AFRIDYNE SYSTEMS · TECHNICAL GUIDE

VLANs for Home and Small Office

Keep guests, smart gadgets and cameras off your main network.

Updated November 2026 | home and small office | about 10 minutes to read

A VLAN splits one physical network into separate virtual ones. The classic uses are keeping guests off your main network, isolating smart-home gadgets and CCTV cameras, and keeping office computers apart from everything else. Devices on different VLANs cannot see each other unless you allow it.

> **What you need:** a router or firewall that supports VLANs (OpenWrt, pfSense, OPNsense, MikroTik and Ubiquiti all do; most ISP-supplied routers do not), a *managed* switch that supports 802.1Q, and Wi-Fi access points that can map several networks to VLANs.

1. Decide what to separate

Keep it small. Three or four VLANs cover most homes and small offices.

VLAN	Name	Range	Can reach
10	Main	`192.168.10.0/24`	Everything, including the internet
20	Guests	`192.168.20.0/24`	Internet only
30	IoT and cameras	`192.168.30.0/24`	Internet only (or one NVR)
99	Management	`192.168.99.0/24`	Switches and access points

2. Tagged and untagged, in plain words

- **Untagged (access) port:** one device plugged in, belonging to one VLAN. Used for a PC, printer or camera.
- **Tagged (trunk) port:** carries several VLANs at once, each frame labelled with its VLAN number. Used between the router and switch, and to access points.

3. Build it in this order

1. **Router:** create a VLAN interface for each VLAN (10, 20, 30, 99), give each its own address, and turn on DHCP for each range.
2. **Router firewall:** allow Main to reach everything; allow Guests and IoT to reach the internet only. Block Guests and IoT from the other VLANs.
3. **Switch:** make the port to the router a trunk carrying all VLANs. Set each device port to untagged in the VLAN it belongs to. Make the access point port a trunk.
4. **Access points:** create one Wi-Fi name per VLAN (for example a separate Guest network) and tie each to its VLAN number.
5. **Test:** connect a phone to Guest Wi-Fi. It should reach the internet but not your main computers or printer.

> **Do not lock yourself out.** Change the switch port you are using to configure last, and keep your own computer on the Main or Management VLAN. If a change drops you, unplug and replug your cable or reset the switch to recover.

4. Checking a VLAN on a Linux machine

These commands are useful when testing a trunk port. They are temporary and disappear after a reboot. Replace `eth0` with your interface name.

terminal

```
sudo ip link add link eth0 name eth0.30 type vlan id 30
sudo ip addr add 192.168.30.50/24 dev eth0.30
sudo ip link set eth0.30 up
ip -d link show eth0.30
```

To watch tagged traffic arriving on the port:

terminal

```
sudo tcpdump -e -n -i eth0 vlan
```

Remove the test interface when you are done:

terminal

```
sudo ip link delete eth0.30
```

Common problems

- **Devices get no address:** DHCP is not running on that VLAN, or the trunk does not carry that VLAN number.
- **Wrong network on Wi-Fi:** the SSID is not tied to the right VLAN on the access point.
- **Printing or casting stops working:** these use discovery that does not cross VLANs. Put the printer in the same VLAN, or add a specific firewall rule.
- **Everything can still see everything:** the VLANs exist but the firewall rules between them are missing.