Using Virtual LANs at Home

James Henstridge
June 2025

What I wanted to do

What are VLANs?

How do they work?

VLAN support in Linux

Managed or Smart Switches

What I wanted

I don’t trust all the devices on my network equally.

I have some IoT that only need to talk to their cloud service.

I’ve hosted PLUG hack days, and didn’t want to give full access to my computers and devices.

I wanted to be able to be able to isolate some devices whether they were wired or wireless.

What are VLANs

A method of turning one physical network link into many logical networks

Operates at “layer 2”

Can be implemented in pure software, but will be more useful with support from the network switch

Layer 2?

Reference to OSI network model

Runs at a layer below TCP and IP

Only concerned with sending packets to other nodes on the same link.

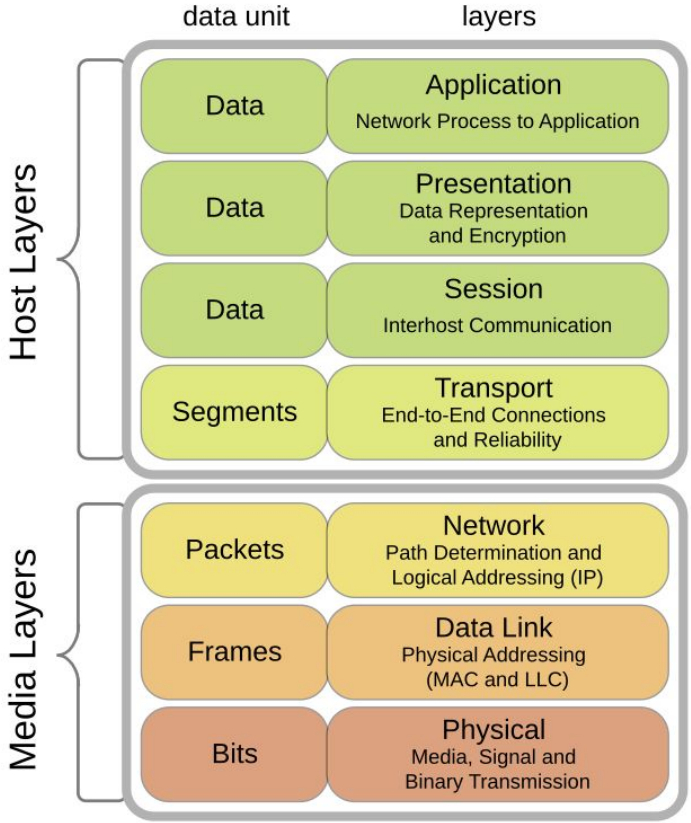


Image source: https://commons.wikimedia.org/wiki/File:OSI_Model_v2.svg

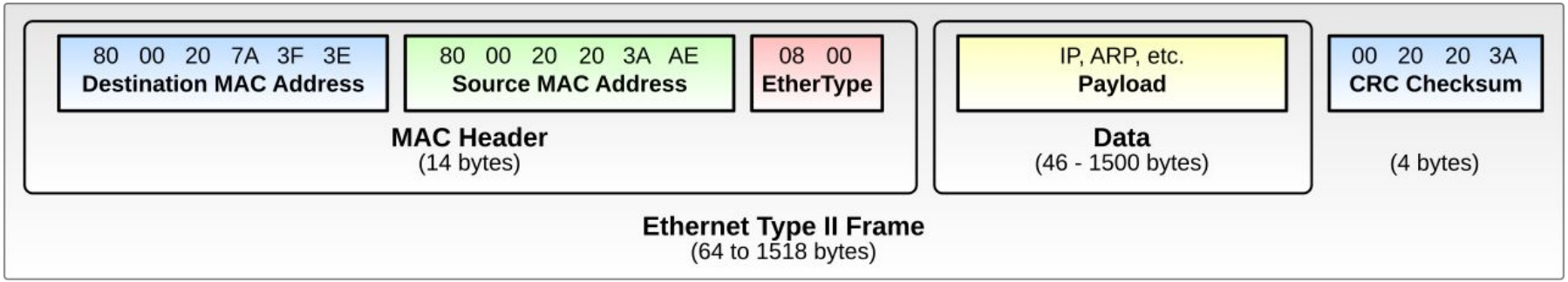
How do they work?

IEEE 802.1Q

- 802 is the IEEE’s networking standards committee
- 802.1 is the high level protocols working group
  - compare with 802.3 for wired Ethernet and 802.11 for Wifi
- 802.1Q is the standard from the 17th study group within the working group

Describes a way to encapsulate and tag Ethernet frames

Regular Ethernet frames



Source and destination addresses identify nodes

EtherType used to distinguish payload type (e.g. 0x0800 for IPv4, 0x86DD for IPv6)

Payload holds higher layer data

Image source: https://commons.wikimedia.org/wiki/File:Ethernet_Type_II_Frame_format.svg

802.1Q frames

EtherType set to 0x8100

Payload prepended with 4 bytes:

- Priority (3 bits)
- Drop eligibility (1 bit)
- VLAN ID (12 bits)
- Original EtherType (16 bits)

Checksum recalculated

Maximum frame size increased by 4 bytes

Consequences

Regular network switches only use the source and destination fields from the Ethernet frame to forward packets, so should handle VLAN packets by default.

(assuming frames aren’t too large)

Theoretically possible to support 4096 virtual networks on a network segment.

Any node can send frames with any VLAN ID, and it will be delivered to the destination node.

Tagged and untagged traffic can coexist.

VLAN Support in Linux

The `ip` command can create new VLAN devices:

```
ip link add link eth0 name eth0.100 type vlan id 100
```

All incoming traffic tagged with VLAN ID 100 will be directed to new `eth0.100` device.

All outgoing traffic on `eth0.100` device will be tagged with VLAN ID 100.

Assign IP addresses and two machines can start communicating on their new virtual Ethernet devices

systemd-networkd can help configure things more permanently

Managed and Smart Switches

Necessary to securely isolate your VLANs.

Recognise VLAN tags, and use them to make forwarding decisions.

Allow devices without 802.1Q support to participate.

Managed switch: device can be controlled from some network wide dashboard software.

Smart switch: device provides a web interface for configuration.

My own setup

TP-Link router set up with home and guest networks

- Doesn’t support 802.1Q, but can expose different networks on different ports
- so two cables connecting it to switch

Two Netgear GS308EP smart switches

Homeplug powerline Ethernet between them

Unifi APs present VLANs as two wifi networks

⇒ VLANs everywhere in the house

Advanced 802.1Q VLAN

The following lists the port members in each VLAN.

VLAN ID	*VLAN Name*	*Port Members*	
1	Default	1 3 4 5 7 8	⌄
20	Guest	2 6 7 8	⌃

EDIT DELETE

ADD VLAN

PVID Table

You may also check the PVID Table to identify or edit the PVID of each port.

VLAN ID (A numeric value between 1 - 4094)

1

The following lists the port members in each VLAN.

Port	Tag All	Untag All	Exclude All
Port 1 - Router	T	U	E
Port 2 - Router-Guest	T	U	E
Port 3 - unnamed	T	U	E
Port 4 - unnamed	T	U	E
Port 5 - unnamed	T	U	E
Port 6 - unnamed	T	U	E
Port 7 - Unifi-AP	T	U	E
Port 8 - Uplink	T	U	E

VLAN ID (A numeric value between 1 - 4094)

20

The following lists the port members in each VLAN.

Port	Tag All	Untag All	Exclude All
Port 1 - Router	T	U	E
Port 2 - Router-Guest	T	U	E
Port 3 - unnamed	T	U	E
Port 4 - unnamed	T	U	E
Port 5 - unnamed	T	U	E
Port 6 - unnamed	T	U	E
Port 7 - Unifi-AP	T	U	E
Port 8 - Uplink	T	U	E

Port and VLAN IDs

The following lists the port members in each VLAN.

Port	*VLAN(*denotes PVID)*
1 Router	1*
2 Router-Guest	20*
3 unnamed	1*
4 unnamed	1*
5 unnamed	1*
6 unnamed	20*
7 Unifi-AP	1*, 20
8 Uplink	1*, 20

Questions?

I wrote more about my setup in this blog post:

https://www.jamesh.id.au/blog/2023/08/29/unifi-guest-network/