

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).



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>.

Revision #2

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

Updated 2026-09-16 16:19:35 UTC by Bodo