PACNOG 37 • 6 JULY 2026

USP — Laucala Campus, Suva, Fiji

The Invisible Basics

My (MSP's) view of the small networking fundamentals that quietly cause problems

The basics

Packet sizes, names, time, paths

The routing

How BGP & OSPF learn the way

The last mile

Wi-Fi: where users actually feel it

Thomas Murgan ~ Snr. Network Engineer, Netcraft Australia

E: thomas(at)netcraft.com.au

What we'll cover

A high-level tour of network deployment and the fundamentals underneath

How a network fits together

The big picture — from a user's device out to the internet.

The fundamentals

The quiet basics every network leans on: packet sizes, names, time, paths.

How traffic finds its way

Routing and transport — OSPF/BGP/MPLS, and where they go wrong.

The last mile & mixed kit

Wi-Fi, vendor interop, and the things users actually feel.

How we troubleshoot

Divide & conquer, and reading symptoms back to causes.

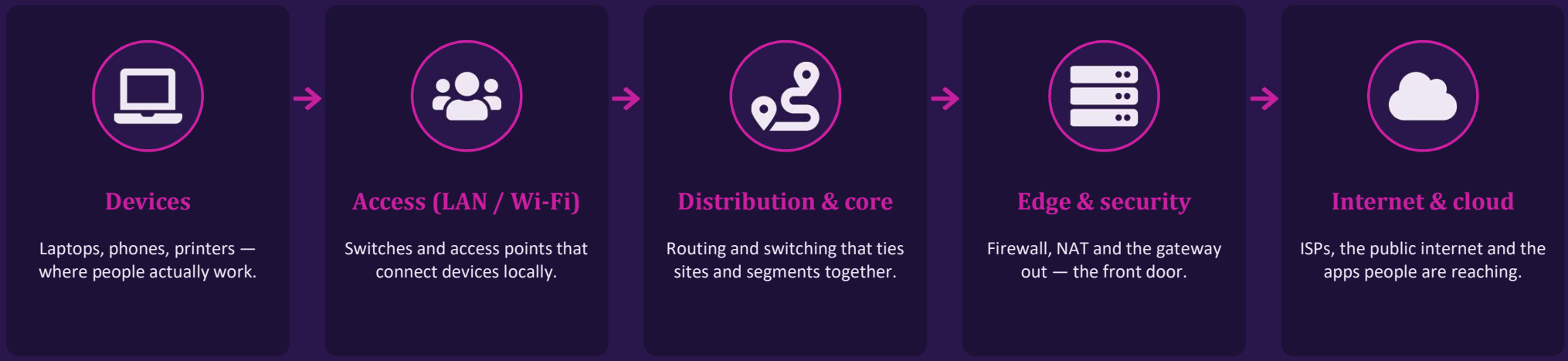
Where it's all heading

SD-WAN, automation and AI — and why the basics still rule.

How a network fits together

Every deployment is layers — a user's click travels through all of them

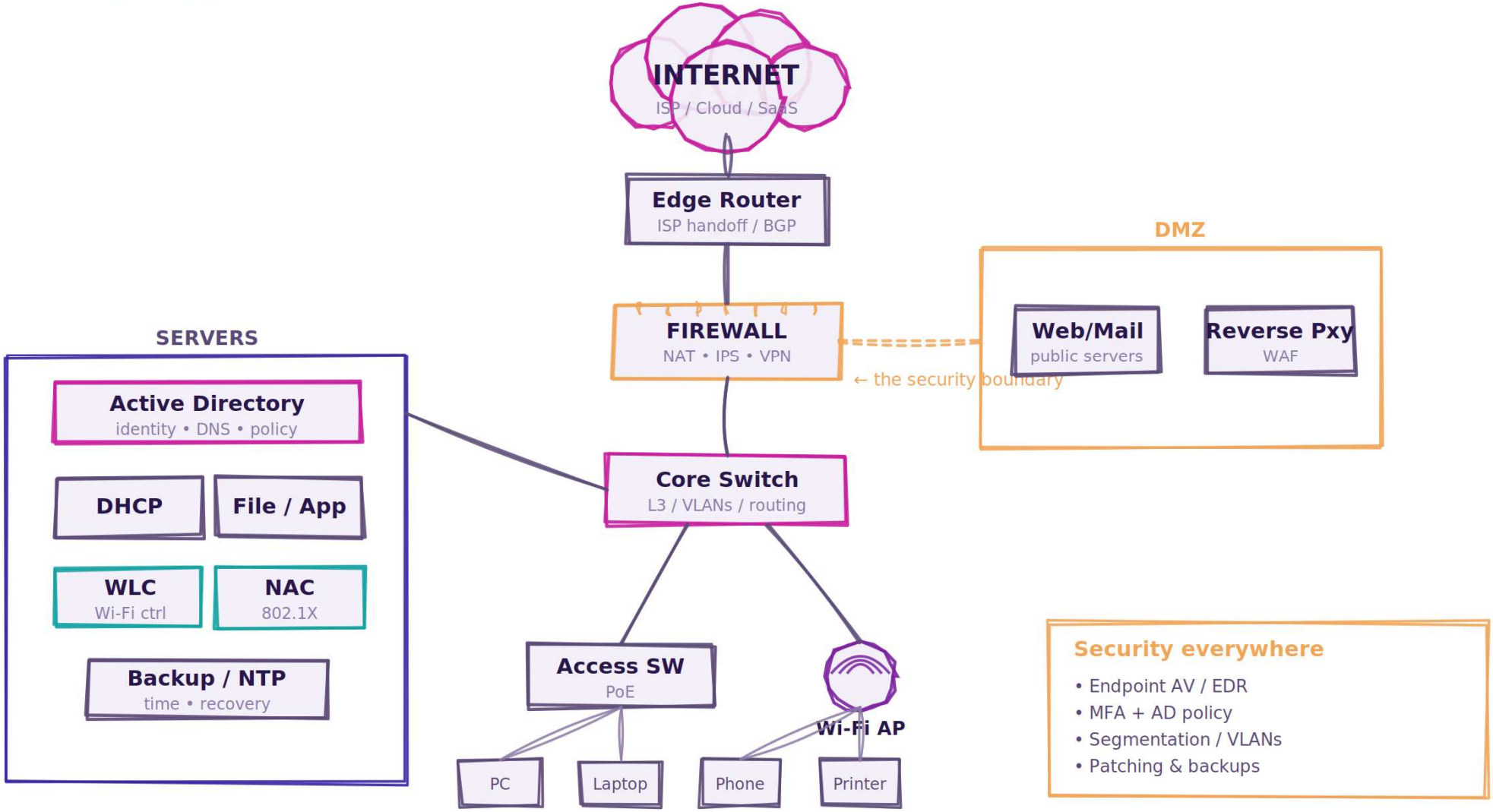
From the device in someone's hand to a server on the other side of the world, traffic passes through the same stages. Knowing the stages tells you where to look when something breaks.



Most faults live at one of these stages — the rest of this talk (sort of) walks them.

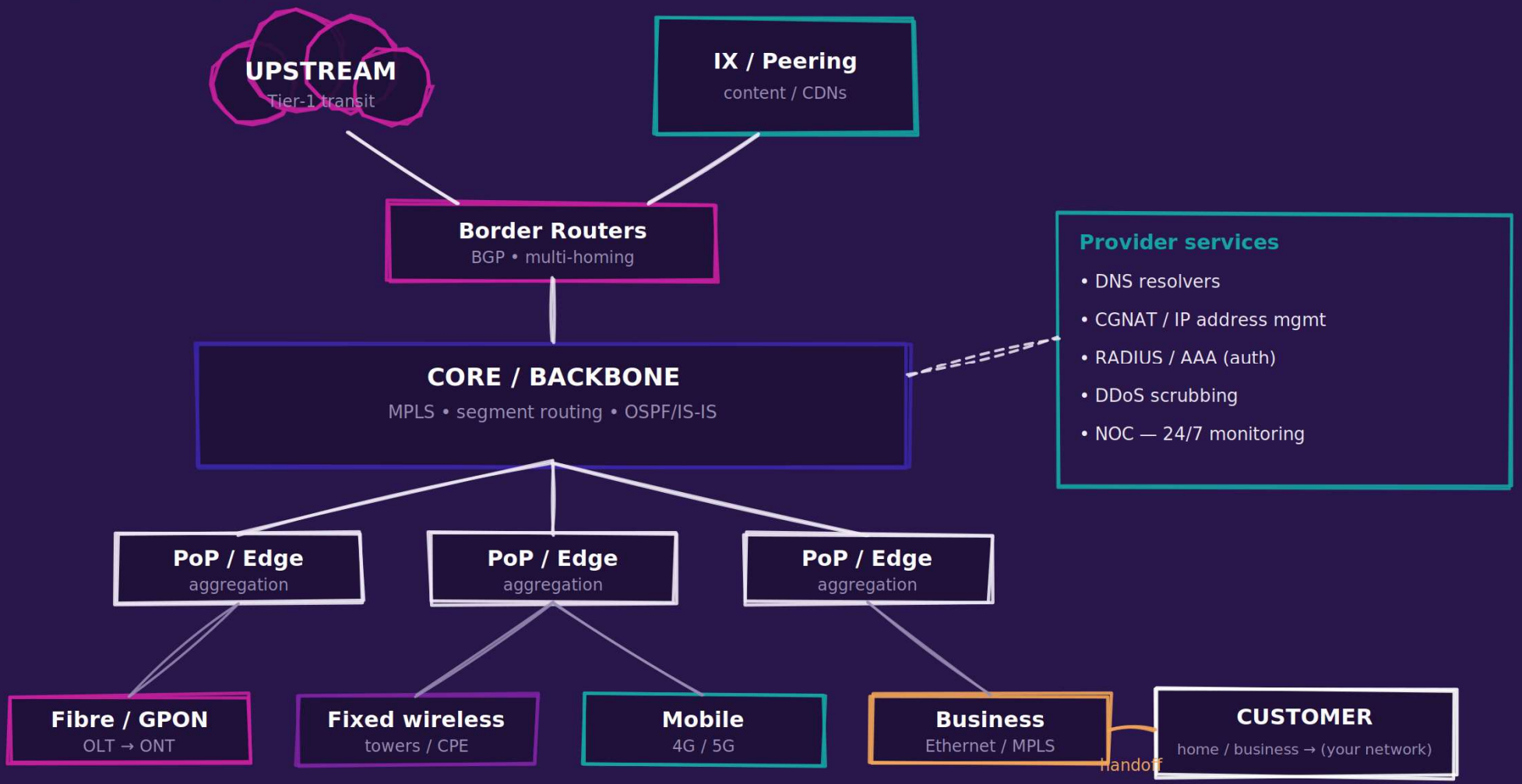
The Enterprise Network

Every element of a typical deployment, and how it connects



The ISP / Provider Network

The carrier network your connection plugs into



Why the basics get missed

The network usually "works" — until one quiet setting bites under the right conditions.

It mostly works

Small misconfigurations hide because everyday traffic never triggers them

Symptoms mislead

"The internet is slow" gets blamed on the ISP, not a packet-size or routing issue

No one owns it

Defaults get inherited from old kit, VPNs and ISP changes nobody revisits

As an MSP, we see the same few culprits again and again — so we check them first.

How networks find the way

How devices and carriers decide which path your traffic takes

The GPS analogy: Devices don't know every road in advance. Routing protocols are the live traffic map — they share which paths exist and pick the best one. When the map is wrong, traffic drives into a dead end.

OSPF / EIGRP / RIP / Static

Inside one organisation

Interior protocols that map the roads within your own network — finding the best path between your sites and devices.

BGP

Between organisations

The map of the whole internet. Decides how your traffic reaches other networks and ISPs — and how the world reaches you.

MPLS

Carried across a provider

Private, labelled “express lanes” a carrier uses to move your traffic between sites — predictable and prioritised, not the public internet.

Segment routing — the modern evolution: the path is written into the packet itself instead of signalled hop-by-hop. Simpler, more programmable, and a natural fit with SD-WAN and automation.

When the map is wrong

Routing problems are quiet, then sudden — and they rarely look like "routing"

Flapping links

A path that keeps dropping and recovering makes the network constantly re-decide — things feel intermittently broken.

Wrong or missing routes

A bad default route or a forgotten static entry sends traffic into a black hole; some sites work, others don't.

BGP at the edge

Lose your internet routing session and you can be invisible to the world even though your office LAN is perfectly healthy.

Overlapping networks

Two sites using the same address range (common after mergers/VPNs) makes traffic go to the wrong place.

MTU & MSS

How big a "chunk" of data the network can carry at once

The moving-truck analogy: MTU is the size of the truck. If a package is too big for a tunnel on the route (a VPN, an ISP link), it must be cut down or it gets stuck. MSS is the two ends agreeing how big each package should be so it always fits.

When it's right

Packets fit end-to-end. Everything just works — fast and invisible.

When it's wrong

Big transfers stall, pages half-load, VPN/email/file shares act 'flaky' while ping looks fine.

When vendors don’t play nice together

“Standards” leave room for interpretation — and mixed kit is where it shows

Two boxes can both “speak BGP” or “do VPN” and still not agree. Defaults, optional features and quirks differ between brands — it works in the lab, then breaks with the client’s existing gear.

Protocol mismatches

Same protocol, different defaults — timers, MTU, hashing or VPN settings that must match exactly on both ends.

“Optional” features

One vendor’s extra (a proprietary tweak, an off-by-default option) that the other side silently ignores or rejects.

Version & firmware gaps

A feature that works on one firmware breaks on another — or a bug only appears in one brand’s implementation.

Vague error trails

Each box blames the other; logs are thin. The fault is the gap between them, not inside either one.

Our habit: test interop on the actual mix before go-live, and keep firmware versions deliberate — not whatever shipped.

Wi-Fi: the last mile

Where most "the internet is bad" complaints are actually born

The link the user actually touches. The fastest fibre in the world doesn't help if the last few metres of Wi-Fi are weak. This is where blame lands — usually unfairly on "the internet."

Coverage & dead spots

Distance and walls kill signal; one bad corner becomes "it's down."

Channel congestion

Too many networks (or your own APs) fighting on the same channel = slow for everyone.

Roaming between APs

Devices clinging to a far AP instead of switching to the close one feels like random drops.

Interference & old kit

Microwaves, neighbours, and ageing access points quietly drag speeds down.

QUICK QUIZ

Thomas was given a 10 Mbit/s link.

What's the maximum download speed Thomas can achieve — in megabytes per second?

- **A** 5 MB/s
- **B** 1.25 MB/s
- **C** 10 MB/s
- **D** 8 MB/s

*Have a guess, please **don't cheat by using AI** — answer on the next slide.*

QUICK QUIZ

Thomas was given a 10 Mbit/s link.

What's the maximum download speed Thomas can achieve — in megabytes per second?

- **A** 5 MB/s
- **B** 1.25 MB/s
- **C** 10 MB/s
- **D** 8 MB/s

Answer: B — 1.25 MB/s

Why: there are 8 bits in a byte, so you divide by 8. 10 Mbit/s ÷ 8 = 1.25 MB/s.

And in the real world: protocol overhead (TCP/IP headers, etc.) shaves a bit more off — expect roughly 1.1–1.2 MB/s. The bits-vs-bytes mix-up is behind countless "my link is too slow!" tickets.

Tshoot - Divide & conquer

Don’t test everything — test the middle, and halve the problem each time

Instead of checking every link end-to-end, test a point in the MIDDLE. Whatever side it fails on, the other half is cleared — then split again.

Halve, don’t hunt

One test in the middle eliminates half the possibilities — a few splits beat checking everything.

Works both ways

Split the PATH (here → internet → far end) or the STACK (cable → IP → DNS → app). Same logic.

Symptom → likely culprit

How we shortcut diagnosis from what the user actually reports

“Ping is fine but big files / VPN / email fail”	→ **MTU / MSS mismatch**
“Some sites work, others don’t / black holes”	→ **Routing or default-route fault**
“The whole office is suddenly off the internet”	→ **BGP / upstream session**
“Everything slow to start, then OK”	→ **DNS resolution**
“Slow for everyone at the busy times of day”	→ **Congestion / link saturation**
“Slow only in one room / keeps dropping”	→ **Wi-Fi coverage or roaming**
“One PC slow, the rest fine”	→ **Duplex / cable / port fault**

Cheap habits that prevent outages

None of this is expensive — it's mostly about checking the boring things on purpose

- **Document the basics** — MTU, DNS, gateways, routing and VPN settings — written down once, saving the 3am guesswork.
- **Test after every change** — ISP swap, new firewall, new VPN — re-check packet sizes, routes and big transfers, not just “can I ping”.
- **Survey the Wi-Fi** — Walk the site, check coverage and channels — don’t design wireless from the comms room.
- **Monitor, don’t wait for calls** — Catch DNS, time drift, link flaps and route changes before users feel them.
- **Standardise across sites** — Same baseline everywhere means problems are obvious and fixes repeatable.

Where networking is heading

New tools change how we run networks — but the basics underneath don't change

SD-WAN & SASE

Software steers traffic across multiple links (fibre, 4G/5G, satellite) and bakes in security.

Wi-Fi offloading

Pushing traffic off cellular onto Wi-Fi — and steering between them — to save mobile data and ease congestion.

Network automation

Configure and check many devices from code, not by hand — fewer typos, faster rollouts.

AI & AIOps

Tools that spot patterns and flag trouble before users call, pointing you at the likely cause.

The catch: automation and AI scale whatever you give them — including mistakes. If MTU, routing or DNS is wrong underneath, these tools just spread it faster. New layers on top; same fundamentals underneath.

The basics are the whole game

Packet sizes, names, time, the routing map and the last mile of Wi-Fi — most "weird" problems are one of these, unchecked. Check the boring things first.

Next time it's "slow," ask: ping OK but big stuff fails? one room or everywhere? That narrows it fast.

Vinaka Vakalevu ~ Thank you

PacNOG 37 • 6 July 2026 • USP Laucala Campus, Suva, Fiji

Visit **https://www.netcraft.com.au** to learn more about the services we offer!