5 Common VLAN Mistakes I Still See (and How to Avoid Them)



https://www.linkedin.com/pulse/5-common-vlan-mistakes-i-still-see-how-avoid-them-jarryd-de-oliveira-babce

VLANs are one of the simplest yet most powerful tools we have in networking. Whether you're isolating IoT devices, building a secure guest Wi-Fi, or segmenting traffic in a complex enterprise, VLANs give order and control to what would otherwise be chaos.

But despite being such a foundational concept, I still see the same mistakes made repeatedly across home networks, small businesses, and even large enterprise deployments.

Here are five of the most common VLAN missteps and how to avoid them, with examples from different sectors where these mistakes can have real impact.

1. Leaving the Native VLAN in Use

By default, most switches drop untagged traffic into the "native" VLAN (often VLAN 1). Many engineers leave it as-is, but this opens the door to both security and troubleshooting issues.

Best practice: Assign an unused VLAN (e.g., VLAN 999 or 888) as the native VLAN and shut down any unused ports by placing them into that VLAN. That way, if untagged traffic appears, it's effectively blackholed.

Scenarios:

- **Hospitality:** A guest plugs into a spare Ethernet port in a hotel conference room. If that port is left in VLAN 1, they may accidentally (or maliciously) gain access to internal systems.
- **Enterprise:** A mismatched trunk configuration between Cisco and HP switches defaults to different native VLANs, leading to spanning-tree loops and hours of downtime.
- **Home networks:** That cheap smart TV you just connected doesn't tag traffic properly. If your native VLAN is active, it suddenly has access to your work-from-home lab gear.

2. Native VLAN Mismatches on Trunks

I've walked into too many environments where the native VLAN doesn't match on both ends of a trunk link.

The result? Inconsistent connectivity, VLAN hopping risks, and troubleshooting nightmares.

Best practice: Explicitly configure trunk VLANs on both sides and ensure the native VLAN is the same everywhere or better yet, unused entirely.

Scenarios:

- **Warehousing & Logistics:** An Autonomous Mobile Robot (AMR) controller in the warehouse can't communicate because one trunk has VLAN 20 as native and the other

defaults to VLAN 1. Result: production floor downtime.
- **Healthcare:** Wireless access points in a hospital drop off the network because the management VLAN isn't consistently tagged across all trunk uplinks.

3. No Dedicated Management VLAN

If your switches, firewalls, and APs share the same VLANs as user traffic, you're asking for lockouts and headaches.

Best practice: Always use a dedicated management VLAN that is allowed across all trunks. This provides a reliable "back door" to access your gear when other VLANs are misbehaving.

Scenarios:

- **Hospitality:** During a guest Wi-Fi outage, engineers can't even log into the access switches because management is tied to the same VLAN as guest traffic.
- **Enterprise campus:** Firewall misconfiguration pushes a new rule that blocks IT from reaching their own core switches. With a management VLAN in place, recovery is minutes instead of hours.
- **Home labs:** Tinkering with VLAN tagging on your main SSID accidentally knocks out DHCP. Without a management VLAN, your switch is now unreachable without a factory reset.

4. Incorrect Access vs. Trunk Port Assignments

I often see devices like access points or IP phones placed on the wrong type of port. An AP connected to an access-only VLAN won't broadcast multiple SSIDs. A phone trunk misconfigured as access can break VoIP.

Best practice: Double-check your design. Endpoints (PCs, TVs, cameras) go on access ports. Devices that need to carry multiple VLANs (APs, switches, IP phones with passthrough PCs) go on trunks. Prune unused VLANs from trunks to reduce unnecessary broadcast traffic.

Scenarios:

- **Corporate office:** A VoIP phone and PC are daisy-chained, but the port is left in access mode. The phone works, but the PC behind it never gets an IP.
- **Healthcare:** Wireless access points in patient wards lose connectivity to the voice VLAN because trunks weren't configured correctly.
- **Home networks:** You set up VLANs for IoT and guest Wi-Fi, but your AP is connected to an access port. Suddenly, all SSIDs are dropping into the same VLAN, defeating the purpose.

5. Using Unmanaged Switches in a VLAN Environment

The quickest way to break a carefully segmented VLAN design is by adding an unmanaged switch into the mix. These devices don’t understand VLAN tags, some strip them, some drop them, and some behave inconsistently.

Best practice: Always use managed switches end-to-end if VLANs are in use. Even for small environments, the cost difference is negligible compared to the troubleshooting time saved.

Scenarios:

- **Retail:** A store manager adds a cheap switch behind the till to plug in more devices. Suddenly, payment terminals lose PCI isolation, and compliance auditors raise a red flag.
- **Warehouse:** A supervisor plugs an unmanaged switch into a trunk port for “extra ports,” breaking communication for half the racking APs.
- **Home networks:** You carefully separated your IoT VLAN from your work devices. Then you add a small unmanaged switch in your office and suddenly the VLAN tags are gone and everything is dumped back into the same network.

Final Thoughts

VLANs aren’t complicated, but sloppy implementation can introduce big risks.

Across every sector I’ve worked in, hospitality, logistics, healthcare, enterprise and even with home labs, the same mistakes come up time and time again.

The good news? They’re all avoidable with careful planning, consistent configuration and a mindset of **“design with intent.”**

Whether you’re segmenting thousands of devices in a warehouse or just keeping your smart bulbs away from your work laptop at home, following these practices will keep your network secure, stable, and easier to manage.

Revision #2
Created 29 August 2025 04:23:00 by Jarryd
Updated 29 August 2025 04:41:19 by Jarryd