

MikroTik fabric

Operator view of the household MikroTik fabric: three L2 islands (production, vlan89 out-of-band, Quickline ISP handoff), dual WAN with OSPF + BFD, a CHR VRRP standby on hp02, and the VLAN plan the dashboard judges on `/vlanplan`. DNS anycast lives in the [DNS APUs](https://naumann.dev/books/dns-apus) book. Physical plant photos come from [Fiber at home](https://naumann.dev/books/fiber-at-home). This is not a runbook to rewrite production routers.

- [Architecture](#)
- [VLAN plan](#)
- [Routing and WAN](#)
- [Devices and sites](#)

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.

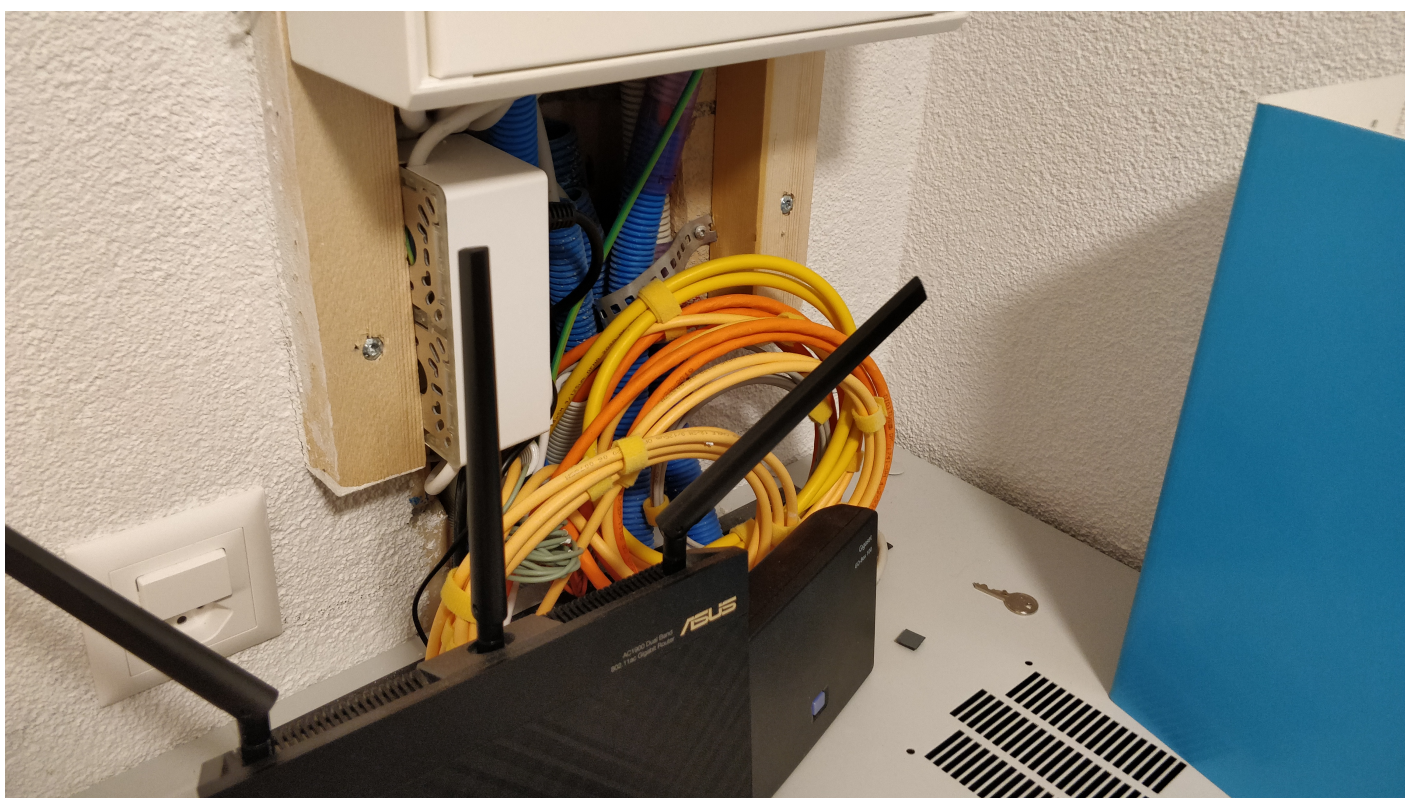
This page is the map. Addressing is on [VLAN plan](#). OSPF, dual ISP and the CHR standby are on [Routing and WAN](#). Device table and remote hEXes are on [Devices and sites](#). Recursive DNS is the [DNS APUs](#) book.

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

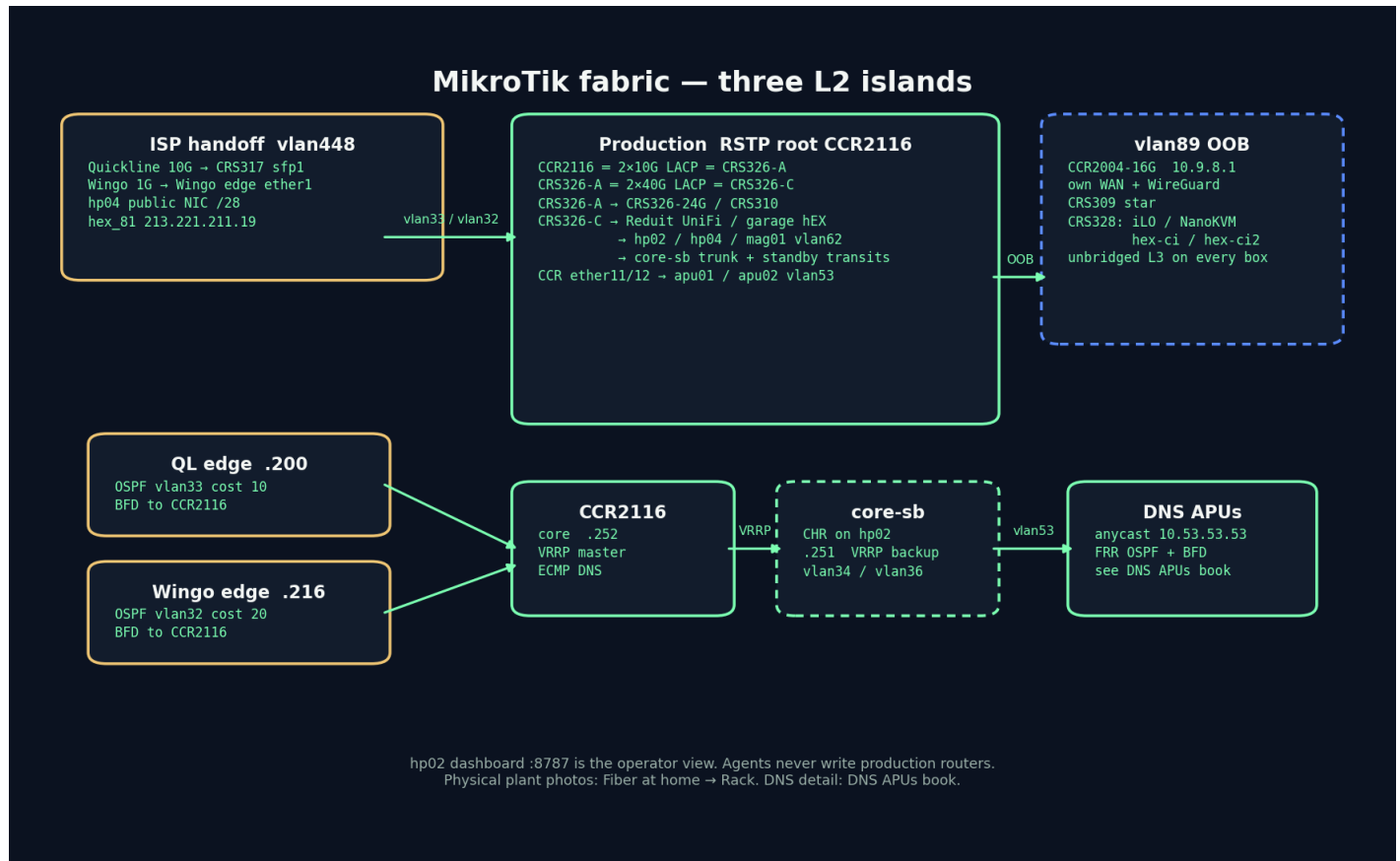


Fibre and copper in the cabinet



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 00B]
  MGMT[CCR2004-16G 10.9.8.1]
  S309[CRS309]
  S328[CRS328 iL0 / 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 <code>172.16.62.1</code>	VRRP VIP; core-sb holds <code>.3</code> and takes <code>.1</code> 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 (<code>10.9.8.0/24</code>), from hp02 <code>10.9.8.253</code>	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`).

VLAN plan

VLAN plan

`vlan_plan.json` in `mikrotik-dashboard` is the git-only intent. The dashboard page `/vlanplan` reads every REST device's bridge / VLAN / port / list membership and judges it against that file. Snapshot below is plan version **2026-09-06**, still the live intent on 2026-09-16 (overview: 0 critical, 2 warnings, 0 unknown VLANs, 16/16 pathproof green).

VLAN groups on the CCR2116

Trusted

62 172.16.62.0/24 servers
58 172.16.50.0/24 CRS326-G
99 172.16.99.0/24 garage

Restricted / IoT

35 work CRS310
58 heat pump garage ether2
59 IoT / Shelly / UniFi
7 / 81 reserved

Guest / DNS

90 guest (no access port)
53 DNS APUs ether11/12
anycast 10.53.53.53

Transit

32 Wingo ↔ core
33 Quickline ↔ core
34 / 36 standby copies

OOB island

89 10.9.8.0/24
own WAN on 16G
WireGuard 10.9.9.0/24

ISP L2

448 Quickline /28
65 Wingo local LAN
not on the core SVIs

Live intent: mikrotik-dashboard vlan_plan.json · judged on /vlanplan · 16 pathproof intents

Production SVIs (CCR2116, VRRP

.1)

VLAN	Name	Prefix / gateway	List on core	Where hosts sit
------	------	------------------	--------------	-----------------

62	LAN-TRUSTED-62	172.16.62.1/24	LAN-TRUSTED	hp02, hp04, mag01, desk (CRS326-C SFP+ and CRS310)
50	LAN-50	172.16.50.1/24	LAN-TRUSTED	CRS326-24G copper (syn01 and neighbours)
99	LAN-TRUSTED-99	172.16.99.1/24	LAN-TRUSTED	Garage hEX management; CRS310 ether4
35	LAN-WORK	172.16.35.1/24	LAN-RESTRICTED	CRS310 ether3 "Work"
58	LAN-HEATPUMP	172.16.58.1/24	LAN-RESTRICTED + VLAN58-ANY	Garage hEX ether2 → Luxtronik 172.16.58.10
59	LAN-IOT	172.16.59.1/24	LAN-IOT	Shelly / UniFi / Ikea; FAB-10 moved this off LAN-TRUSTED
90	LAN-GUEST	172.16.90.1/24	LAN-GUEST	Carried on core + both CRS326-24S+; no access port today
7	LAN-RESTRICTED-7	172.16.7.1/24	LAN-RESTRICTED	No adopted access port
81	LAN-RESTRICTED-81	172.16.81.1/24	LAN-RESTRICTED	Core-only reserved; never had a host

core-sb (CHR on hp02) holds the same SVIs as VRRP backup: real .3, VIP .1, priority 100. DHCP scopes on the standby are **disabled until it is VRRP master**.

DNS fabric

VLAN	Name	Prefix	Notes
53	LAN-DNS	192.168.53.0/24 gw 192.168.53.1	Untagged on CCR2116 ether11 (apu01) and ether12 (apu02) only. OSPF + BFD.
—	anycast	10.53.53.53/32 on each APU 10	Advertised by FRR. Clients never pick a box. See DNS APUs .

Unbound ACL is fabric prefixes, not all of RFC1918. Production DHCP DNS is the anycast, not a vlan89 Grafana address.

Routed transits (not bridged)

VLAN	Name	Prefix	Speakers	Cost
33	TRANSIT-QUICKLINE	192.168.33.0/24	QL edge .1 ↔ core .2	10 + BFD
32	TRANSIT-WINGO	192.168.32.0/24	Wingo edge .1 ↔ core .2	20 + BFD
34	TRANSIT-STANDBY-QUICKLINE	192.168.34.0/24	QL edge ↔ core-sb	30 (no BFD yet)
36	TRANSIT-STANDBY-WINGO	192.168.36.0/24	Wingo edge ↔ core-sb	40 (no BFD yet)

Standby transits live on **CRS326-C only**, not on the backbone. That is how the CHR can talk OSPF to both edges without depending on the CCR2116.

Other islands

VLAN	Name	Prefix	Island
89	MGMT	10.9.8.1/24 on CCR2004-16G	Out-of-band. Every other device joins with an unbridged L3 port . REST, Winbox, iLO, NanoKVM, hex-ci.
448	ISP-HANDOFF	Quickline 213.221.211.16/28	CRS317 fan-out. hp04's public NIC, QL edge WAN, hex_81. Not a core SVI.
65	WINGO-LAN	192.168.65.1/24	Local LAN on the Wingo CCR2004 only.

WireGuard on the mgmt router is 10.9.9.0/24 (wg1). Home WireGuard (wg-home) terminates on **apu01** 172.16.75.1/24, not on the CCR2116.

```
flowchart LR
    subgraph trusted [LAN-TRUSTED]
        V62[vlan62 servers]
        V50[vlan50 copper]
        V99[vlan99 garage]
    end
    end
    subgraph rest [Restricted]
```

```
V35[vlan35 work]
V58[vlan58 heatpump]
V59[vlan59 IoT]
V90[vlan90 guest]
end
CORE[CCR2116 SVIs]
trusted --> CORE
rest --> CORE
CORE --> WAN[vlan32 / vlan33 OSPF]
CORE --> DNS[vlan53 + 10.53.53.53]
00B[vlan89 10.9.8.0/24] -->|unbridged L3| BOXES[every router / switch]
```

How to read `/vlanplan`

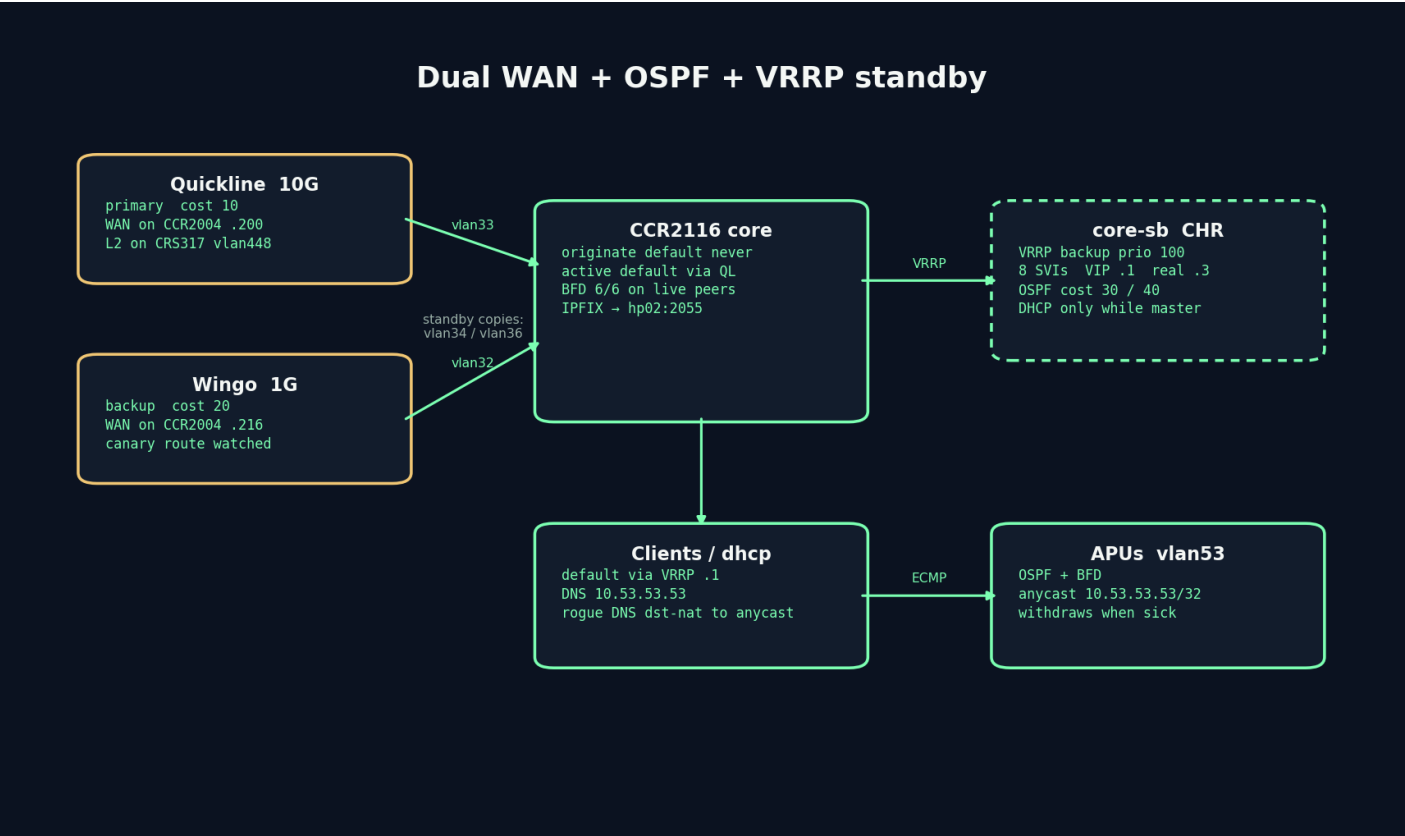
A link is a **trunk** only when both ends tag at least one VLAN (routed vlan sub-interfaces count). Access ports must match the plan's `pvid`. Unknown VLANs and unplanned access ports show as findings; they are not silently adopted into git.

Live UI: <http://172.16.62.253:8787/vlanplan>.

Routing and WAN

Routing and WAN

Two ISPs, OSPF with BFD, a canary route, and a CHR hot standby. The core **does not originate default**; it installs whichever ISP is cheaper and currently adjacent.



Dual ISP

Path	Box	WAN	Transit to core	OSPF cost	BFD
Primary	CCR2004 Quickline 10.9.8.200	10G on CRS317	vlan33 192.168.33.0/24 (core sfp-sfpplus4 ↔ edge sfp-sfpplus2)	10	yes

Path	Box	WAN	Transit to core	OSPF cost	BFD
Backup	CCR2004 Wingo 10.9.8.216	1G on ether1	vlan32 192.168.32.0/24 (core sfp- sfpplus1 ↔ edge sfp-sfpplus2)	20	yes

Dashboard `/wan` names the active path (`quickline` expected) and whether the Wingo canary is alive. Fail-over is an audited drill (`docs/wan-failover-drill-dash06.md` in the dashboard repo), not a DHCP-timeout flip.

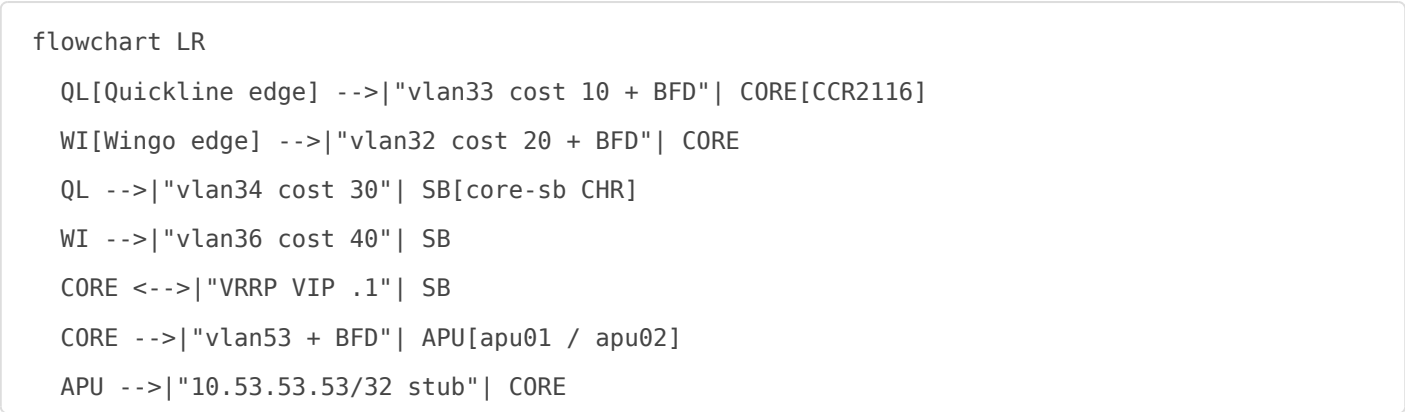
Wingo also has a **VPN fallback** dst-nat of UDP/13231 toward apu01 (`wg-home`). That path is configured; the handshake drill is still awaiting a bodo window.

VRRP standby (FAB-13)

`core-sb` is a RouterOS CHR on hp02 (`10.9.8.251`).

- VRRP backup, priority 100, on SVIs **7 / 35 / 50 / 58 / 59 / 62 / 90 / 99**.
- Real address `.3`, VIP `.1` (the address clients already use).
- Own OSPF to both edges: vlan34 cost 30 (Quickline copy), vlan36 cost 40 (Wingo copy).
- DHCP servers stay **disabled** until VRRP master.
- Config is generated from the **live** core (`scripts/gen_core_standby.py`). Drift is the standby tile on the dashboard.
- Trunk is hp02 `eno5np0` → CRS326-C `sfp-sfpplus4`. That port is DHCP-snooping **trusted** so a real core failure can still offer leases.

vlan53 (DNS) and vlan81 are **not** on the standby. The APUs stay pinned to the CCR2116.



DNS in the routing picture

Clients send DNS to **10.53.53.53**. Each APU puts that address on `lo` and FRR advertises it as an OSPF stub. The core ECMP-hashes **per source/destination pair**. One probe source only ever sees one arm — that is why `/dns` probes from both `172.16.62.253` and `10.9.8.253`.

If an APU cannot serve DNS it **withdraws** the address from `lo` (anycast healthcheck). OSPF Full with an empty kernel FIB is not enough; that was the Sep 2026 blackhole. Full story: [DNS APUs — Anycast self-heal](#).

The core also intercepts rogue DNS (dst-nat of UDP/TCP 53 not already aimed at 10.53.53.53, from sources not on `DNS-SERVERS`) and sends it to the anycast.

Management-plane routing

vlan89 is a **different router**: CCR2004-16G `10.9.8.1`, own WAN (`213.221.211.27`) and WireGuard (`10.9.9.1`). Every fabric device joins it with an unbridged L3 port. That island surviving when production RSTP or the CCR2116 is down is the point.

OOB recovery path: WireGuard → `10.9.8.1`. Keep that reachable in every change plan.

hp02 talks RouterOS REST **only** from `10.9.8.253` (and its own vlan62 address is not used to reach routers). hp04 has a public `/28` address on vlan448 **and** a vlan62 NIC; it must not forward between them. Agents on hp04 jump through hp02 for every fabric command.

What `/wan` and `/overview` should look like when healthy

From the 2026-09-16 dashboard snapshot used to write this book:

- devices 21 / 21 up, watched uplinks up
- OSPF 4 / 4 Full, BFD 6 / 6 up
- active default via Quickline, canary active
- pathproof 16 / 16 green
- DNS probes 9 / 9, anycast 3 / 3, cache hit ~99 %

Devices and sites

Devices and sites

Source of truth: `mikrotik-dashboard/inventory.json`. REST is allow-listed to hp02. Addresses below are the **management** IPs the dashboard uses (vlan89 `10.9.8.x` first).

L3 routers

Role	Device	OOB	Notes
Core	CCR2116-12G-4S+	<code>10.9.8.252</code>	RSTP root of production (<code>0x1000</code>). OSPF RID <code>10.255.255.16</code> .
Standby	core-sb (CHR on hp02)	<code>10.9.8.251</code>	VRRP backup, OSPF vlan34/36.
Primary WAN	CCR2004 Quickline	<code>10.9.8.200</code>	OSPF vlan33 cost 10 + BFD. WAN on CRS317.
Backup WAN	CCR2004 Wingo	<code>10.9.8.216</code>	OSPF vlan32 cost 20 + BFD.
Mgmt island	CCR2004-16G-2S+	<code>10.9.8.1</code>	vlan89 gateway, own WAN, WireGuard <code>10.9.9.1</code> .

Switch fabric

Role	Device	OOB	STP
ISP switch	CRS317-1G-16S+	<code>10.9.8.212</code>	vlan448 island root
Spine	CRS326-24S+2Q+_A	<code>10.9.8.205</code>	production <code>0x2000</code>
Access-core	CRS326-24S+2Q+_C	<code>10.9.8.213</code>	production <code>0x3000</code> ; servers, UniFi, garage, core-sb trunk
Copper access	CRS326-24G-2S+	<code>10.9.8.249</code>	vlan50 / vlan62 / vlan59
Desk	CRS310-8G+2S+	<code>10.9.8.203</code>	work / IoT / brother

Role	Device	OOB	STP
PoE (vlan448 + OOB)	CRS418-8P-8G-2S+	10.9.8.204	access
Mgmt fabric	CRS309-1G-8S+	10.9.8.210	vlan89 star
Mgmt PoE	CRS328-24P-4S+	10.9.8.232	hp02 mgmt, iLO, NanoKVM, hex-ci
Mgmt leaf	CRS305-1G-4S+	10.9.8.202	vlan89

Servers and DNS

Host	Addresses	What it is
hp02	172.16.62.253 vlan62, 10.9.8.253 vlan89	Dashboard :8787 , Gitea :3030 , CHR labs, syslog, backups. Only host allowed to hit RouterOS REST. iLO 10.9.8.218 .
hp04	172.16.62.40 vlan62 and 213.221.211.30/28 public	Workspace + CI runners. Cannot reach vlan89. Must not forward public ↔ LAN. iLO 10.9.8.224 .
mag01	172.16.62.246	CI lab runner (lab label).
apu01	10.9.8.206 / 192.168.53.3 / wg0 172.16.75.1	Unbound + FRR. SSH bodo . DNS APUs .
apu02	10.9.8.207 / 192.168.53.2	Same without wg-home.
NanoKVM	10.9.8.225 / .229 / .230	OOB console.

CPE and lab hardware

Device	Address	Notes
hEX S garage	172.16.99.69	Trunk vlan58/59/99 to CRS326-C sfp14. ether2 = Luxtronik. REST from hp02's vlan62 address (no vlan89 route).
Luxtronik	172.16.58.10	Isolated on vlan58. Path attested on /pathproof .
hex-ci	10.9.8.240	Physical hEX lab on vlan89. Agents may reconfigure it. Dual uplink into CRS328, RSTP blocks one. Rescue 192.168.88.1 .
hex-ci2	10.9.8.241	Same pattern, CRS328 ether7/8.

Lab networks on chr/lab/fwlab stay in 198.18.0.0/15 (and the other documentation prefixes). Never put a lab bridge on 10.9.8.0/24, 172.16.0.0/12, 192.168.53.0/24, or 100.64.0.0/10.

Remote sites

Reached from hp02's production NIC, not vlan89.

Site	Prefix / CPE	Path
hex_51	172.16.52.1	Quickline WG / EoIP; prefixes also via apu01 OSPF
hex_19	172.16.18.1	Same
hex_81	213.221.211.19	On the vlan448 public segment

/sites is the live tunnel view (peers, last handshake). A leftover NEVER peer is a display bug, not a down site.

Operator surfaces

Surface	URL	Use
Overview	http://172.16.62.253:8787/overview	Fleet health, issues, WAN, DNS, pathproof
VLAN plan	http://172.16.62.253:8787/vlanplan	Intent vs live bridges
WAN	http://172.16.62.253:8787/wan	Which ISP, canary
Sites	http://172.16.62.253:8787/sites	Remote tunnels
SFP / optics	http://172.16.62.253:8787/sfp	DDM, path loss
DNS / APU	http://172.16.62.253:8787/dns · /apu	Anycast probes; metrics over SSH after HOST-APU-01
Gitea	http://172.16.62.253:3030/bodo/mikro tik-dashboard	Issues, PRs, CI
Grafana APUs	http://10.9.8.206:3000/ · http://10.9.8.207:3000/	vlan89 only

Related books

- [DNS APUs](#) — Unbound anycast, self-heal, listen map
- [Fiber at home](#) — splice plant, FHD boxes, 2020 rack photos
- [Network](#) — historical iWay / t-online / DrayTek, not this fabric

Rules that do not change because a page exists

Agents **never write production routers**. Deliverable is a dry-run script plus a one-liner for bodo. hp02 is the jump host. This book is the picture, not a change ticket.