IGNITION
DESIGN LABS

TECHNICAL WHITE PAPER

SD-Access
The Zero-Trust Campus

Policy-driven segmentation and zero trust for the campus —
without replacing the switches you already own.

Segmentation shouldn't cost you a forklift

The technology is agreed. The bill is the problem.

Modern campuses need networks that adapt to the business while staying secure and simple to manage. The industry consensus is clear enough: policy-driven automation, micro-segmentation, zero trust. Nobody argues with the destination.

The obstacle is how you get there. Competing campus fabrics generally require a complete set of equipment from a single vendor — which means switches and other devices must be replaced or upgraded before the first policy can be written. For a campus with tens of thousands of ports already installed and working, that is not a network project. It is a capital project.

> **IDL takes a different route.** We use tunnel overlay technology. Only user traffic needs to be directed to policy enforcement nodes — the campus keeps its existing switches. Typical tunnels are VxLAN, SRv6 or QinQ, building a large Layer 2 network on top of what is already there.

What the overlay buys you

Once traffic reaches the enforcement nodes, the large Layer 2 network makes it possible to identify customer assets accurately — especially IoT devices — to allocate addresses uniformly, and to support seamless mobility. That is what true internal network security and zero trust actually require.

IDL has applied for three patents in this area.

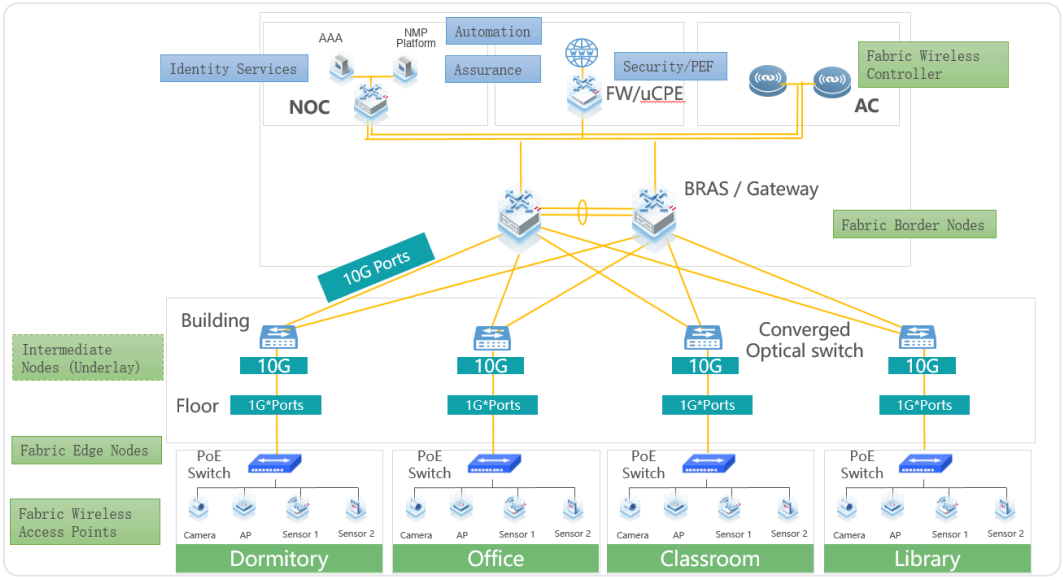
Identity, not ports

Dynamic segmentation, under the hood.

Rather than configuring VLAN segmentation at the access switch, departments or individuals are assigned to VLANs based on their role or identity. This associates the VLAN concept entirely with the user — so policies remain unchanged when someone moves desks or changes offices.

Users within a VLAN are isolated using VRFs on the enforcement node, logically separating them from other services. Traffic inside a VLAN is governed by security policy; traffic between VLANs is routed.

Edge nodes encapsulate packets to the enforcement nodes using QinQ, VxLAN or SRv6, creating the Layer 2 overlay that gives the campus its flexibility, scale and segmentation.



SD-Access campus fabric — automation, assurance, identity services and policy enforcement

PON/POL — the differentiator

Remove a whole layer of the network, and its cost with it.

IDL's SD-Access can extend to integrate with PON (Passive Optical Network) or POL (Passive Optical LAN). This is where the architecture departs most sharply from the alternatives.

What changes

- **Fabric edge nodes disappear.** Adopting the POL approach removes the need for them entirely, leaving a streamlined architecture with fewer components to buy, power and maintain.
- **One hop to the BRAS.** The optical path connects directly, simplifying the network and cutting latency.
- **Capital cost falls.** Fewer active devices and a simpler architecture mean a materially lower investment, which matters most precisely where deployments are largest.
- **Power draw falls.** Passive optical infrastructure consumes less than an equivalent Ethernet build.

Optical splitters distribute signal from a single fibre to many endpoints. Direct fibre connections run from the central office or BRAS to endpoint devices, bypassing intermediate nodes. Management remains centralized, so policy enforcement and assurance are unchanged.

The pieces

Five roles, one platform.

Network automation

An intent-based automation platform: administrators declare the outcome they want and the system configures the network to achieve it, reducing manual configuration and the errors that come with it. A straightforward GUI keeps complex networks manageable without deep expertise; open APIs let the platform integrate with the rest of the IT estate.

Network assurance

Data collectors analyse endpoint-to-application flows and monitor fabric device health, giving a holistic view of performance. AI-driven AIOps enables predictive analytics — foreseeing problems before they reach users — which is what actually reduces support effort and operating expense.

Identity services

Network access control maps endpoints to groups automatically based on device identity, so a new device is recognized and given the right policy immediately. Granular enforcement means only authorized devices reach sensitive resources. Asset visibility is not a reporting feature here; it is the precondition for securing a campus full of devices nobody remembers installing.

Policy enforcement

Enforcement nodes take policy from the management platform or from a security centre, and can also hold locally defined static policies. They support firewall, VPN and DPI, report telemetry back for coordinated enforcement, and handle campus-specific duties — PPPoE dialing, and preventing unauthorized devices from connecting.

Wireless

The fabric wireless controller brings access points and wireless endpoints into the fabric, and can itself be integrated with uCPE through NFV — so the wireless edge inherits the same virtualization flexibility as the wired.

What a campus deployment looks like

Dormitories, offices, classrooms, libraries — one fabric.

Access points are managed centrally through the controller. Users are authenticated and managed by the platform. Both APs and controllers stream telemetry, which the platform uses to optimize the network and improve quality of experience. Configuration and visibility are centralized.

The campus data centre carries the supporting systems: AAA for authentication, authorization and accounting; a work-order system for handling faults and maintenance; and a large-screen display system giving operations staff a live view of network status.

> **Zero trust, in practice.** Dynamic segmentation partitions the network by user role, device type and other criteria. Every user and device is continuously authenticated and authorized before reaching resources — not once at the door, but continuously.

In production

- A university town network covering teaching areas, dormitories, living areas, libraries and outdoor public spaces — with over **20,000 access points** deployed, serving hundreds of thousands of students and staff, with seamless roaming throughout.
- A national campus deployment in Central Asia.

Why it wins

- **Keep your switches.** The overlay does not care who made them.
- **PON/POL integration** removes an entire layer of hardware and cost.
- **Policy follows identity**, so moves and changes stop generating tickets.
- **AI-driven assurance** turns operations from reactive into predictive.

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**