



TECHNICAL WHITE PAPER

SD-Branch

One Gateway per Site

Routing, switching, security, SD-WAN and Wi-Fi management, converged into a single software-defined platform.

The SMB is asked to digitize on an enterprise budget

Nobody at a twelve-site retail chain is a certified network engineer.

Digitalization is no longer optional; connectivity and data have become basic production tools. But small and medium businesses face the same infrastructure demands as large enterprises with none of the resources:

- **Cost and complexity.** Traditional networking is expensive and intricate, requiring specialized staff to design, deploy and maintain it.
- **Security.** Protecting information processing is a genuine concern, and the tooling assumes a security team.
- **Scalability.** Traditional solutions do not flex with a business that is growing — or contracting.

SD-Branch answers this by combining routing, switching, security and Wi-Fi management into one unified, software-defined platform. The integration is the product: it is what removes the complexity, not just the hardware.

The design constraint that shaped everything. If a device has to be configured by an engineer on site, the model does not work at thirty branches. Everything below follows from taking that seriously.

The intelligent security gateway

The cornerstone. Everything else attaches to it.

The gateway is the core device in an SD-Branch deployment, and the sole interface between the branch and the cloud orchestrator. It carries three jobs at once:

SD-WAN

Link optimization and automatic routing across the branch's available WAN paths.

Security

Firewall and DPI, protecting the branch and enforcing compliance — the same gateway IDL sells as a next-generation firewall.

Local management

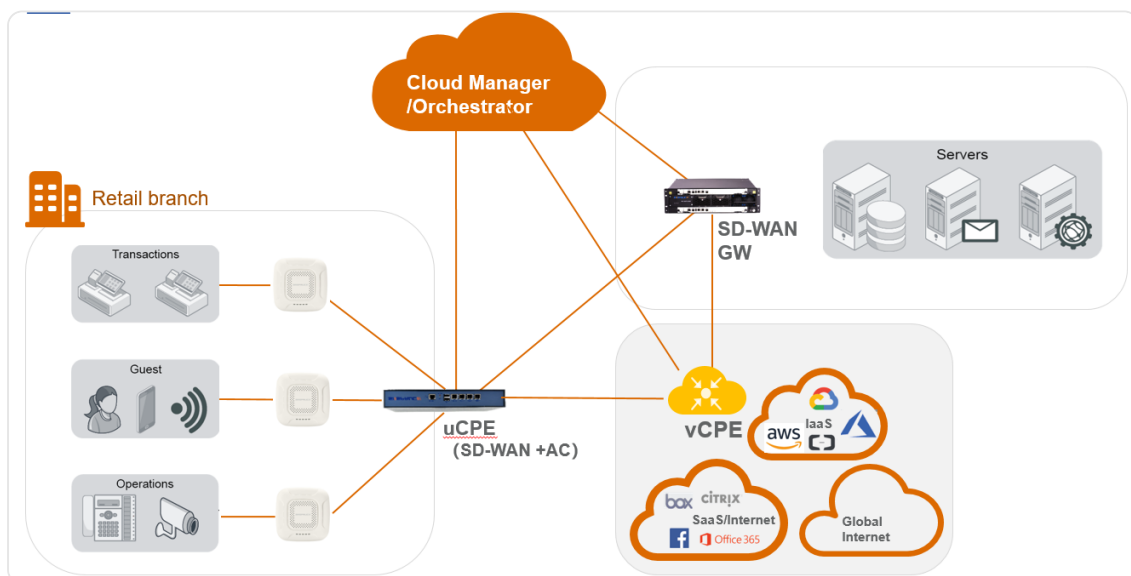
Manages the branch's own wireless devices, IoT devices and switches.

Cloud control

The only interface to the orchestrator, supporting cloud-edge collaborative scheduling.

Zero-touch provisioning

ZTP is the feature that makes multi-branch deployment economic. Devices are shipped directly to the site and come up configured, without on-site IT intervention. That lowers operating cost, and it collapses the time required to bring a new site online from days to the length of a courier delivery.



SD-Branch — branch gateway, SD-WAN, and cloud orchestration

Cloud-edge collaboration

Compute at the edge, scheduled from the cloud.

Cloud-edge collaborative scheduling places computing nodes at the edge and connects them to cloud servers, achieving dynamic resource allocation and distributed computing. Cloud and edge work together: data is processed and analysed efficiently, latency falls, computing cost falls, and internal network devices remain flexibly accessible and manageable.

An app store for the branch network

Using Docker or virtual machine technology, AI applications deploy independently onto the converged gateway. This enables a flexible, scalable app-store model — applications are added and removed dynamically rather than provisioned as projects.

- **AIoT data aggregation** — collects and consolidates data from IoT devices into a unified view.
- **QoE probes** — monitor network performance and quality of experience, detecting issues proactively rather than waiting for a complaint.
- **Line-of-business applications** — deployed at the edge, integrating with existing infrastructure.

Through cloud-edge fusion and edge computing with containers, an ecosystem forms around the network: OS, application, terminal and service together — which is what allows industry-specific applications to be built on top of it.

AI-driven operations

The SMB has the least tolerance for troubleshooting, and the least capacity for it.

The cloud management platform applies AI and big data to improve operational efficiency, optimize user experience, and perform precise root-cause analysis of network issues.

Wi-Fi assurance

- Monitors and guarantees service levels for users
- Automated event correlation for troubleshooting
- Dynamic packet capture for detailed diagnosis
- Dynamic policy configuration and guest network management

Quality of experience

End-to-end measurement locates user experience problems using data from access points, switches and gateways. Automated SLA measurement diagnoses and optimizes network performance with AI-driven adjustment — so the network is predictable and measurable rather than merely monitored.

Why this matters more here than in the enterprise. A large enterprise can absorb a slow diagnosis with staff. A twelve-site business cannot. Automation is not a luxury feature at this scale — it is the only way the economics work at all.

Asset tracking

High-value resources are located across the network — equipment, devices, and the things a business cannot afford to lose track of.

Where the market is going

Security is absorbing networking. Plan for it.

Network design has relied on broadly the same protocols for five decades. What is changing is that security is no longer a layer on top of the network — it is becoming the network. As remote work and zero-trust access become standard, demand for secure networking grows faster than for connectivity alone.

The cost and complexity of running multiple separate devices for IoT and network security is significant. Integrated platforms that consolidate these functions are consequently displacing point products.

Where SD-WAN is heading

- **Smarter optimization** — AI and machine learning applied to path selection and user experience
- **Security integration** — threat detection, firewall, encryption and access control built in
- **Multi-cloud and hybrid cloud** — connectivity and security across diverse cloud environments
- **IoT support** — managing and optimizing large numbers of device connections
- **Edge computing** — more processing at the network edge, reducing latency and congestion

SASE

Secure Access Service Edge combines network security and access policy into comprehensive protection, on a cloud-native architecture, with unified identity and single sign-on across applications. SD-WAN and SASE are converging, and IDL builds toward that convergence rather than around it.

IDL's position

IDL invests in AI, machine learning and edge computing, and consolidates functionality into a unified platform rather than shipping a portfolio of boxes that customers must integrate themselves. The goal is scalable, secure, efficient networking that a business without a network team can actually run.

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-Edge** — vCPE and uCPE: a fully virtualized, software-defined carrier edge
- **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