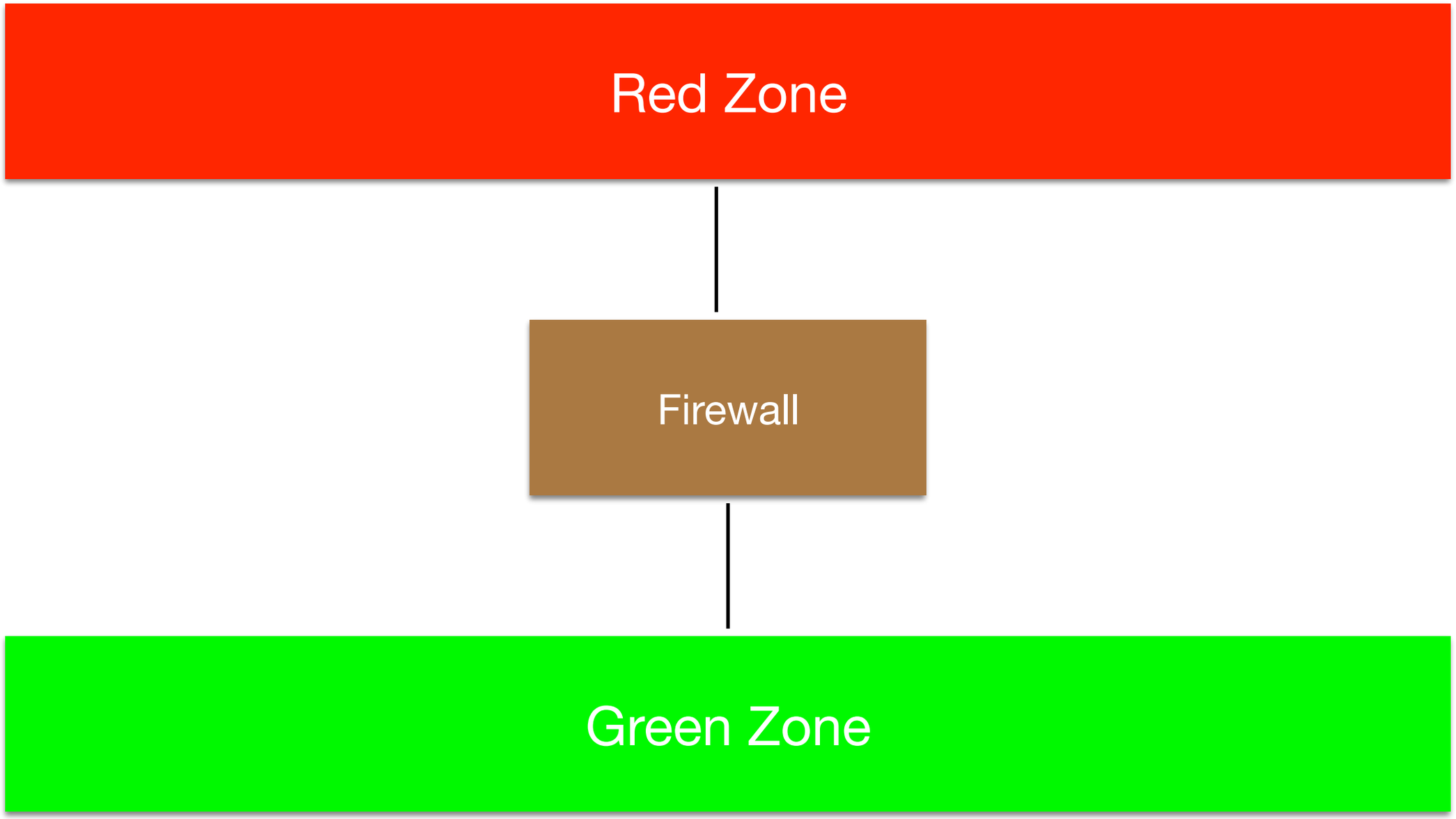
Network Security 8: Virtual Firewalling

i.g.batten@bham.ac.uk

Security Health Warning

- It is not universally true that “VLANs are insecure”
- But it is a useful rule of thumb.
- If you have a problem with a security angle and decide to use VLANs, ask someone who understands your problem, understands VLANs and understands security to look at your proposal.
- More next semester, but it is horrifyingly easy to make mistakes.
  - Throws stress on security of switches and cables.

Physical Firewalls, Physical Networks



Definitions

- Problem with word “Virtual” is that it means many different things.
- In networking, a Virtual Network is a set of tags on a physical network
- In virtualisation, a Virtual Network is a purely software construct
- Today we are talking about tags on physical networks.

VLANs on Physical Nets

- An extra “tag” inserted into the Ethernet packet format, saying which network the packet belongs to.
  - 4 extra bytes ahead of type/size fields, first 16 bits 0x8100 to unambiguously mark “this is a tag” (no real untagged packet will have 0x8100 there), 3 bits of priority, 1 bit to specify if frame is droppable, 12 bits for tag.
  - Tag 0 is equivalent to untagged, tag 1 is often used internally by switches, tag 0xFFF (4095) is reserved.
- In principle, MAC addresses only need to be unique on a per-tag basis, but relying on this will break lots of switches.

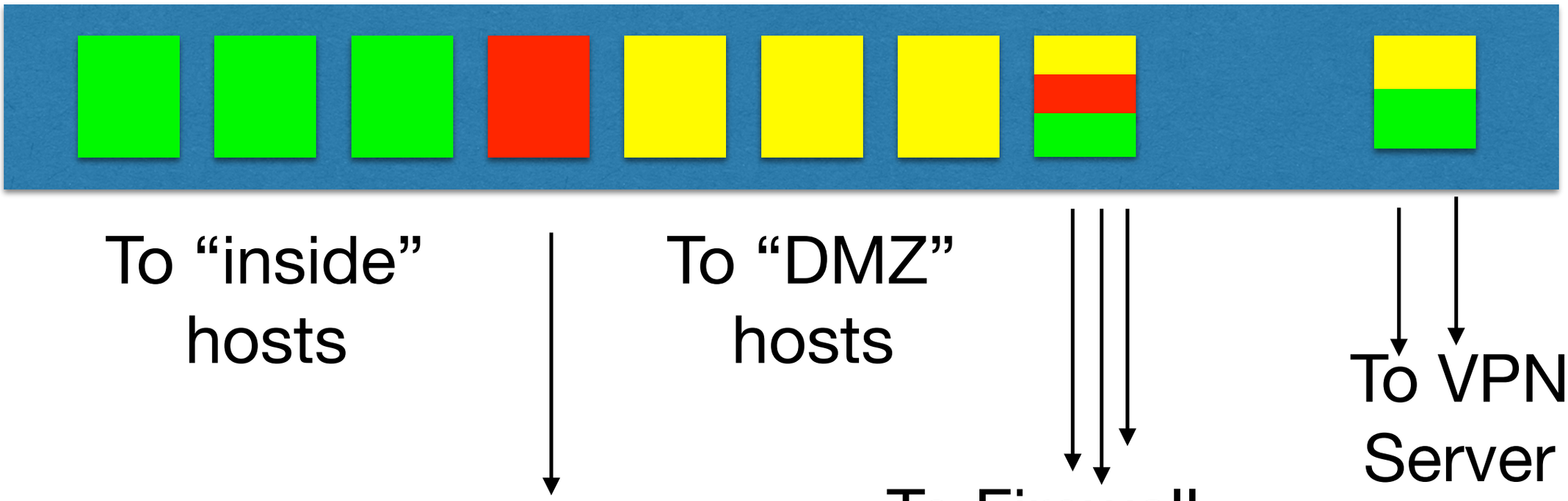
VLANS allow…

- Trunking of multiple networks along one cable
- Trunking of multiple networks through one interface
- Segregation of traffic by type, security label, etc

Common scenario

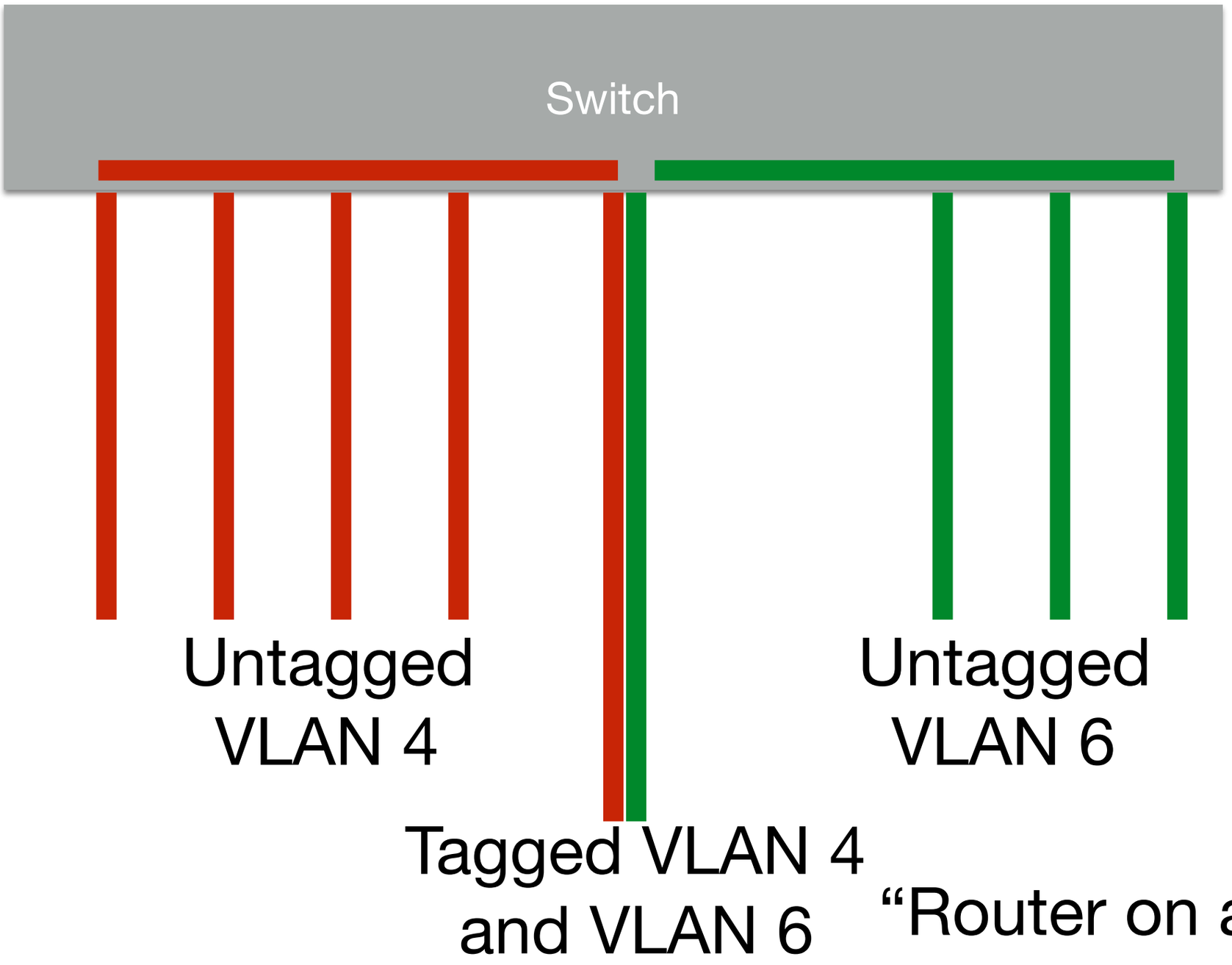
- Some ports of a switch “trunked” and carrying multiple VLANs with tagged packets, either to other switches, or VLAN-aware routers, firewalls, hosts.
- Some ports of a switch only carrying the default VLAN
- Some ports of a switch carrying a single non-default VLAN, untagged

Switch Config



LACP later!

Logically divide switches



“Router on a stick”

Port Types

- “Tagged” or (confusingly) “Trunk” ports: each packet is marked with its tag.
  - In sane networks, the global tag for its network. On enterprise kit, you can map tags on a per-port basis, but you **should not rely on this.** Assign a VLAN tag to a logical network and stick to it.
- “Untagged” or “Access” ports: some or all packets are untagged, and are assumed to be members of some default network (set on a per-port basis).

PVID

- Each switch port has a Port Virtual ID (or some similar language – vendors vary)
  - the tag assumed to be present on all untagged packets
    - the VLAN whose packets are output untagged on this port
- Confusingly, some switches require you to configure this even for access ports which only have one VLAN assigned to them (Netgear, I'm looking at you). Get this wrong and it just doesn't work.

Policing

- You can ~~if you are an idiot~~ permit packets with any and all tags on all interfaces.
- In practice, you limit the input tags to the set of VLANs you expect to see on that port.

Lots of ways to “see” VLANS

- You can get at them directly, as on (some) Linuxes:

Note MAC addresses

```
igb@pi-one:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr b8:27:eb:e1:96:51
          inet addr:10.92.213.231  Bcast:10.92.213.255  Mask:255.255.255.0
          inet6 addr: 2001:8b0:129f:a90f:ba27:ebff:fe00:efe7/64 Scope:Global
          inet6 addr: fe80::ba27:ebff:fee1:9651/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:88366 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69956 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8540091 (8.1 MiB)  TX bytes:12480470 (11.9 MiB)

eth0.5    Link encap:Ethernet  HWaddr b8:27:eb:e1:96:51
          inet addr:81.187.150.211  Bcast:81.187.150.223  Mask:255.255.255.240
          inet6 addr: 2001:8b0:129f:a90e:ba27:ebff:fe00:efe7/64 Scope:Global
          inet6 addr: fe80::ba27:ebff:fee1:9651/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27889 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3565578 (3.4 MiB)  TX bytes:5562868 (5.3 MiB)
```

“eth0” is untagged traffic

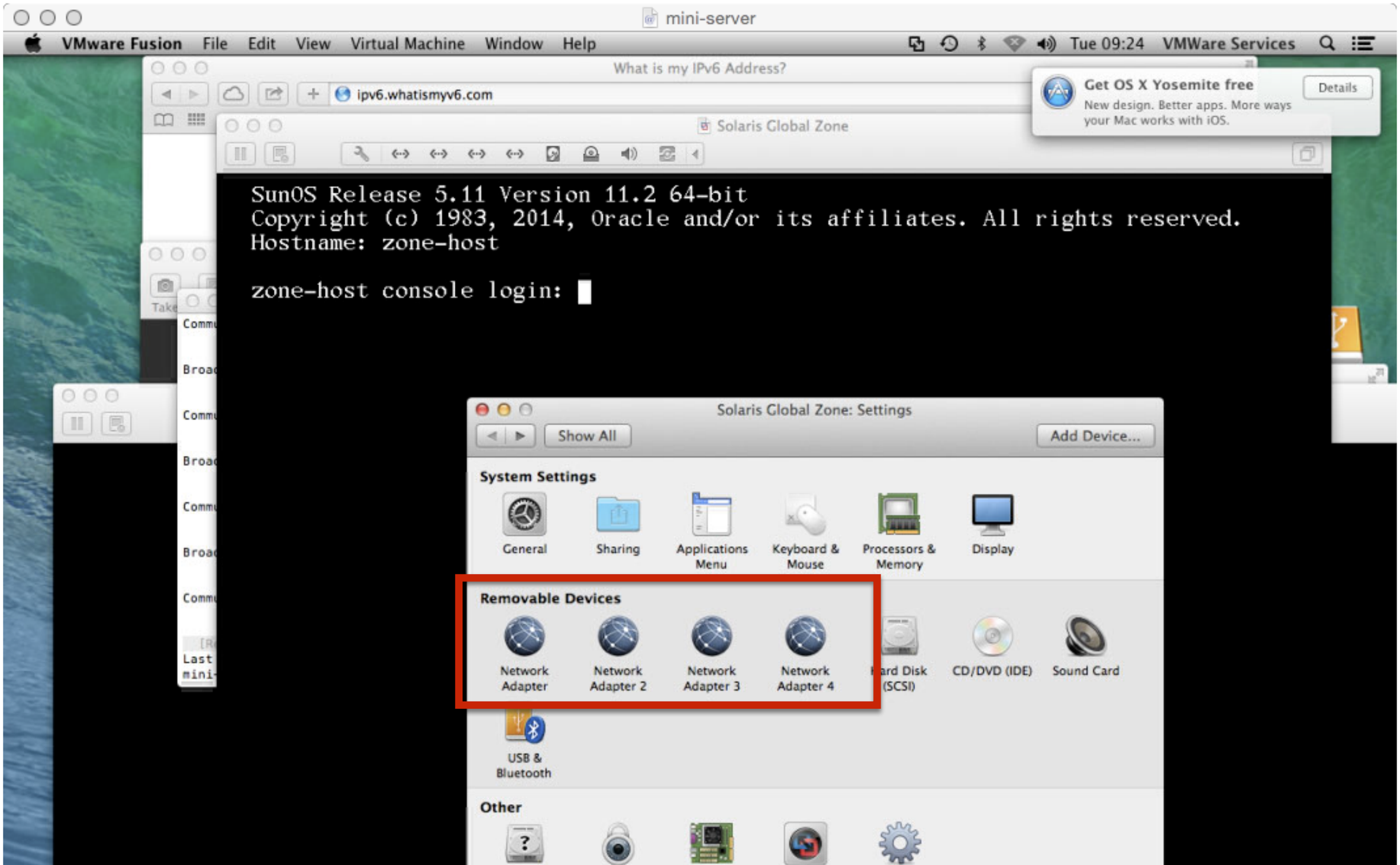
“eth0.5” is traffic using VLAN tag 5

Virtual Interface per tag

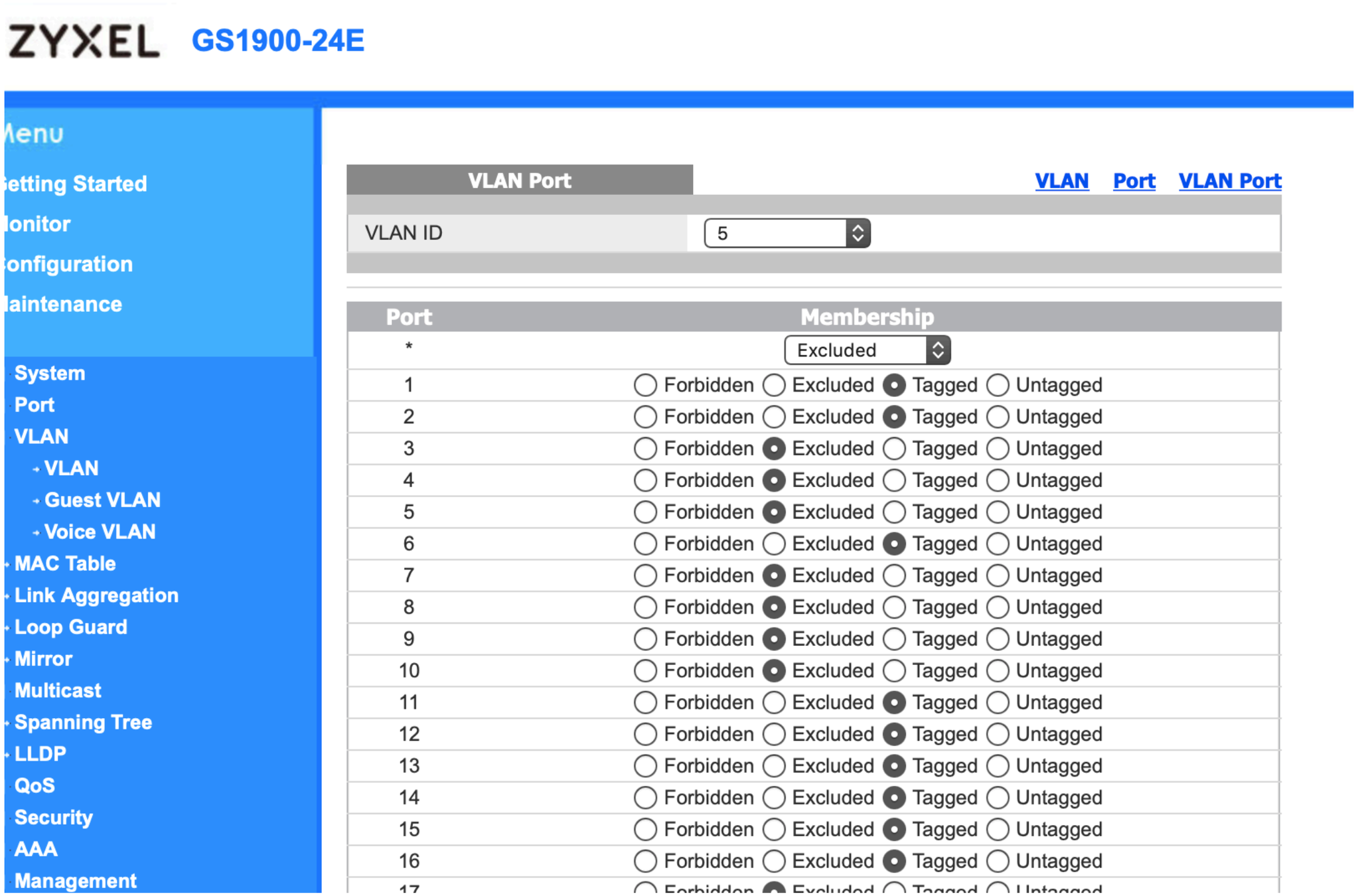
- You can see them as virtual interfaces, as on (modern) Solaris
- The physical link is the interface, then there are multiple virtual interfaces, one per tag

```
igb@research-1:~$ dladm
LINK                CLASS     MTU    STATE    OVER
net0                phys      1500   up       --
vnic6               vnic      1500   up       net0

igb@research-1:~$ dladm show-vnic vnic6
LINK                OVER              SPEED  MACADDRESS        MACADDRTYPE VIDS
vnic6               net0              1000   2:8:20:89:b5:a0   random      4008


igb@research-1:~$ ifconfig -a
net0: flags=100001000943<UP,BROADCAST,RUNNING,PROMISC,MULTICAST,IPv4,PHYSRUNNING> mtu 1500 index 2
        inet 147.188.192.246 netmask ffffff00 broadcast 147.188.192.255
vnic6: flags=120202000841<UP,RUNNING,MULTICAST,IPv6,CoS,PHYSRUNNING> mtu 1500 index 3
        inet6 fe80::8:20ff:fe89:b5a0/10
```

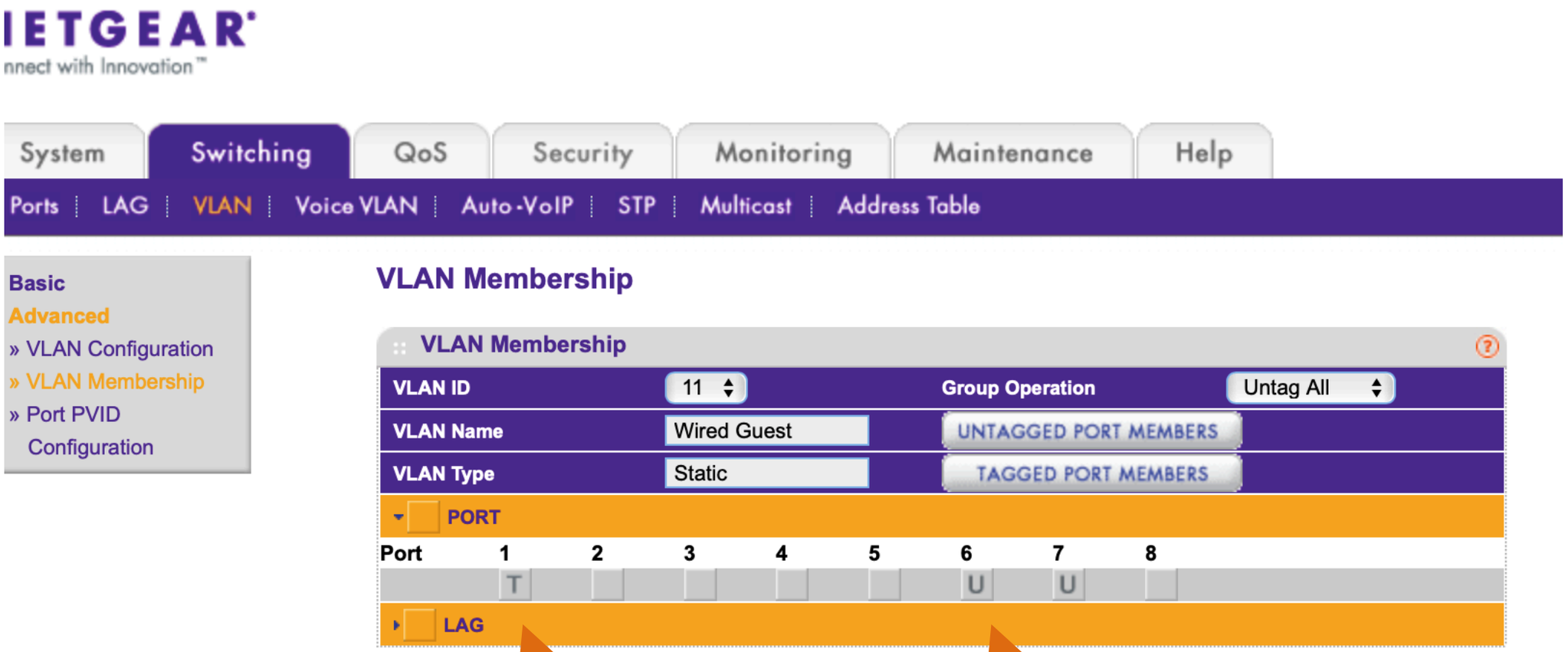
VLANs in Virtualisation



VLANs in switches



VLANs in switches



Tagged on backhaul

Untagged on 6 and 7

Tags have all been stripped

```
igb@zone-host:~$ dladm
LINK                CLASS     MTU    STATE    OVER
net1                phys      1500   unknown  --
net0                phys      1500   up       --
net2                phys      1500   up       --
ossec/net2          phys      1500   up       --
net3                phys      1500   up       --
ossec/net3          phys      1500   up       --
ossec/net0          vnic      1500   up       net0
igb@zone-host:~$
```

Good uses for VLANs

- Reducing the number of physical cables and interfaces used between a switch and a firewall
- Reducing the number of physical switches (you can use different tags with only access ports to split a single switch between disjoint networks, getting economies of scale)
- Bringing multiple networks into machines with insufficient physical interfaces (general case of firewall).

VLANs for segregation of management

- Telecoms practice divides hardware into three “planes”. It’s not common as a distinction in IT, but it’s a useful abstraction.
  - Management
  - Control
  - Data

Data Plane

- The actual switching of data, at speed and scale. Equivalent to the ethernet ports on an ethernet switch.

Control Plane

- Setting up calls, determining routes, and other less frequent, potentially higher impact, but usually automatic tasks
- Doesn’t always have a direct IT equivalent, but routing protocols like OSPF and BGP would fall into this category.
  - Not TCP SYN SYN/ACK ACK

Management Plane

- Reconfiguration of devices by manual action or by action of higher-level management systems
- Has ability to reroute traffic, shut down or reconfigure interfaces, etc, etc.
- Real telecoms equipment does not allow “in-band management” — you cannot cross to the management plane from the data plane.

Building a Management Plane

- Some very high-end, specialised equipment does have a separate management port, through which the equipment can be managed.
- It's rare for that port to be the **only** way to manage the device, and running separate cabling is a pain
- With care, you can use VLANs to get much of the benefit

Management VLAN

- Only listen for management traffic on one particular VLAN: packets for management must have that tag
- Why doesn’t this work without more care?

VLANs are insecure

- Anyone can put any tag on any packet
- VITAL that you police tags where they enter “trusted” (roughly, physically secure) parts of your network, by stripping tags that are not expected from edge ports

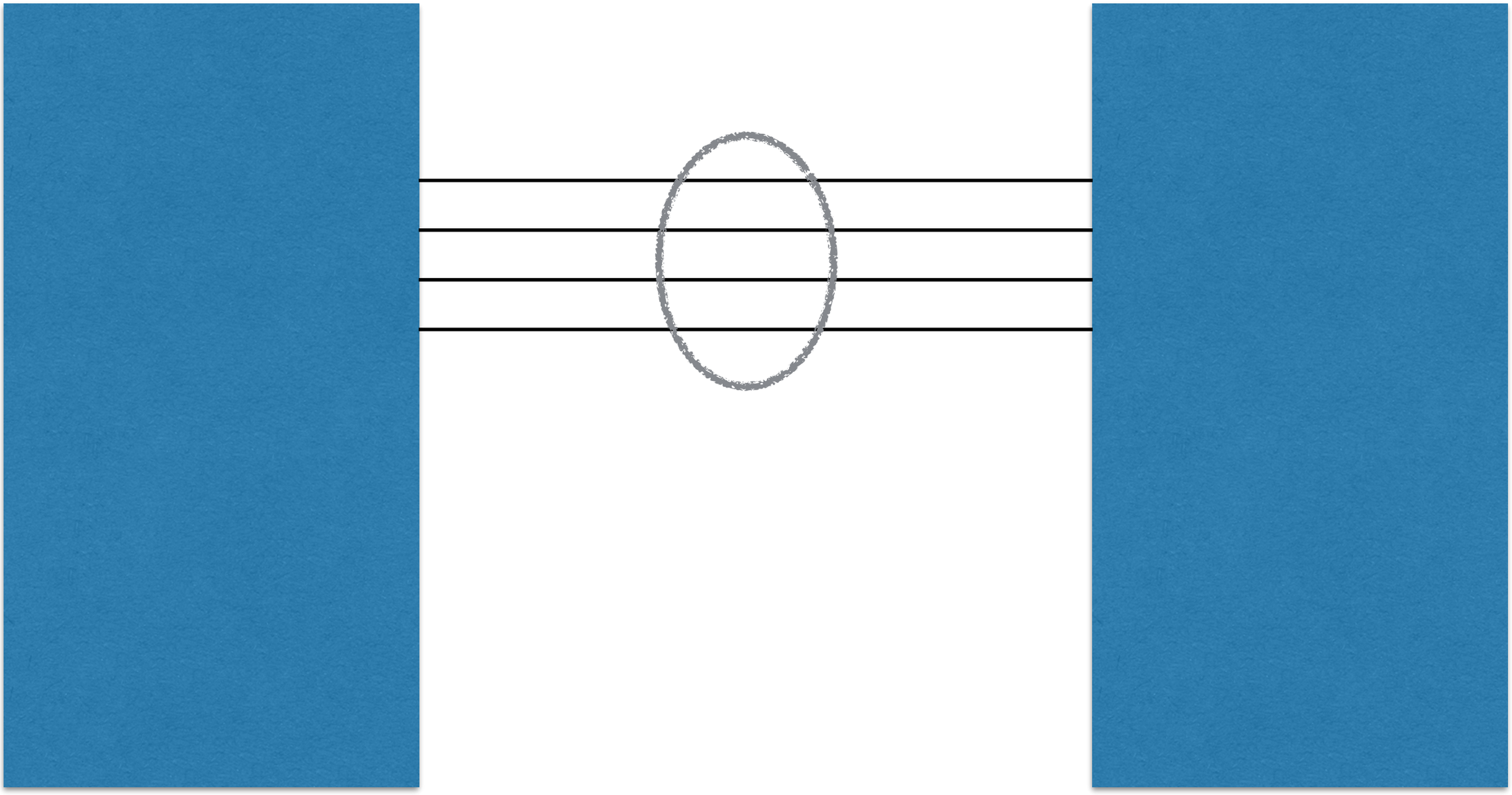
802.1x might have a role

- There are various dynamic solutions which allow you to configure switch ports based on MAC addresses, authentication material and so on.
- They are messy and tricky to get right (see previous discussion on 802.1x) but the alternatives can be messy as well.
- Planning a VLAN infrastructure requires a lot of thought.
- If I had my time again, I would not use default VLAN, and would tag **everything** except on access ports.
  - Usually you aren’t starting from a green field, and no-one uses VLAN tagging on their first switch.

Link-Agg

- If switch supports it, you can put interfaces into a Link Aggregation group, controlled with LACP, Link Aggregation Control Protocol
  - Confusingly, sometimes called “trunking”. Also “bonding”, “channel bonding”, etc.
- Appears to operating system or switch as one “**logical**” interface, one IP number, one entry in routing table, etc.
- Packets divided by round-robin, header hash or some other mechanism.
- Modern solution for performance and availability
  - Failure detection much faster and simpler
  - Fancy equipment lets you link-agg to multiple switches, or at least multiple independent cards in same switch

Link Agg



Link-Agg + VLANs

- You can deliver two or more networks over two or more cables, with full load balancing and failover
- Aggregate using Link Aggregation
- Then apply VLAN tagging for the separate networks
- Not enough people do this: it is very, very effective

Link Agg plus VLAN