IGNITION
DESIGN LABS

TECHNICAL WHITE PAPER

SD-Edge
vCPE and uCPE

A fully virtualized, software-defined carrier edge — running in the cloud, in edge data centres, and in regional centres.

Broadband stopped being a growth business

The triple-play era is over. What replaces it has to be built, not bundled.

The broadband network gateway (BNG) sits at the heart of fixed broadband infrastructure. It starts and supervises subscriber sessions, authenticates users, assigns addresses, manages quality of service and enforces policy. For most operators it is still a piece of hardware, and it is still where the network's flexibility goes to die.

Meanwhile the market moved. There was a time when triple-play packages were compelling to consumers and lifted ARPU for the provider. That time has passed. Households now buy broadband access, and nothing else.

> **The squeeze is structural.** Providers must deliver a flexible, high-performance, affordable service to households whose expectations keep rising — while margins narrow and the pressure to cut both operating and capital expense intensifies. Hardware-based session management makes every one of those goals harder.

What SD-Edge is

SD-Edge is IDL's fully virtualized, software-defined carrier edge. Its vBNG/vCPE was designed from the start as a cloud-native broadband network gateway — not a hardware BNG with a hypervisor bolted underneath.

Separating the control and data planes, and simplifying packet processing, is what buys the operator dynamic scaling, flexibility, optimized performance and lower cost. An open architecture then allows service chaining on top of native BNG functions: DPI, security gateway, TDF, CGNAT, WAG, BNG and ACF converge onto a single virtualized platform.

The commercial point is simple. It lets a provider stop selling a dumb pipe.

vCPE — the remote edge

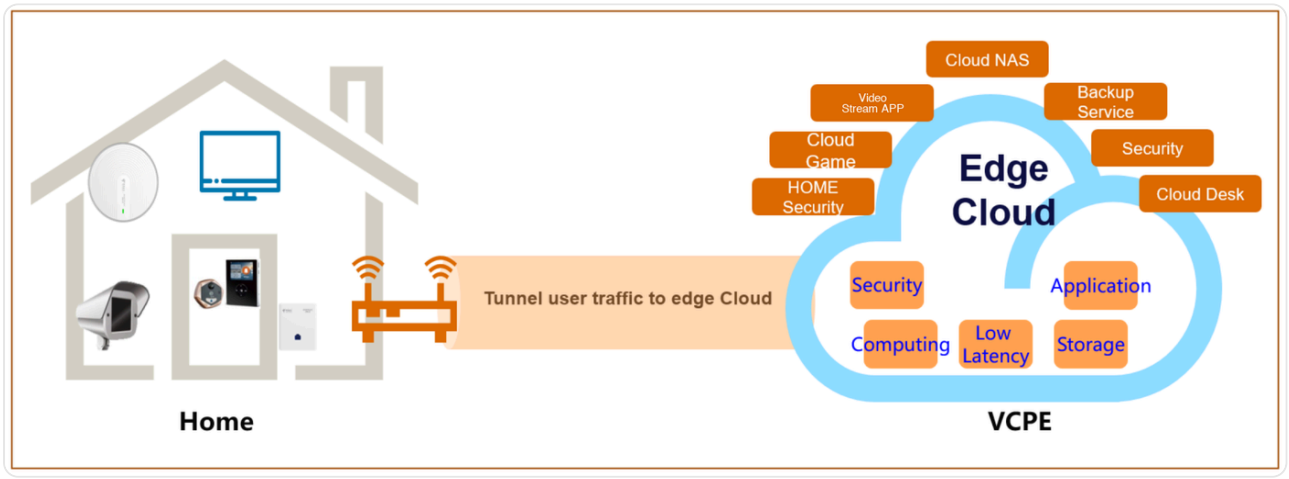
Move the home gateway into the cloud. Leave the fibre exactly where it is.

In the traditional model, an ONT is installed at the subscriber's premises and configured as a bridge or a router, and the household builds its own network behind it. The operator cannot see how many devices are in that home, or what they are. When something breaks, nobody can say why — and a single fault can degrade the whole PON branch.

Edge-cloud networking extends the home LAN into the cloud. Compute, storage, security and the gateway function itself move to the provider's edge. The ONT at the subscriber's premises only needs to be a bridge. Existing equipment is reused rather than replaced.

How it works

- The OLT transparently passes the subscriber's Layer 2 traffic. SRv6 carries it to the cloud gateway.
- The cloud gateway identifies each household by its QinQ tag and assigns it an instance.
- When traffic is internet-bound, the gateway initiates PPPoE/IPoE dialing through an SRv6 tunnel to the vBRAS to obtain the subscriber's WAN address.
- Virtual gateways are allocated on demand and reclaimed when a household is idle — **256 vGWs pooled per vCPE instance** — so capacity is not wasted on homes that are asleep.



vCPE — home traffic tunneled to the edge cloud, where the gateway now lives

What the operator gets back

Six things, and they are not abstractions.

One line, many services

A single FTTH connection carries both internet access and internal VPN access.

Zero network rebuild

Existing FTTH access is reused. Only the metro service structure is adjusted.

Short activation cycle

Services activate through a self-service app instead of a two-to-three-day service-centre process.

Flexible expansion

Interconnection is a service activation, not a construction project.

Low operational complexity

Central cloud management gives clear visibility of bandwidth use and network health, reducing field staff.

Full autonomy

All POPs sit inside the operator's own cloud, so requirements iterate quickly and control stays in-house.

Quality, cost, revenue

The three ledgers this actually moves.

Quality

Cloudifying the subscriber-side gateway and connecting homes over a large Layer 2 network shortens the path and cuts access latency. Firewall, virus scanning and intrusion detection deliver carrier-grade protection to households that had little or none. Business-continuity mechanisms in the cloud are more robust than a home gateway with no failover — no technician dispatched, no trip to the service centre.

Cost

Existing hardware is used optimally, so there is no additional hardware spend. Faults are identified and resolved online rather than on site. Cloud storage replaces the NAS a subscriber would otherwise buy — and the operator can sell it back to them as a carrier-grade service.

Revenue

New services layer onto existing subscriptions for an additional monthly fee. Edge-cloud services attract subscribers away from competing networks. Usage analysis enables precise, differentiated marketing — offering a higher-bandwidth plan to the household that has been saturating its link for months. Binding services, content and habits to the network increases stickiness, and stickiness is what protects ARPU.

uCPE — the near edge

Some customers need the box on their own premises. The software doesn't have to change.

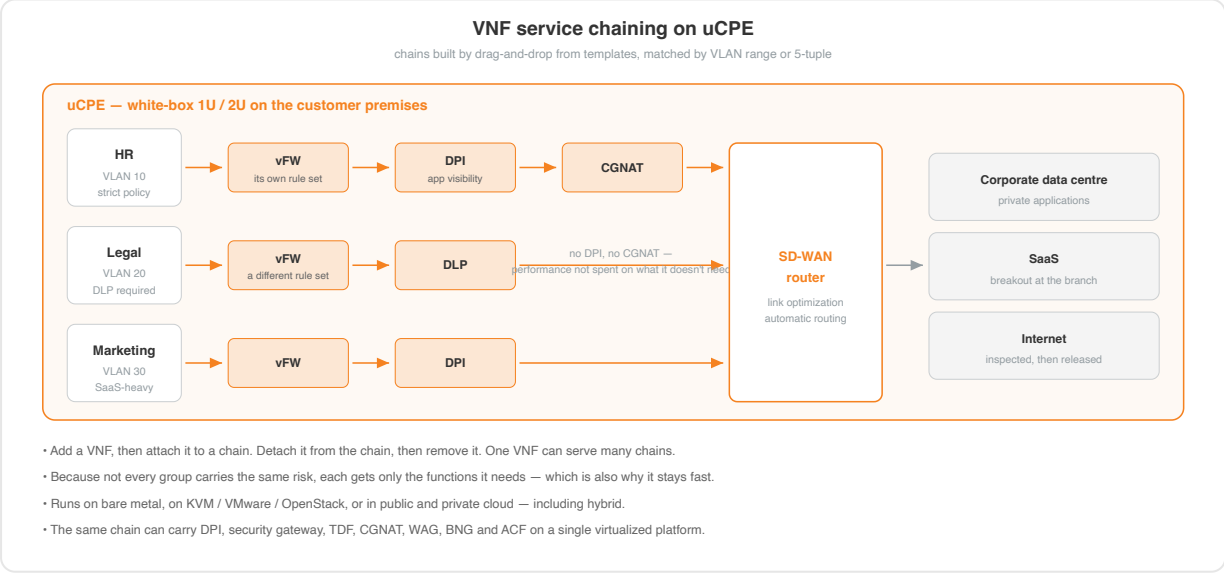
vCPE solves NFV and edge-cloud deployment for home subscribers and small businesses. For traditional enterprise customers, however, placing network infrastructure at the service provider's end may not be acceptable. The CPE stays on the customer's premises, typically as a gateway.

Using the same SD-Edge technology, those software functions are modularized and virtualized, and deployed as a **universal CPE (uCPE)** on white-box hardware — a 1U server at the access edge, a 2U server at the central office. Hybrid deployments are supported, so this is not a fork in the road.

Service chaining, by department

VNF service chains are orchestrated through a template-based, drag-and-drop workflow, matched by VLAN range or by 5-tuple. Add a VNF, then attach it to a chain; detach it from the chain, then remove it. A single VNF can be referenced by many chains.

> **Why segment at all?** Not every group carries the same security requirement. HR, legal and marketing can each run their own vFW and their own function set — which is also why the platform stays fast: no group pays the performance cost of a policy it does not need.



VNF service chaining on uCPE — each department gets only the functions it needs

Wi-Fi, security, and where they meet

Access points should do radio. Security belongs at the gateway.

The Wireless Access Gateway

Most access points use chip acceleration for data-plane processing. Turning on security features can collapse their forwarding performance. So the AP handles wireless access, and centralized security control happens at the edge gateway.

A Wi-Fi Access Gateway (WAG) lets enterprises meet the demands of a modern Wi-Fi network — user management, security, mobility, quality of experience — in a simple, uniform, consistent way. It also allows cost-effective or multi-vendor Wi-Fi networks to be used without compromising on capability.

WAG deployments share one theme: **large numbers of guest users**. Public and community Wi-Fi, mobile offload, smart cities, venue Wi-Fi, hotel Wi-Fi, multi-dwelling units. Enterprise Wi-Fi solutions serve employees well; they are not built for a transient population an order of magnitude larger.

- Multi-vendor Wi-Fi aggregation via GRE, EtherIP, CAPWAP or VLAN; AAA proxy and load balancing
- Policy enforcement per AP, per VLAN or per user; access control and advanced QoS
- Carrier-grade NAT and stateful firewall; high-scale DHCP; full IPv6 and dual-stack combinations
- Content filtering and malware/phishing protection; service function chaining; lawful intercept

Cloud security as a service

Most households have no security equipment and no security policy. Attacks, viruses, malicious links and phishing sites reach them unopposed, and a subscriber without security awareness can lose real money.

Once the network is cloud-integrated, the household inherits carrier-grade protection: internet traffic protection (malicious URL and fraudulent site identification, virus detection), internet behaviour management (filtering sites and applications, controlling access time, protecting children), and internal network scanning (endpoint vulnerabilities, weak passwords, open ports).

Deploy it the way your network is built

Three runtimes, because not every operator is at the same place.

Bare metal

Software runs on servers with no virtualization. The right answer for fixed operators not yet ready for a cloud-native stack.

Virtual machine

Deployed on KVM, VMware or OpenStack environments.

Public or private cloud

Runs in the cloud environment the operator already operates.

Hybrid

SD-Edge blends into existing network architecture, so virtualization is a choice rather than a migration.

The ecosystem

SD-Edge's ecosystem centres on integrating applications with the edge cloud: cloud security, cloud NAS, cloud desktop and cloud gaming. Edge-side container technology allows AI workloads to be deployed onto converged gateways independently, in an app-store model, with cloud-trained models cooperating with a local AI engine.

> **The commercial summary.** vBNG/vCPE separates control and data planes so it can be deployed centrally or at the distributed edge. Its open architecture lets providers converge TDF/DPI, CGNAT, security gateway and BNG onto one virtualized platform, at ultra-low latency. With SD-Edge, a provider moves beyond selling dumb-pipe broadband and starts delivering value-added services quickly — reducing churn and raising ARPU.

In production

Deployed with Tier-1 fixed and mobile operators in East Asia.

About Ignition Design Labs

Ignition Design Labs (IDL) is a market leader in next-generation carrier-grade convergent Wi-Fi and 4G/5G wireless access technologies.

IDL has distinguished itself in the telecommunications sector most notably through its partnership with a Tier-1 operator in East Asia serving over 100 million subscribers — a collaboration that produced one of the world's largest integrated Wi-Fi and cellular systems, with over 400,000 access points across the capital area.

Beyond convergence, IDL addresses the user-experience problems of large-area Wi-Fi coverage: scalability, cognitive radio management, and integration with 4G/5G. It applies AI to network management and IoT security so that customers gain a better experience while spending less on maintenance.

IDL is headquartered in Silicon Valley, with R&D in Taiwan.

Related solutions

- **SD-WiFi** — carrier Wi-Fi offload inside the 3GPP core
- **SD-Access** — a zero-trust campus fabric without replacing your switches
- **SD-Branch** — networking, security and SD-WAN converged into one gateway
- **MDU** — one SSID for the whole property, a private network for every unit
- **AIOps** — from reactive monitoring to a network that explains itself
- **Security** — secure gateway and DPI engine

> Learn more at **ignitiondl.com/solutions**