

NSE NGFW • CAMBIUM Wi-Fi • mmWave Backhaul • Smart Switching



Resilient Connectivity & Security for Education & Enterprises in the Pacific

Campus backhaul, Secure Wi-Fi, remote access and cellular resilience
— built for universities, schools and distributed enterprises across the Pacific.

Roy Wittert – Regional Sales Director
FNU NCIT Conference, Fiji
2026



What We'll Cover

01

The Challenge

Why campuses & distributed enterprises need a new approach to connectivity

02

Campus & Site Backhaul

LEO satellite + NSE for connecting remote campuses, branches and outdoor sites

03

Unified Campus Wi-Fi

Cambium ONE Network for secure, high-density Wi-Fi across buildings and outdoor spaces

04

Secure Remote Access

Solving CGNAT and multi-site VPN challenges for IT teams

05

Resilience & Failover

Cellular backup for always-on connectivity

06

Business Value, Why Cambium & Next Steps

Benefits, use cases, and how FNU NCIT and Pacific institutions can engage

Connecting Campuses & Enterprise Sites

Universities, schools and distributed organisations across the Pacific face the same infrastructure gaps

No Fiber Access

Remote campuses, satellite teaching sites and rural offices often have no terrestrial fiber, leaving institutions dependent on costly alternatives.

High Backhaul Costs

Microwave links and leased circuits are expensive to deploy and maintain across dispersed island geographies.

Limited Resiliency

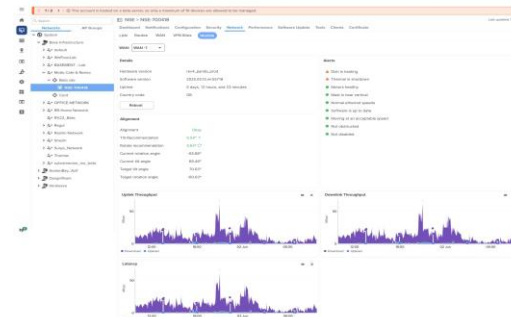
Single-path connectivity creates a single point of failure with no failover for critical learning and business services.

Complex Multi-Vendor Operations

Separate vendors for WAN, LAN, Wi-Fi and security increase operational complexity and slow troubleshooting for lean IT teams.

Campus & Remote Site Backhaul via LEO + NSE

- Replace expensive or unavailable terrestrial backhaul with LEO satellite + NSE overlay
- NSE3000 deployed at remote campuses / branch sites as spoke, NSE4000 as hub or use TailScale
- WireGuard IP overlay delivers a secure, encrypted backhaul link (SD-WAN)
- NSE supports application management and control. Help optimise use of the Starlink backhaul bandwidth.
- Web filtering (DNS) helps schools meet, US Children's Internet Protection Act (CIPA) or the UK's Keeping Children Safe in Education (KCSIE)



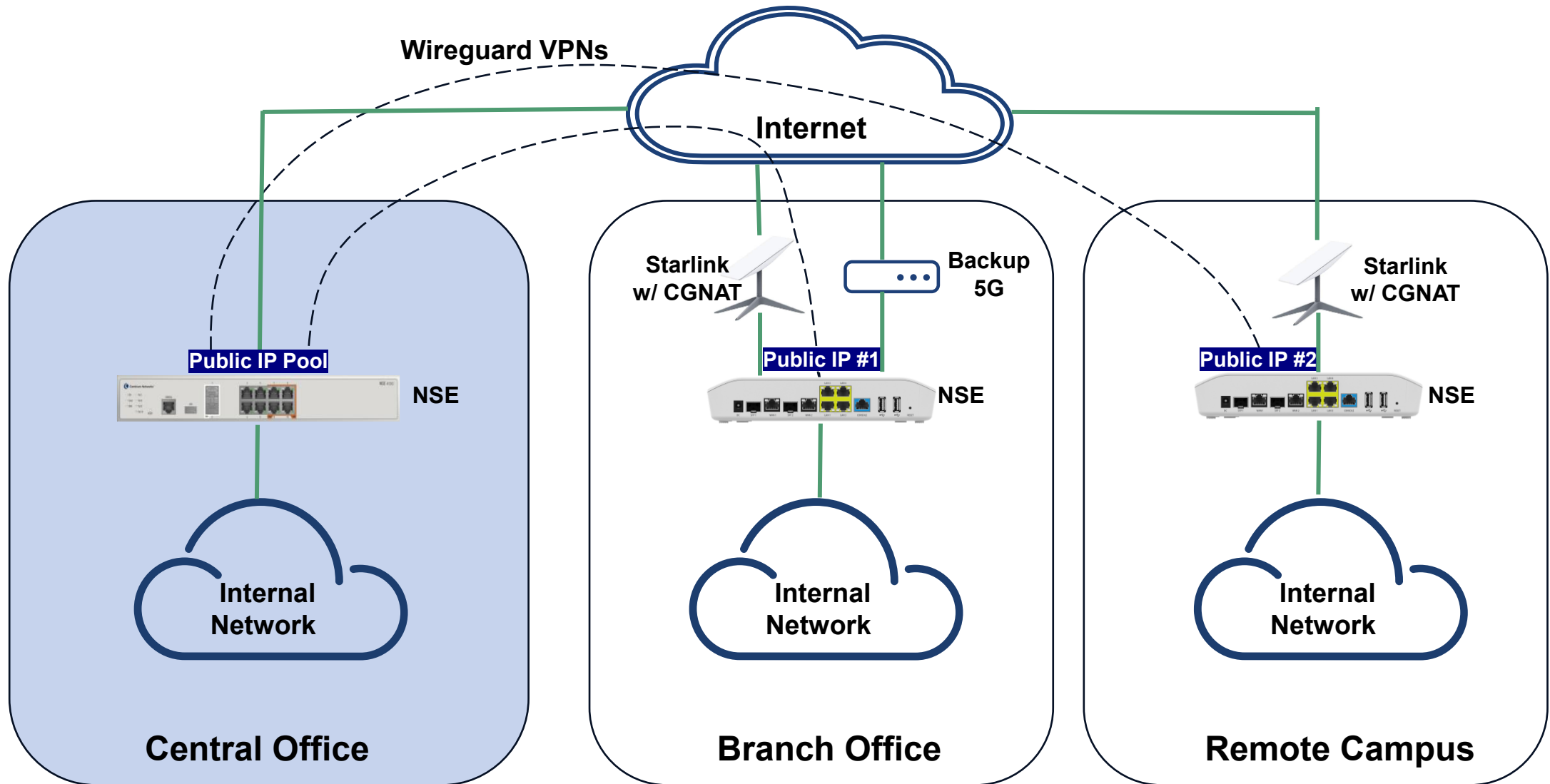
Campus Backhaul via LEO + NSE

- Connecting a remote campus or branch site back to the core network
- cnMaestro Monitoring



WireGuard encrypted overlay secures every link end-to-end

NSE-Starlink Integration – Public IP with Wireguard VPN



Unified Campus Wi-Fi via Cambium ONE Network

- Deliver reliable, high-density Wi-Fi 6/6E & 7 across lecture halls, libraries, dorms and outdoor campus spaces
- NSE + cnMatrix + Cambium Wi-Fi (XV/XE) combine into a single managed network
- Identity-based authentication (RADIUS / SSO) for students, staff and guests
- mmWave Campus Connectivity – cnWave 60GHz



Cambium ONE Network



Every layer — WAN, LAN, Wi-Fi, security and management — from a single vendor



NSE (SD-WAN Gateway)

Secure SD-WAN, firewall and IP overlay via WireGuard. NSE3000 at sites, NSE4000 as hub.



cnMatrix (PoE Switch)

Power-over-Ethernet switching and network segmentation at every building or site with added value of Policy Based Automation (PBA)



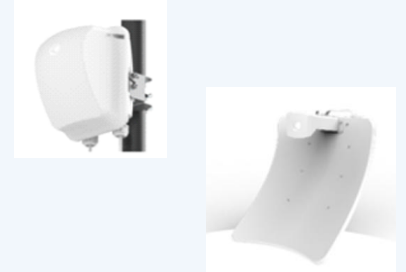
Cambium Wi-Fi 6/6E + 7 (XV/XE/X7)

Enterprise-grade access points delivering high-density Wi-Fi coverage.



cnMaestro (Management)

Cloud-based single pane of glass for unified management across the whole estate.

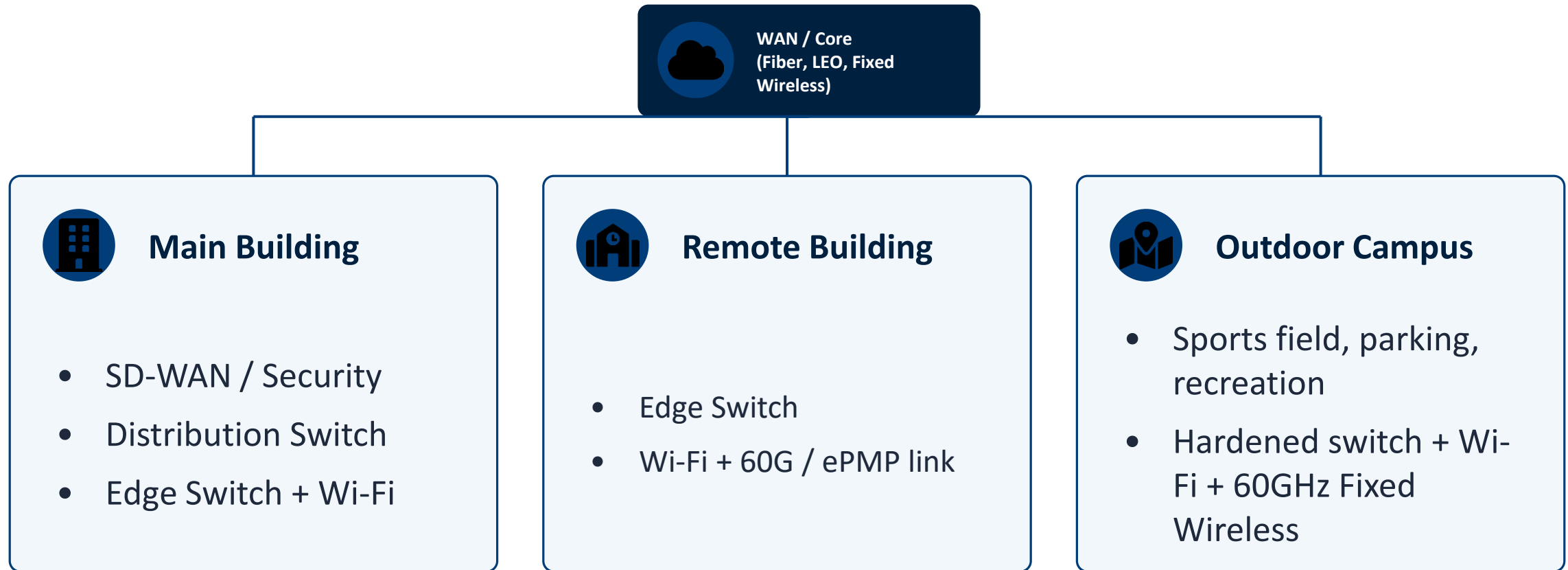


60GHz PTP/PMP

High-capacity building to building connectivity.

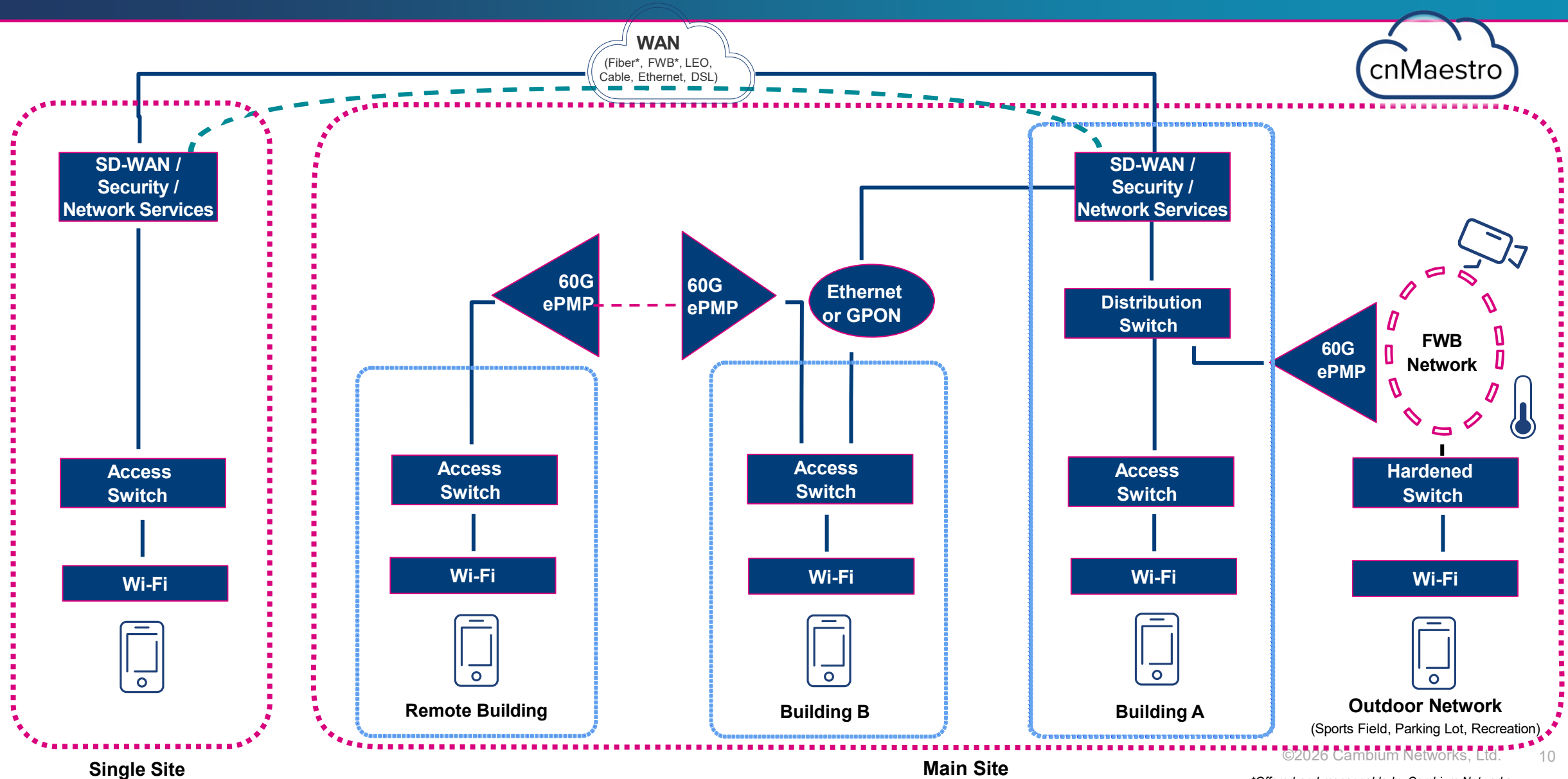
Campus-Wide Network Architecture

From the WAN edge to every classroom, library and outdoor space



WAN: Fiber, Fixed Wireless, LEO Satellite, Cable or DSL — same overlay regardless of underlying transport

Cambium's ONE Network for the Enterprise

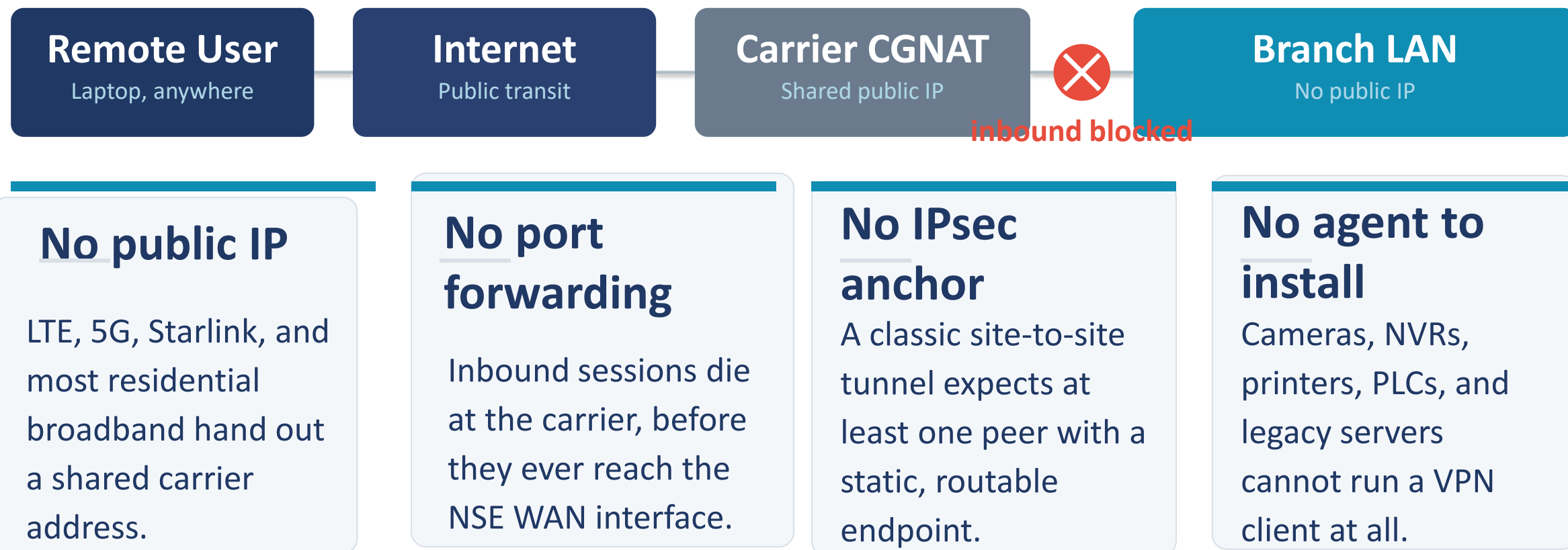


- **cnWave 60 GHz**
 - V5000 – Mesh
 - V5000 – Hub and Spoke (PMP)
 - V3000- PTP
 - V1000 – Client Nodes
- cnMaestro Managed.



The Reachability Gap

Most sites the customer needs to reach cannot be reached at all.



Four separate blockers, one root cause: the site is not addressable.

Solving the CGNAT Problem with IP Overlay and Tailscale

Most ISPs across the Pacific deploy Carrier-Grade NAT — making remote management and site-to-site VPNs difficult for multi-campus IT teams

NSE offers two ways to solve CGNAT — choose based on your customer's needs.

Public IP over CGNAT

Architecture:

Hub-and-spoke — provider hosts public IP pool

Best for:

- MSPs/ISPs selling static IP as a service
- Inbound access from the public internet
- CCTV/NVR that needs internet-routable IP
- IoT/SCADA requiring real public IP

Real static public IP at site

Reachable from anywhere on the internet

Tailscale Subnet Router

Architecture:

Peer-to-peer mesh — sites connect directly

Best for:

- Site-to-site VPN between CGNAT sites
- NSE connects outbound; Tailscale coordinates NAT traversal
- Remote admin access to LAN devices
- Quick deployment, no hub required
- Internal-only access (no public exposure)
- Free for up to 100 end points

No public IP assigned to site

Access via Tailscale network only

Both use WireGuard. Different use cases, same NSE appliance.

 JOIN US IN SAN FRANCISCO FOR TAILSCALEUP! [GRAB YOUR TICKET ->](#)

[BLOG](#) [DOCS](#) [DOWNLOAD](#) [CONTACT](#) [SALES](#)



[Platform +](#) [Solutions +](#) [Customers +](#) [Community +](#) [Partnerships +](#) [Pricing](#)

[Login](#)

[Get started - it's free!](#)

The best secure connectivity platform for the AI era

A Zero Trust identity-based connectivity platform that replaces your legacy VPN, SASE, and PAM and connects remote teams, multi-cloud environments, CI/CD pipelines, Edge & IoT devices, and AI workloads.

[Start connecting devices](#)

[Contact sales](#)



Business VPN

Secure internal access to apps and data, anywhere.



Privileged Access

Auditable access to SSH, K8s, databases, and more.



Securing AI

Bring AI usage into focus with Aperture.



Infra access

Direct access to infra. No bastions required.



Zero Trust networking

Enforce least privilege with identity-based access.

What the NSE Now Does

The appliance joins the customer tailnet and routes on behalf of the LAN behind it.

Advertises the LAN

SUBNET ROUTER

The NSE publishes its local subnets into the tailnet. Every device behind it becomes reachable without installing anything on that device.

Traverses any NAT

WIREGUARD

Peers negotiate a direct encrypted path through carrier NAT automatically, and fall back to a relay only when no direct path exists.

Enforces identity

ACLs AND IDP

Authorization comes from the user and device identity in the customer identity provider, not from an IP address or a network location.

One appliance turns an unreachable site into an addressable one.

What the Customer Pays Tailscale

Seat-based. The NSE is not a seat, and the free tier is not a plan.

List price, tailscale.com/pricing, verified July 2026

Personal	Standard	Premium	Enterprise
\$0 free forever	\$8 per user / month	\$18 per user / month	Custom contact sales
▪ Up to 6 users ▪ 3 ACL groups ▪ Individuals, non-commercial	▪ Unlimited users, 10 ACL groups ▪ SCIM and MDM configuration ▪ Posture via MDM, EDR, XDR	▪ 300 ACL groups ▪ Just-in-time access ▪ Flow logs, streaming, priority support	▪ Custom quantities and limits ▪ Custom MSA and SLAs ▪ Multiple tailnets, an OEM option

The NSE is a tagged resource, not a seat

- 50 tagged resources included on every plan, then \$1 per month each.
- Subnet routers, exit nodes, ACLs, and SSO are on every tier.
- A 100-site rollout adds \$50 a month, not 100 seats.

What “non-commercial” actually means

- Signup domain decides it. Gmail, Apple, or personal GitHub lands on free Personal.
- A custom domain is treated as business use and starts a paid trial.
- It will run at a business. Support, SCIM, MDM, and contract position are what break.

Quote Standard for a customer site. Schools and non-profits pay half of list.

Performance: WireGuard is generally faster and more efficient than IPsec, making it a better choice for users who prioritize speed and responsiveness.

Ease of Use: WireGuard is designed for simplicity and ease of use, making it easier for users without technical expertise to set up and manage their VPN connections.

Security: Both protocols offer strong encryption and authentication mechanisms, but WireGuard's modern cryptography and streamlined design may provide better security for some users.

Complexity: IPsec is more complex to configure and manage, especially for users unfamiliar with networking concepts. WireGuard's simpler design may be more suitable for those with less technical knowledge.

For a lightweight and efficient, low latency VPN solution, WireGuard is the preferred the better choice.

Note: There are still use cases for IPsec VPNs using IKE v2.

Where This Fits Across Education & Enterprise



Rural & Outer-Island Campuses

Extend reliable connectivity to satellite campuses and teaching sites where fiber is unavailable or uneconomical



Libraries, Labs & Dormitories

High-density Wi-Fi for student-heavy spaces, with content filtering and safe search for education environments



Distributed Enterprise Branches

Multi-site organisations across varied ISPs that need consistent security and remote management



Outdoor & Event Spaces

Sports fields, graduation ceremonies, conferences and temporary deployments needing rapid Wi-Fi or backhaul



Disaster & Continuity Planning

Rapidly deployable connectivity for campuses and offices recovering from outages or natural events

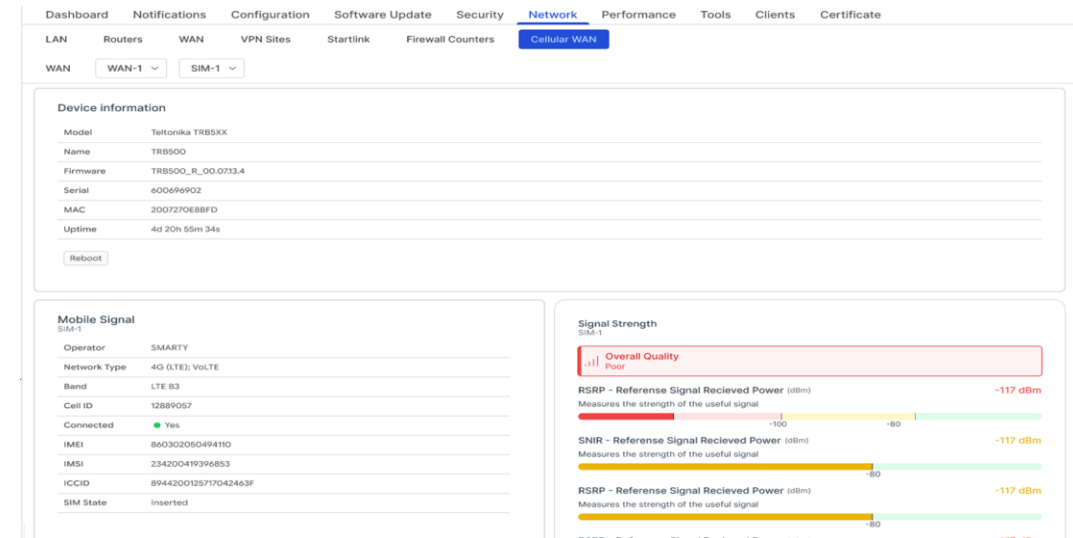


Managed IT for Multi-Site Institutions

Centralised monitoring and troubleshooting for lean IT teams managing many locations from cnMaestro

Cellular Resilience via NSE + Teltonika Integration

- Pair NSE NGFW with Teltonika industrial 4G/5G routers for secure, always-on campus and branch connectivity
- Automatic cellular failover keeps classrooms, libraries and offices online during fiber or LEO outages
- Single cnMaestro pane of glass manages NSE security and Teltonika cellular health together



NSE + Teltonika: Better Together

Each product fills the other's gap — together they deliver a complete edge solution for campuses and distributed sites



NSE NGFW Has

- Next-Gen Firewall & Snort IPS
- SD-WAN / Multi-WAN
- Adaptive QoS
- cnMaestro management

Lacks: 3G / 4G / 5G cellular connectivity



Industrial 4G/5G Routers Add

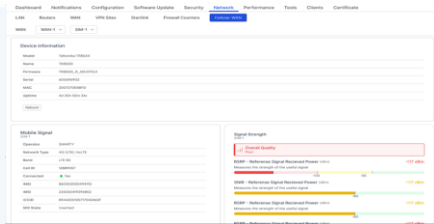
- 4G LTE & 5G Sub-6 / mmWave connectivity
- Dual-SIM automatic failover
- Industrial, rugged design
- Global carrier support

Lacks: NGFW / IPS / SD-WAN

Together: a complete, secure edge solution — wired and wireless backhaul, automatic failover, and unified management

Unified Visibility & Where It Fits

Teltonika router health now lives alongside NSE security inside cnMaestro



Integrated Router Monitoring

- Live signal strength, latency and firmware status inside cnMaestro
- Alerts and health checks alongside NSE firewall and SD-WAN data
- Beta available with cnMaestro 6.1 — no separate vendor portal needed



Where It Fits on Campus

- Primary link for temporary or mobile teaching units and pop-up classrooms
- Automatic failover for libraries, admin offices and labs during outages
- Backup WAN for branch campuses where fiber or LEO service is interrupted

Bundled deployment: bigger-scope projects, simpler procurement, one partner for connectivity and security

Why It Matters for Institutions & Enterprises

- ✓ **Lower CapEx**
LEO terminal + NSE replaces expensive microwave or leased circuits
- ✓ **Lower OpEx**
Unified management through cnMaestro reduces ongoing operational costs
- ✓ **Faster Time to Service**
Rapid deployment — new sites can be online in days, not months
- ✓ **Reduced Connectivity Cost**
Eliminate costly leased lines for remote and rural campus locations
- ✓ **Zero-Touch Deployment**
Standardised architecture enables plug-and-play rollouts to new sites
- ✓ **Centralised Management**
cnMaestro provides a single pane of glass across WAN, LAN and Wi-Fi
- ✓ **Faster Troubleshooting**
Unified platform with end-to-end visibility reduces resolution time
- ✓ **Fewer Site Visits**
Remote management and monitoring minimise on-site truck rolls

Long-Range Outdoor Wi-Fi 6 for Open Campus Spaces

XV2-2T

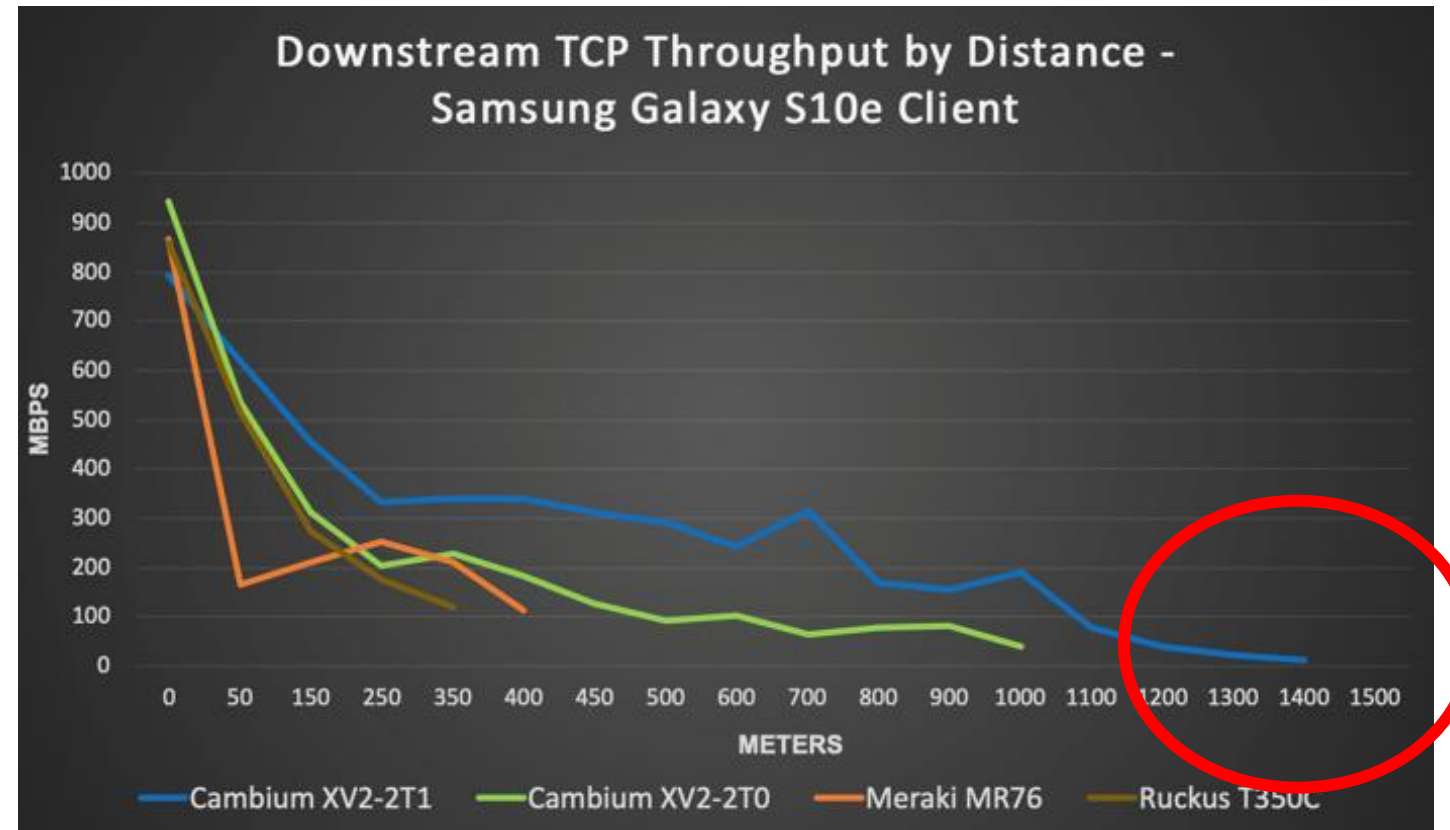


Highlights

- Innovative high gain antennas
- Superior range and consistency
- Better reach to connect weaker clients
- Integrated omni (XV2-2T0) or 120 deg (XV2-2T1) antennas
- Application Control for 5000+ apps
- Integration with Microsoft Azure & Google G-suite directories

Superior Coverage

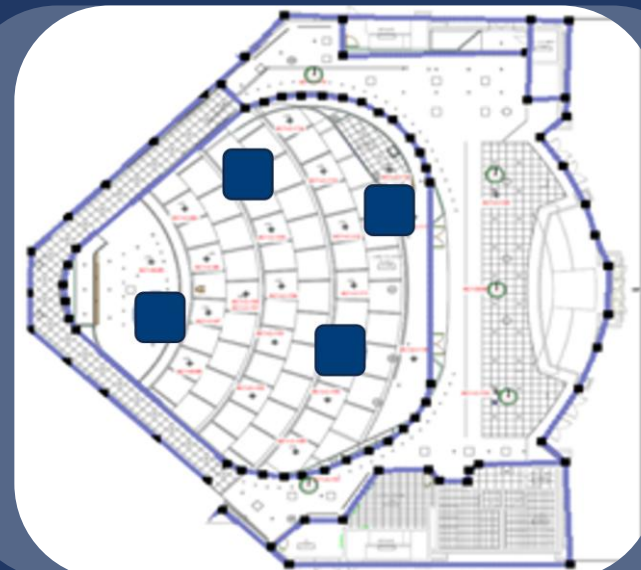
- 2-3X greater range vs. competitors
- Reduced AP count significantly lowers TCO



Large Public Venue Access Points



- The XE5-8 is a five-radio Wi-Fi 6/6E 8×8/4×4 access point (AP) designed to deliver high-density,
- Highest density Wi-Fi 6 solution in the industry.
- Wi-Fi 6E support extends the capacity of Wi-Fi into the 6 GHz band



Cambium Design:

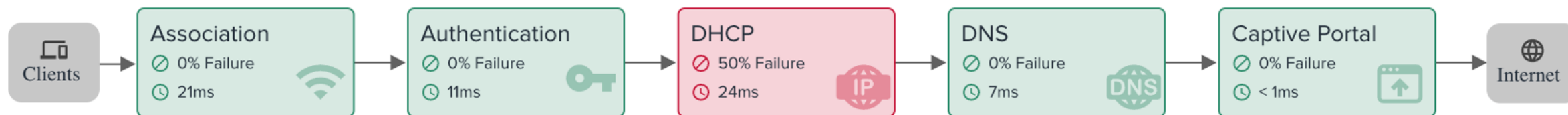
- 4 high-density 5-radio APs
- 4 cables
- 4 switch ports
- No controller appliance

AI Operations - Real Time Visibility and Troubleshooting

- **cnMaestroX** delivers comprehensive, real-time visibility into client health, roaming events, and connection history, complete with Root Cause Analysis.

Wi-Fi Client Analytics X

Period: Last 24 Hours, Resolution: 1 Hour



- ➔ Identify campuses, branch sites or outdoor spaces with connectivity or security gaps
- ➔ Pilot a campus backhaul or Wi-Fi Hotspot deployment with NSE + Cambium ONE Network
- ➔ Engage IT teams on secure remote access and multi-site management via cnMaestro
- ➔ Contact the Cambium Networks and Kastel teams for technical deep-dives and demo support

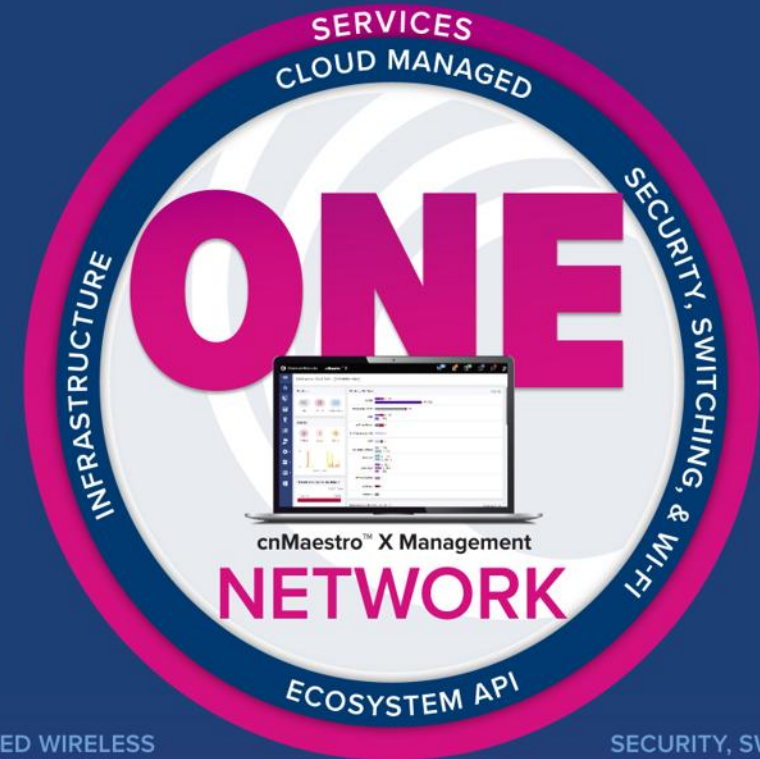
THANK YOU

Resilient Connectivity & Security for Education & Enterprise

Roy Wittert

Cambium Networks

FNU NCIT Conference, Fiji • 2026



FIBER & FIXED WIRELESS
INFRASTRUCTURE



Point-to-Multipoint, Point-to-Point,
Fiber Infrastructure

SERVICES

Network Planning
Network Design
Quality of Experience
24x7 Support

SECURITY, SWITCHING
& WI-FI



Indoor & Outdoor Wi-Fi, Home Router,
Switches, Security & SD-WAN