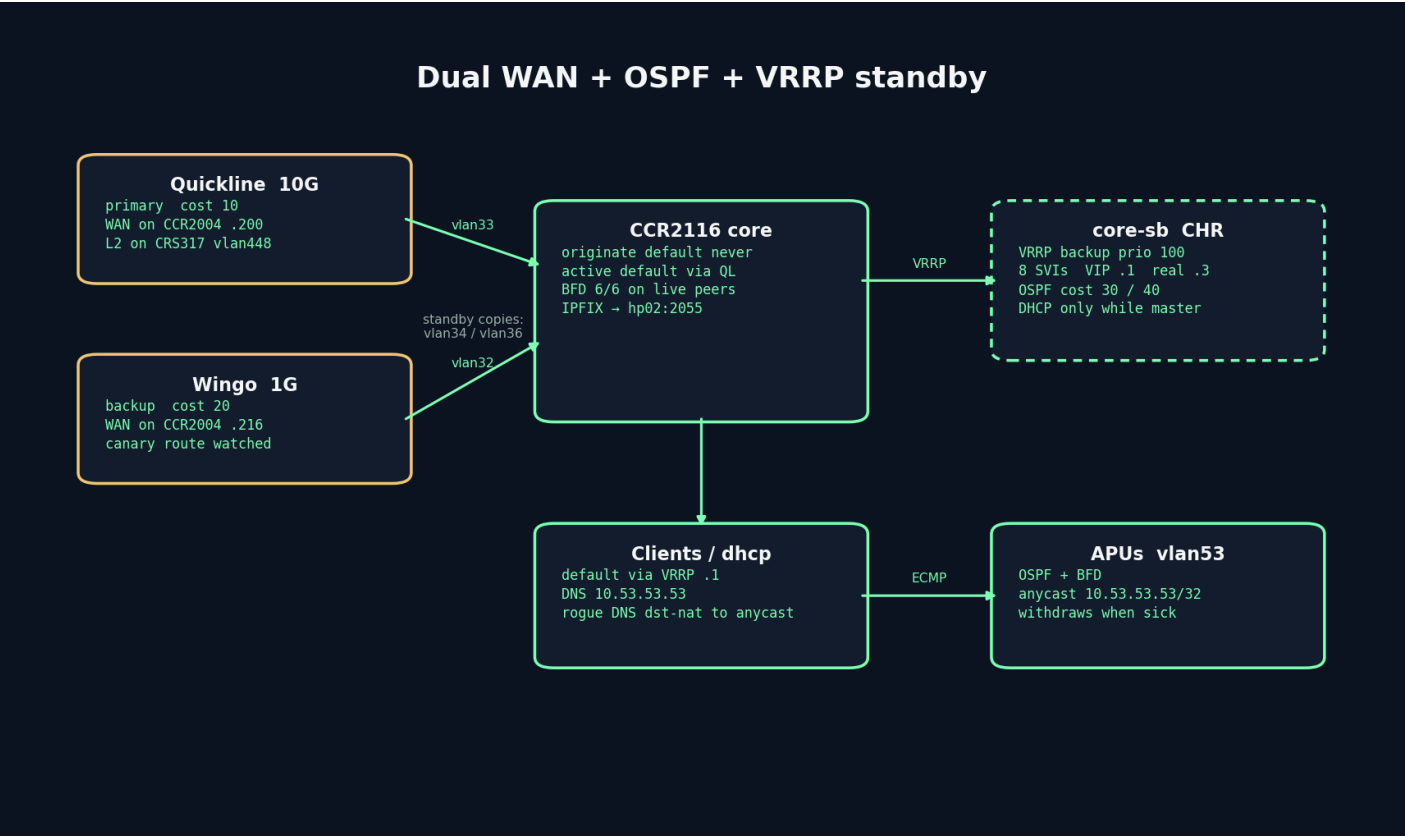


Routing and WAN

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- sfppplus1 ↔ edge sfp-sfppplus2)	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.

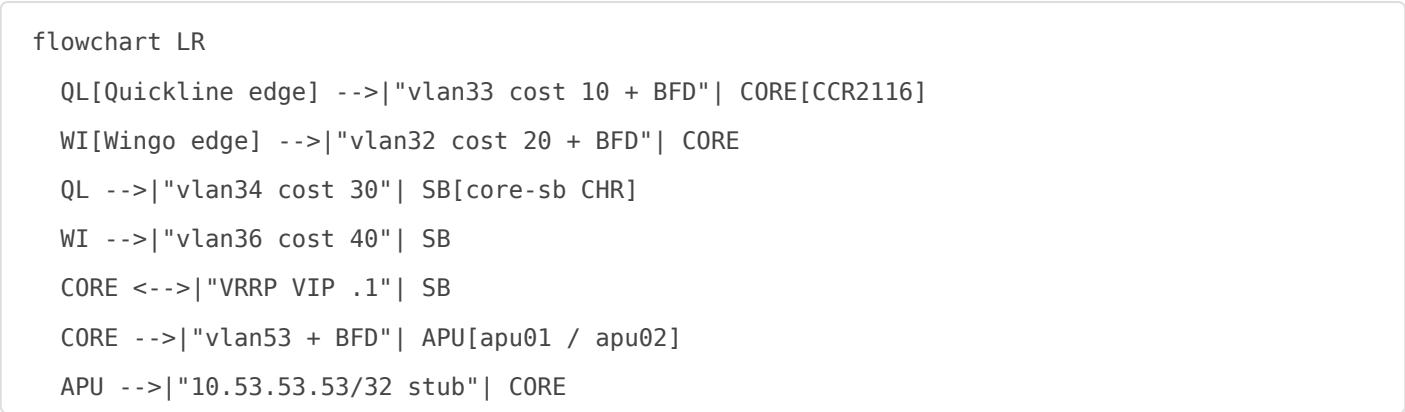
Wingo also has a **VPN fallback** dst-nat of UDP/13231 toward apu01 (`wg-home`). That path is configured; the handshake drill is still awaiting a bodo window.

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-sfppplus4`. 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 %

Revision #2

Created 2026-09-16 16:19:30 UTC by Bodo

Updated 2026-09-16 16:19:37 UTC by Bodo