Architecture

MikroTik fabric — architecture

The household network is **three physically separate L2 islands**, not one big switch. Production RSTP roots on the **CCR2116**. Management (vlan89) has its **own WAN, its own root, and its own WireGuard**. The Quickline public `/28` lives on CRS317 and never mixes with the trusted LAN.

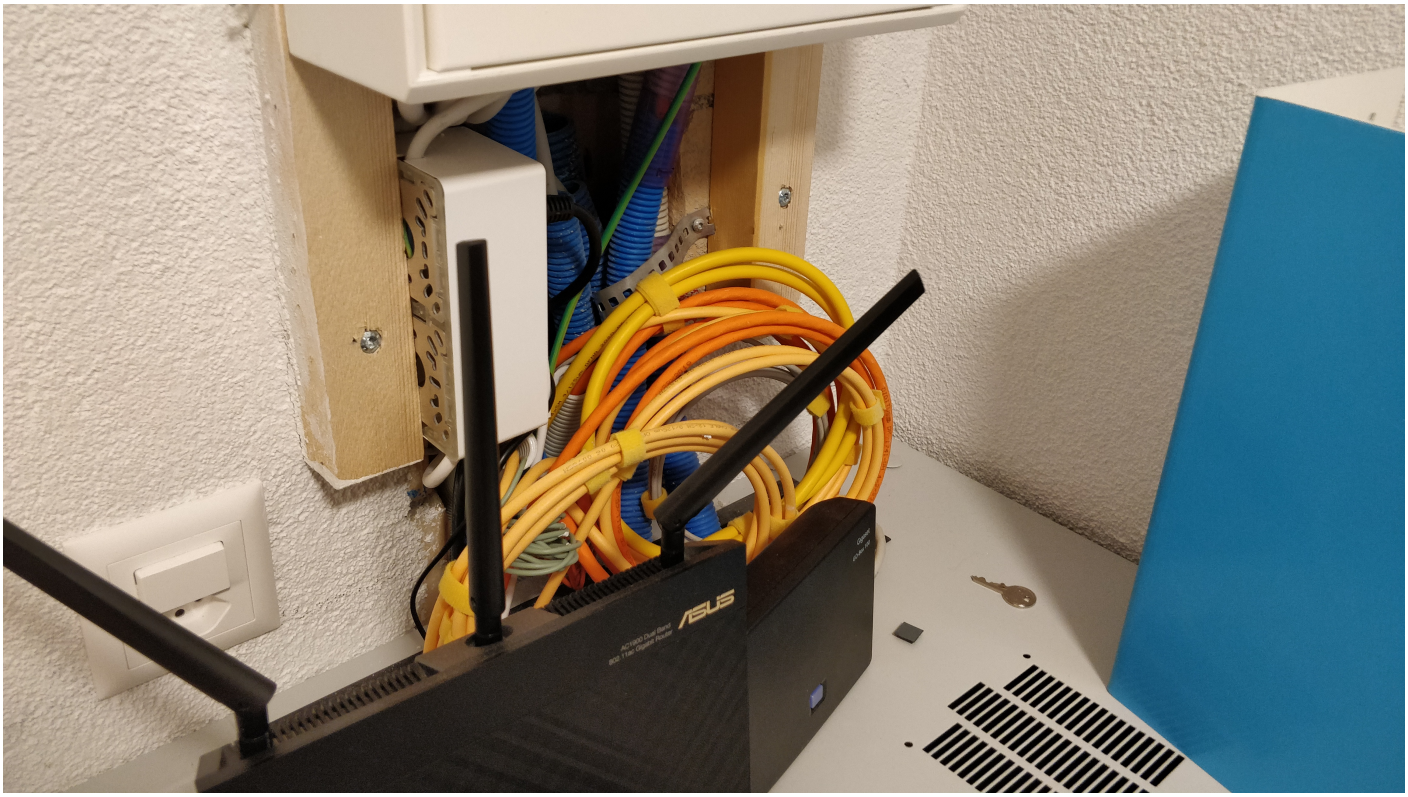
This page is the map. Addressing is on VLAN plan. OSPF, dual ISP and the CHR standby are on Routing and WAN. Device table and remote hEXes are on Devices and sites. Recursive DNS is the DNS APUs book.

Rack photos

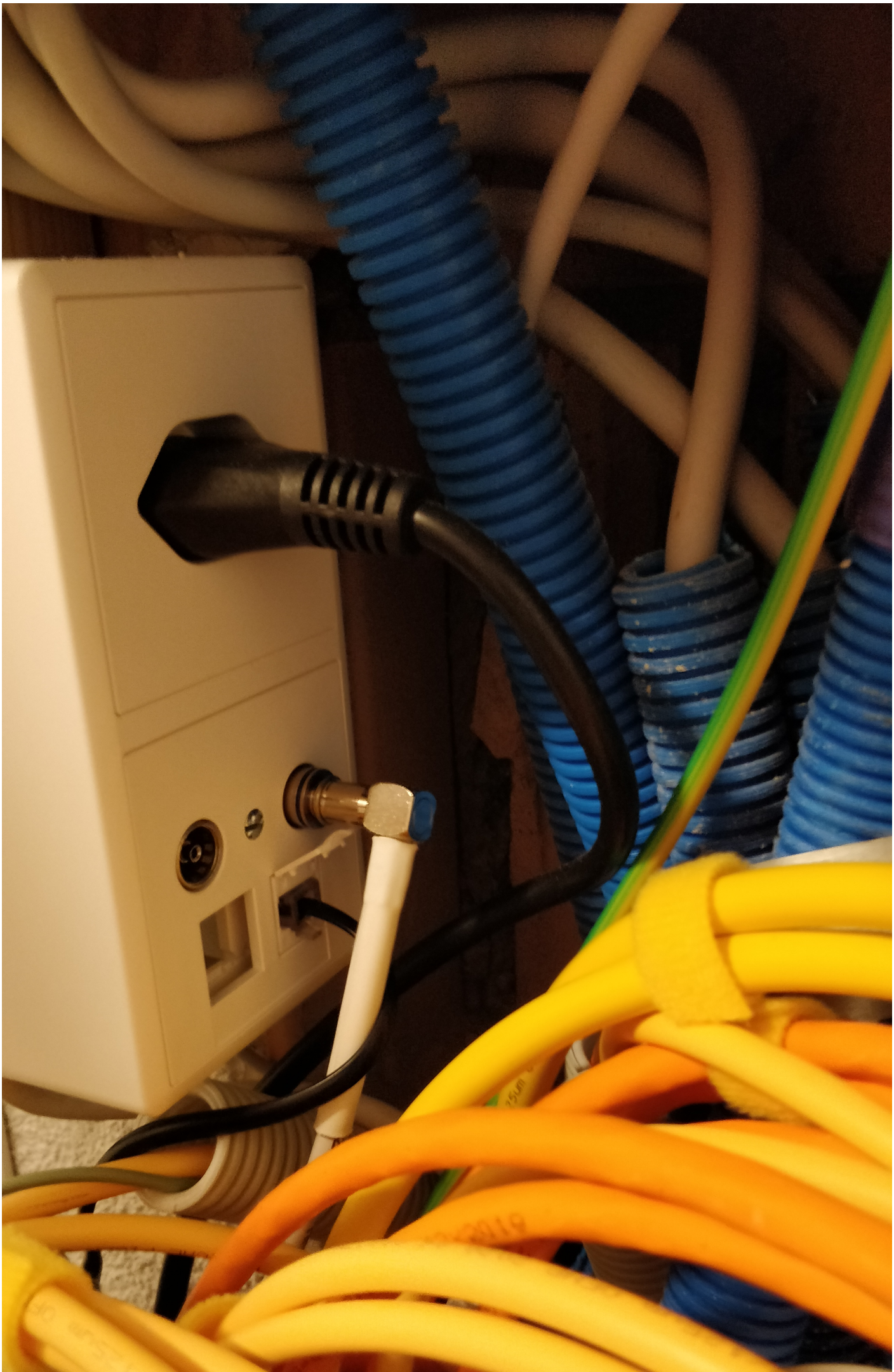
Hardware photos are the 2020 gallery from Fiber at home → Rack. The chassis and fibre plant are the same; the software on the routers has moved on (RouterOS 7.23.5 long-term, dual WAN OSPF, VRRP standby).



Rack top — 2020-11-25



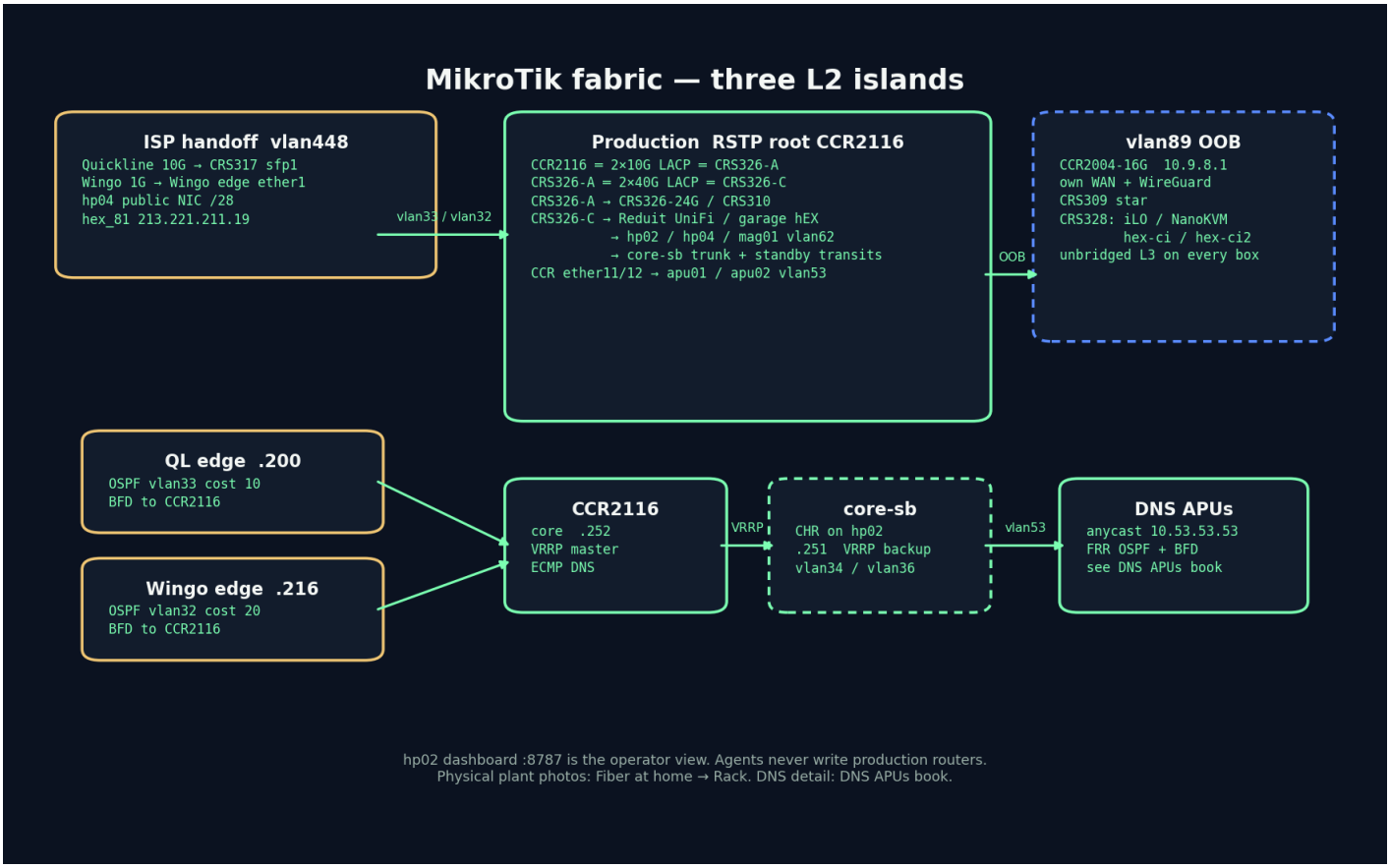
Fibre and copper in the cabinet



Power and internet handoff

Splice inventory and FHD wall boxes stay in Fiber at home. The older iWay / t-online notes stay in Network (historical ISP, not this fabric).

The three islands




```
flowchart TB
  subgraph wan [ISP handoff vlan448]
    QL[Quickline 10G]
    WI[Wingo 1G]
    CRS317[CRS317]
    QL --> CRS317
    WI --> EDGE2[Wingo edge ether1]
  end
  subgraph prod [Production RSTP root CCR2116]
    CORE[CCR2116]
    A[CRS326-A]
    C[CRS326-C]
    CORE -->|"2x10G LACP bond1"| A
```

```
    A -->|"2x40G LACP bond-backbone"| C
    A --> G[CRS326-24G]
    A --> D[CRS310 desk]
    C --> UNI[Reduit UniFi]
    C --> GAR[hEX garage]
    C --> SRV[hp02 / hp04 / mag01 vlan62]
    CORE --> APU[apu01 / apu02 vlan53]
  end
  subgraph oob [vlan89 OOB]
    MGMT[CCR2004-16G 10.9.8.1]
    S309[CRS309]
    S328[CRS328 iLO / NanoKVM / hex-ci]
    MGMT --> S309 --> S328
  end
  CRS317 -->|"vlan33 OSPF"| CORE
  EDGE2 -->|"vlan32 OSPF"| CORE
```

Facts that hold fleet-wide (2026-09-08 wiring review, still the shape on 2026-09-16):

- VLAN filtering with ingress filtering on every bridge; frame-type restrictions on every port.
- BPDU guard and unknown-unicast-flood off on production access ports.
- DHCP snooping on the access switches; CRS326-C `sfp-sfpplus4` (core-sb trunk) is trusted (FAB-21).
- LACP 802.3ad with layer-3-and-4 hashing. Hardware offload on every bridge port. L3 hardware offload **off** on the core and both CRS326-24S+ (on the core it would bypass the filter).
- REST is the telemetry path. SNMP is off. Syslog to hp02. NTP in sync.

How a packet is supposed to move

From	Path	Notes
Trusted host on vlan62	CRS326-C / CRS310 / CRS326-G → backbone → CCR2116 SVI `172.16.62.1`	VRRP VIP; core-sb holds `.3` and takes `.1` if the core dies
Guest / IoT / work / heat pump	Same L2 tree, **different SVI and address-list**	Restricted lists, pathproof intents
DNS	UDP/TCP 53 → **10.53.53.53**; core ECMP-hashes onto the APUs that currently advertise	Rogue DNS is dst-nat'd to the anycast

From	Path	Notes
Router management	**vlan89 only** (`10.9.8.0/24`), from hp02 `10.9.8.253`	hp04 cannot reach vlan89 on purpose
Remote hEX	Prefixes via the Quickline edge / apu01 WireGuard	Not on vlan89; hp02 probes them from vlan62

What this book is not

It is not a runbook to rewrite RouterOS on the live boxes. Production changes are dry-run-by-default `scripts/apply_*.py` that **bodo** applies. Agents read through hp02 and write only to the CHR lab.

Live operator UI: hp02 dashboard (`/overview`, `/vlanplan`, `/wan`, `/sites`, `/sfp`, `/pathproof`).

Revision #2
Created 2026-09-16 16:19:29 UTC by Bodo
Updated 2026-09-16 16:19:33 UTC by Bodo