IMMUNITY NETWORKS · eBOOK

Enterprise Network Best Practices

A practical handbook on switching, segmentation, power and security for modern enterprise networks.

A Make-in-India OEM guide

immunitynetworks.com · +91 91367 90819

Contents

Compiled from the Immunity Networks knowledge base. For tailored design help, contact our engineers.

1. L2 vs L3 switching

“Do we need L2 or L3 switches?” is one of the most common questions in network design. The answer shapes cost, performance and how your network scales. Here it is in plain English.

What a Layer 2 switch does

A Layer 2 switch forwards traffic using MAC addresses within a single network segment. It’s the workhorse of the access layer — the switches your access points, PCs, cameras and phones plug into. Managed L2 switches add VLANs (to separate traffic), QoS (to prioritise it), and PoE (to power devices). For most floors and wiring closets, L2 access switching is exactly what you want. Immunity’s NetForce L2 range covers this layer.

What a Layer 3 switch adds

A Layer 3 switch does everything an L2 switch does, plus routing — moving traffic between networks (VLANs/subnets) using IP addresses, in hardware, at wire speed. This is what you put at the core or aggregation layer to connect all your VLANs and buildings together quickly. Immunity’s NetForce L3 range serves this layer, with models scaling to high switching capacities and 10G uplinks.

The key difference: inter-VLAN routing

If you split your network into VLANs — staff, guests, CCTV, IoT, servers — something has to route between them. A router can do it, but a Layer 3 switch does it far faster because it routes in hardware. In a campus with many VLANs and heavy east-west traffic, an L3 core is the difference between a snappy network and a bottlenecked one.

A simple design rule

Most enterprise networks use a layered design: L2 switches at the access layer (where devices connect), feeding into L3 switches at the aggregation/core layer (where everything is routed together and out to the gateway). Small single-VLAN sites may need only L2. Multi-VLAN campuses, hospitals, hotels and factories almost always want an L3 core.

What about PoE and uplinks?

Access switches usually need PoE or PoE+ to power access points, cameras and phones. Core and aggregation switches need fast fibre uplinks — typically 10G SFP+ using optical transceivers — to carry aggregated traffic between buildings without congestion.

How Immunity fits

Immunity builds both layers as one Make-in-India family, managed together from Net Cloud — so VLANs, routing, PoE and telemetry are configured and monitored from a single console. See the full switching & routing solution.

2. VLANs and segmentation

A VLAN (Virtual Local Area Network) lets you split one physical network into several separate logical networks. It's one of the most useful tools in networking — for security, performance and order. Here's a practical guide without the jargon.

What a VLAN actually is

Imagine one switch serving an office. Without VLANs, every device — staff laptops, guest phones, CCTV cameras, printers — sits on the same network and can potentially see each other. With VLANs, you carve that one switch into separate virtual networks: a staff VLAN, a guest VLAN, a CCTV VLAN, and so on. Devices in one VLAN can't reach another unless you explicitly allow it through a router or Layer 3 switch.

Why VLANs matter: security

Segmentation is a core security principle. If guests, IoT devices or cameras are isolated on their own VLANs, a compromised device can't roam your whole network. Guest Wi-Fi should never reach payment, clinical or operational systems — VLANs are how you enforce that. This is the same model used to keep passenger Wi-Fi separate from airport operations.

Why VLANs matter: performance and order

VLANs also contain broadcast traffic, so a chatty device or a broadcast storm in one VLAN doesn't drag down the rest. And they bring order: clear boundaries make a network easier to manage, troubleshoot and apply policy to.

A typical VLAN plan

A practical business VLAN scheme often looks like: Management (for the network gear itself), Staff/Corporate, Guest/Public Wi-Fi, Voice (phones), CCTV/Security, IoT/Building systems, and Servers. Each gets its own subnet and policy. How many you need depends on your size and risk — but even a small office benefits from at least separating staff, guests and cameras.

How VLANs talk to each other

By design, VLANs are isolated. When they do need to communicate — say, staff reaching a server — traffic is routed between them by a Layer 3 switch or gateway, where you apply access rules. This is called inter-VLAN routing, and doing it in hardware on an L3 switch keeps it fast.

Getting VLANs right with Immunity

Immunity's NetForce L2 and L3 switches support VLANs, tagging and inter-VLAN routing, and the Gateway Controller enforces policy between segments. Because the whole fabric is managed from Net Cloud, you can design, push and monitor VLAN policy across every site from one console. For the security angle, see our network security solution.

3. PoE, PoE+ and PoE++

Power over Ethernet (PoE) lets a single network cable carry both data and electrical power. It's what powers your access points, IP cameras, phones and door controllers without a separate electrician-installed socket at each device. Here's what the different PoE types mean and how to plan for them.

Why PoE matters

Without PoE, every ceiling access point or wall camera needs a nearby power outlet — expensive, ugly and inflexible. With PoE, you run one Ethernet cable from a PoE switch, and the device gets both connectivity and power. You can place devices exactly where coverage needs them, and back the whole network with a single UPS in the comms room.

The PoE standards, simply

PoE (802.3af) delivers up to about 15.4 W at the switch port (~12.95 W at the device). Fine for basic access points, VoIP phones and small cameras.

PoE+ (802.3at) delivers up to about 30 W per port (~25.5 W at the device). This is the practical default today — enough for Wi-Fi 6 access points, PTZ cameras and most devices.

PoE++ (802.3bt) comes in Type 3 (up to ~60 W) and Type 4 (up to ~90–100 W) for power-hungry devices like high-end APs with multiple radios, video phones, displays and some IoT gateways.

What is a "power budget"?

A PoE switch has a total power budget shared across its ports. A switch might support PoE+ on every port individually but not be able to deliver maximum power on all ports at once. When specifying a switch, add up the wattage of every powered device and confirm the switch's total budget comfortably exceeds it — with headroom for growth. This is a common and costly oversight.

Planning PoE for a real deployment

Count your powered devices and their class: access points (often PoE+), cameras (PoE or PoE+), phones (PoE), door controllers and IoT (varies). Sum the worst-case draw, add ~20–30% headroom, and choose access switches whose budget covers it. For a campus, distribute powered devices across multiple switches rather than overloading one. Immunity's NetForce switches offer PoE/PoE+ across the access range, with budgets sized for dense access-point and camera deployments — see PoE adapters & mounts for standalone injectors and mounting.

PoE and your wireless rollout

Because access points are almost always PoE-powered, your switching and wireless plans are linked. Size the PoE budget alongside your Wi-Fi 6 design so every planned access point has guaranteed power. Managing both from Net Cloud means you can see per-port power draw and spot problems early.

4. Secure guest networks

Guest Wi-Fi is a guest's first and most constant impression of a hotel or hospital — and one of the easiest things to get wrong. Done badly it is slow, ugly and a security hole into clinical or operational systems. Done well it is branded, effortless and completely isolated. Here is what "done well" involves.

A captive portal that represents your brand

The splash page should look like you, not your vendor. Full white-labelling — your logo, colours, imagery, languages, even upsell banners — with no equipment-maker branding. Our captive portal is fully customisable per property.

PMS integration for hotels

The smoothest hotel experience lets a guest sign in with a room number or folio, with access created at check-in and revoked at checkout automatically. That means integrating the network with your Property Management System (Opera, IDS Next, eZee and others). Our Gateway Controller handles this, so the front desk does nothing extra.

Isolation is the whole point

In a hospital, guest devices must never reach clinical, PACS or administrative systems; in a hotel, never the PMS, POS or CCTV. We segment guest traffic onto isolated VLANs with client isolation on NetForce switches — the same segregation model we run at airports.

Flexible authentication and fair use

Different sites need different sign-in: OTP, social login, vouchers, PMS folio or one-click. Pair that with bandwidth tiers and fair-use limits so a few heavy users do not starve everyone else, and you can even offer a paid premium tier as a revenue stream.

Log compliance, handled

Public and guest Wi-Fi in India carries data-retention obligations. We provide DoT / PM-WANI-aligned logging with tamper-evident trails and configurable retention through Net Cloud, so audits are simple.

See how this works for healthcare in our Cardinal Hospital case study, or read the full captive portal & guest Wi-Fi page.

5. AIOps for network operations

“AIOps” gets used loosely. Stripped of the hype, it means one thing: using your network’s own data to find and fix problems faster than a human watching dashboards ever could. Here is what that looks like in practice, and what separates a real AIOps platform from a monitoring tool with a new label.

From alerts to insight

Traditional monitoring floods you with alerts — every symptom of one underlying fault rings its own bell. AIOps learns each site’s normal behaviour, detects anomalies in client, RF and throughput data, and correlates them to a root cause. You act on one insight, not fifty alarms.

From insight to action

The real payoff is automatic remediation. When the platform recognises a known fault pattern it can act — optimise an RF channel, bounce a PoE port, roll back a bad config, repair firmware — either automatically or on one-tap approval. Issues resolve before a ticket is raised. Net Cloud does this across access points, switches and gateways together.

One console for the whole stack

AIOps is only as good as the data it sees. If your APs, switches and gateways live in separate tools, correlation is impossible. A single control plane that manages access points, switches and the gateway together is what makes root-cause analysis work.

What to look for

Ask three questions of any “AIOps” product: does it manage your whole stack from one place; does it give root cause or just more alerts; and can it actually remediate, not only notify? If the answer to all three is yes, you have AIOps. If not, you have a dashboard.

Net Cloud is the brain of the Immunity stack — see the full platform overview or book a tour.