record each site's links and data limits.
2. Define per-class primary/backup links, quality thresholds, load-balancing weights and exclusive-link rules.
3. Assign QoS profiles so that critical traffic keeps guaranteed bandwidth during failover.
4. Deploy CN-4 units, with a second unit for VRRP at critical sites, and connect both WAN links.

5. Test failover by disconnecting each link and each CPE, then enable alerts and SLA reports.

Conclusion

Branch resilience needs more than a second cable. ChiefNET SD-WAN measures link quality continuously, moves each class of traffic to the right link, uses backup capacity sensibly without draining metered connections, and protects against device failure with VRRP hot-standby CPEs. The result is a branch network that stays productive through the everyday faults of local ISPs and equipment.

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