Network Access Control and PacketFence

Network Startup Resource Center

What is Network Access Control?

- Requiring users to authenticate before being allowed onto the network
- Establishing a strong link between user identity and network location (physical port, IP address)
- Creates accountability for network users
- Prevents access by unauthorized users

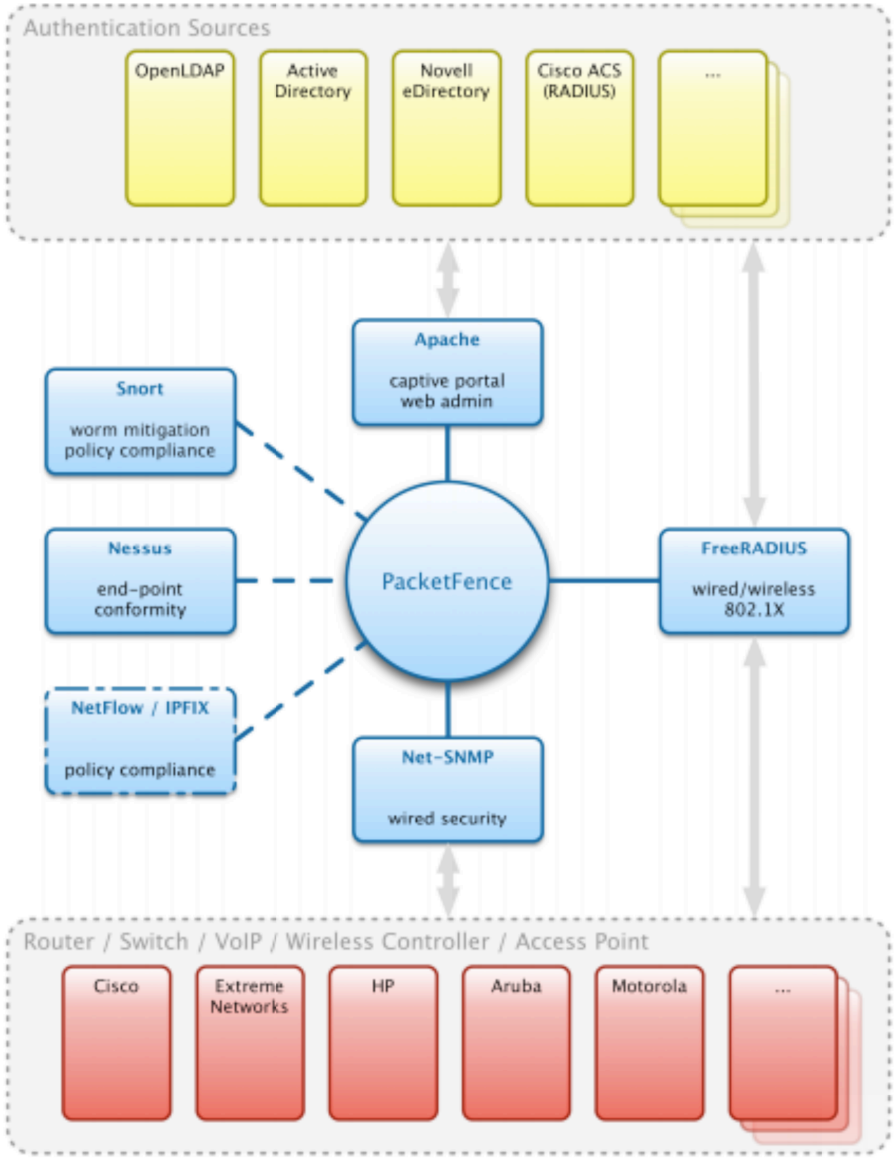
Wireless NAC

- Captive portal (typical hotspot)
  - Browser login required for each session
- WPA Enterprise (WPA 802.1x)
  - Now widely supported by clients
  - Credentials stored in client device
  - In simplest mode (PEAP), client sends a username + password, validated by RADIUS server
- WPA Enterprise becoming the preferred option

Wired NAC

- 802.1x can be used on managed switches too
- Needs special software ("supplicant") on the client, and 802.1x to be configured on the client
  - Client cannot download the software or instructions if their network port is blocked!
- A captive portal solution is more user-friendly
- But you want to avoid funnelling all your network traffic through an in-line box

PacketFence



User authentication database

PacketFence

Edge switches / APs

PacketFence features

- Captive portal
- 802.1x authentication (wireless and wired)
- Dynamic configuration of switch ports
- Act on SNMP traps (e.g. port unplugged)
- Choice of user authentication databases
- Free and open source
  - Perl scripts, readily hackable
  - Commercial support available

Snort/Suricata integration

- Infected or misbehaving machines can be automatically dropped into "isolation VLAN"
- Customized portal page depending on what the problem is
  - e.g. virus detected, bittorrent detected
- Gives user a chance to fix the problem (remediation) and then click to get back onto the main network

Quarantine Established!

Malware Found: Your system has been found to be infected with malware. Due to the threat this infection poses for other systems on the network, network connectivity has been disabled until corrective action is taken.

1. Run an complete antivirus scan
2. Always make sure your system is fully up to date regarding security patches

Re-enabling Your Network Access

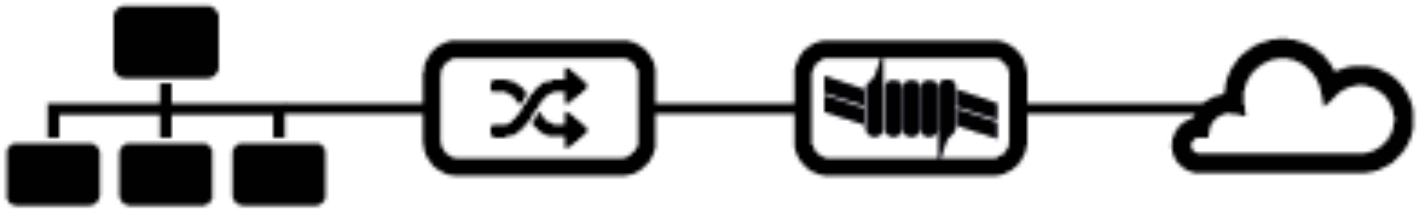
Clicking the *Enable Network* button below will re-enable your network access. Make sure to follow the instructions listed above to correct the issue. Failure to do so will result in network access again being disabled. Repeated failures will result in access being disabled permanently.

help: provide info

- IP: 10.0.0.123
- MAC: c8:bc:c8:ce:65:e1

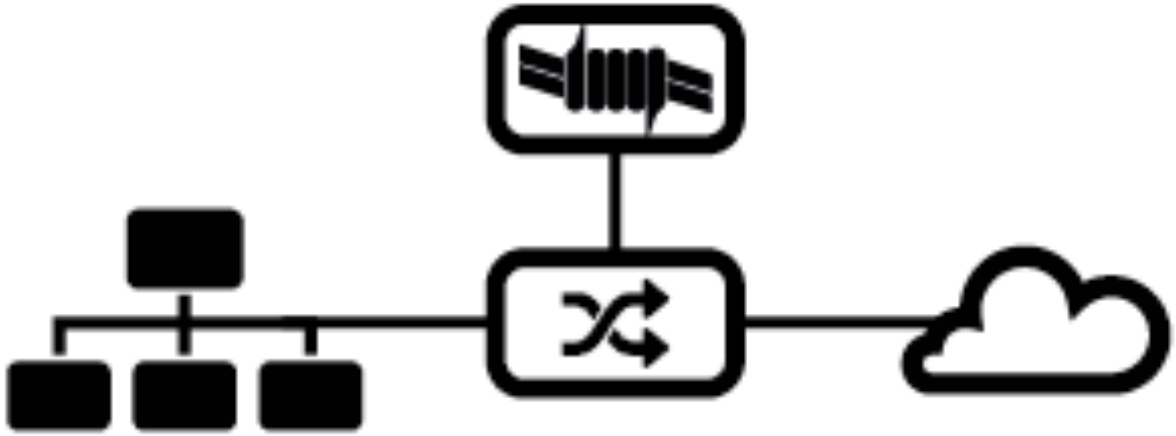
Inline enforcement mode

- PacketFence box acts as network gateway
- Works with dumb (unmanaged) edge switches
- PF adds iptables (ipset) rules to control clients
- All traffic funnelled through PF box; does not scale to large networks



VLAN enforcement mode

- Modifies the switch config in real time to configure access ports



VLAN enforcement mode

- Initially configures port to "MAC detection VLAN"
  - To learn MAC address of connected device
- If MAC is not already registered, move to "registration VLAN"
  - PacketFence is DHCP server and DNS server
  - Forces users to registration page
- After authentication, change to "default VLAN"
- If anomalies seen, change to "isolation VLAN" and display appropriate captive portal page

VLAN enforcement mode

- Return port to registration VLAN on:
  - change of active MAC address
  - timeout (e.g. after one week)
- Requires managed switches at edge
  - Several different types supported
- PacketFence is **out-of-line** on data VLAN!
  - Does not hamper throughput, scales really well

Detection of (new) MAC address

- Several different methods supported
  - Some switches have "security trap"
    - one MAC allowed, send trap if a different one seen
  - Some switches send a bridge table learning trap
  - Otherwise just use port up/down traps and poll for the MAC address when device is connected

http://www.packetfence.org/about/technical_introduction.html

PacketFence and wireless

- Includes FreeRADIUS and 802.1x
- Dropping clients into isolation VLAN requires AP feature "dynamic VLAN assignment" via RADIUS
  - Unifi firmware does not support this yet :-(
  - OpenWrt does
- Same authentication backend for wired and wireless access

PacketFence requirements

- Supported Linux OSes
  - CentOS/RedHat 6 (used to be only option)
  - Debian 7 (Wheezy)
  - Ubuntu 12.04 LTS
- 4GB RAM
- 100GB disk (RAID-1 recommended)
- 1 NIC (+1 for IDS, +1 for high availability)

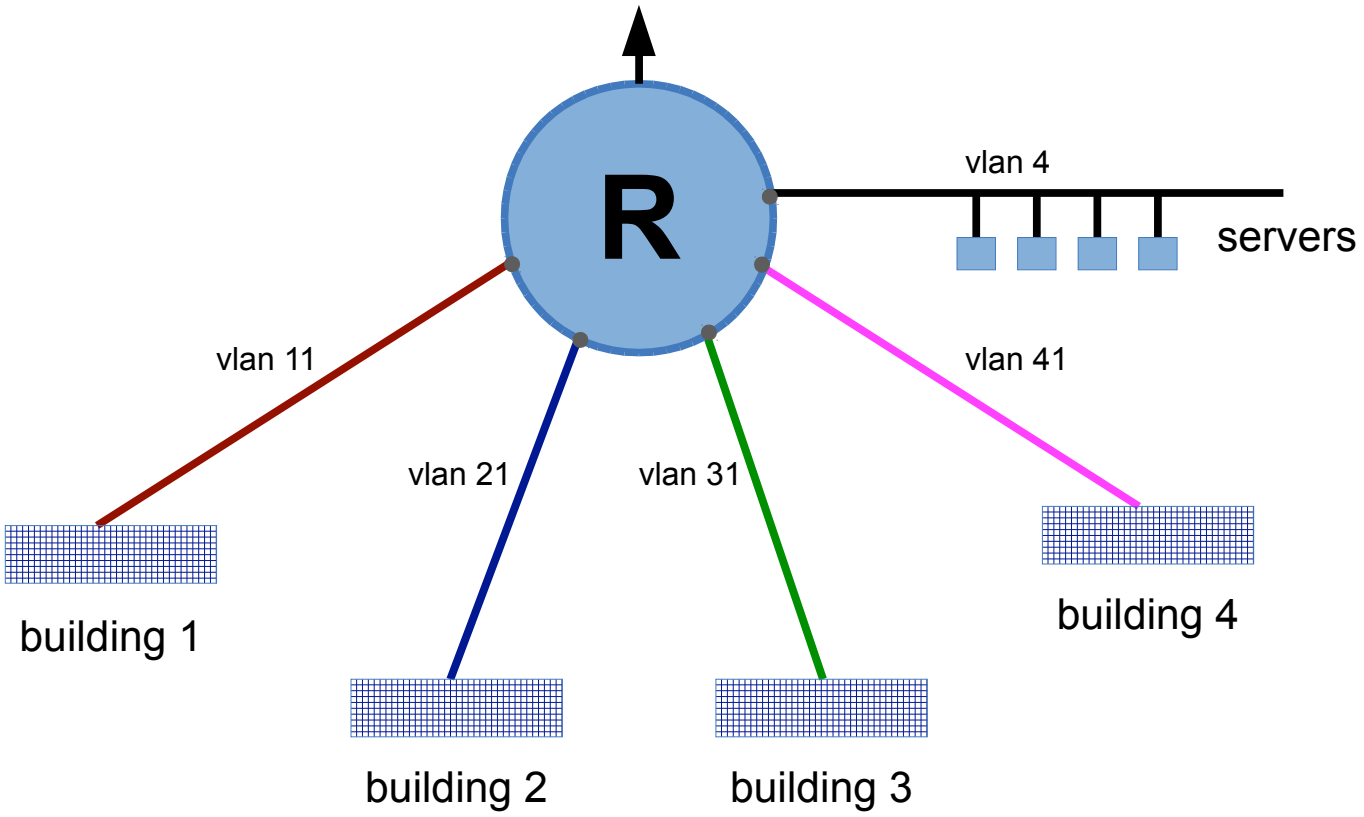
Designing for PacketFence

PacketFence in Campus Network

- Campus networks route at the core
  - Provide building isolation and scalability
  - Don't span VLANs between core ports!
- Don't break this when deploying PacketFence
- Needs a degree of planning

Ideal routed campus network

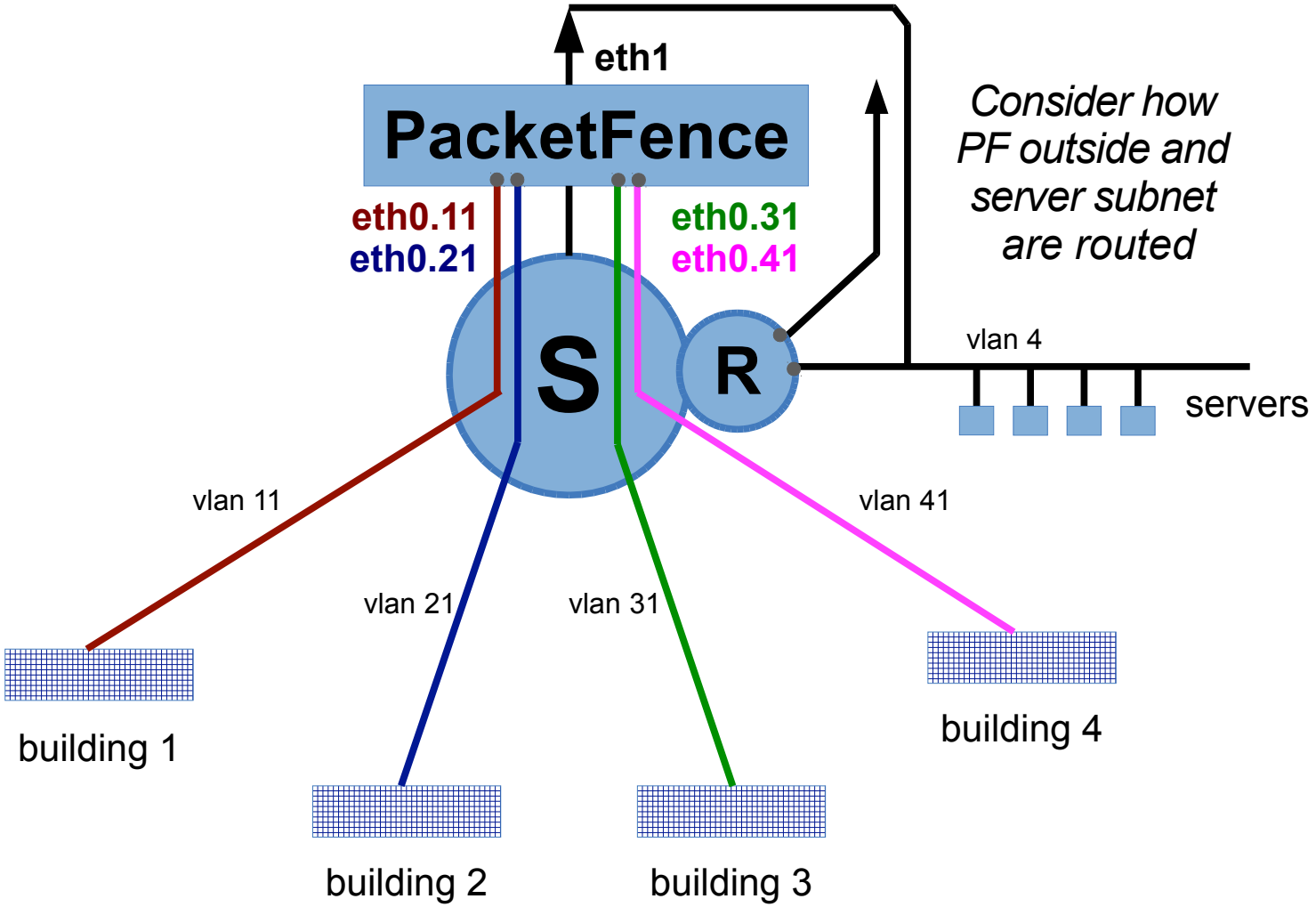
- Separate subnet per building



Inline enforcement (less preferred)

- Don't span the inline VLAN!
- Create a separate inline VLAN per building
- Trunk them through to the PacketFence box
- This means the core device is now switching not routing
- NOT IDEAL but may be the only option with dumb edge switches

Inline enforcement



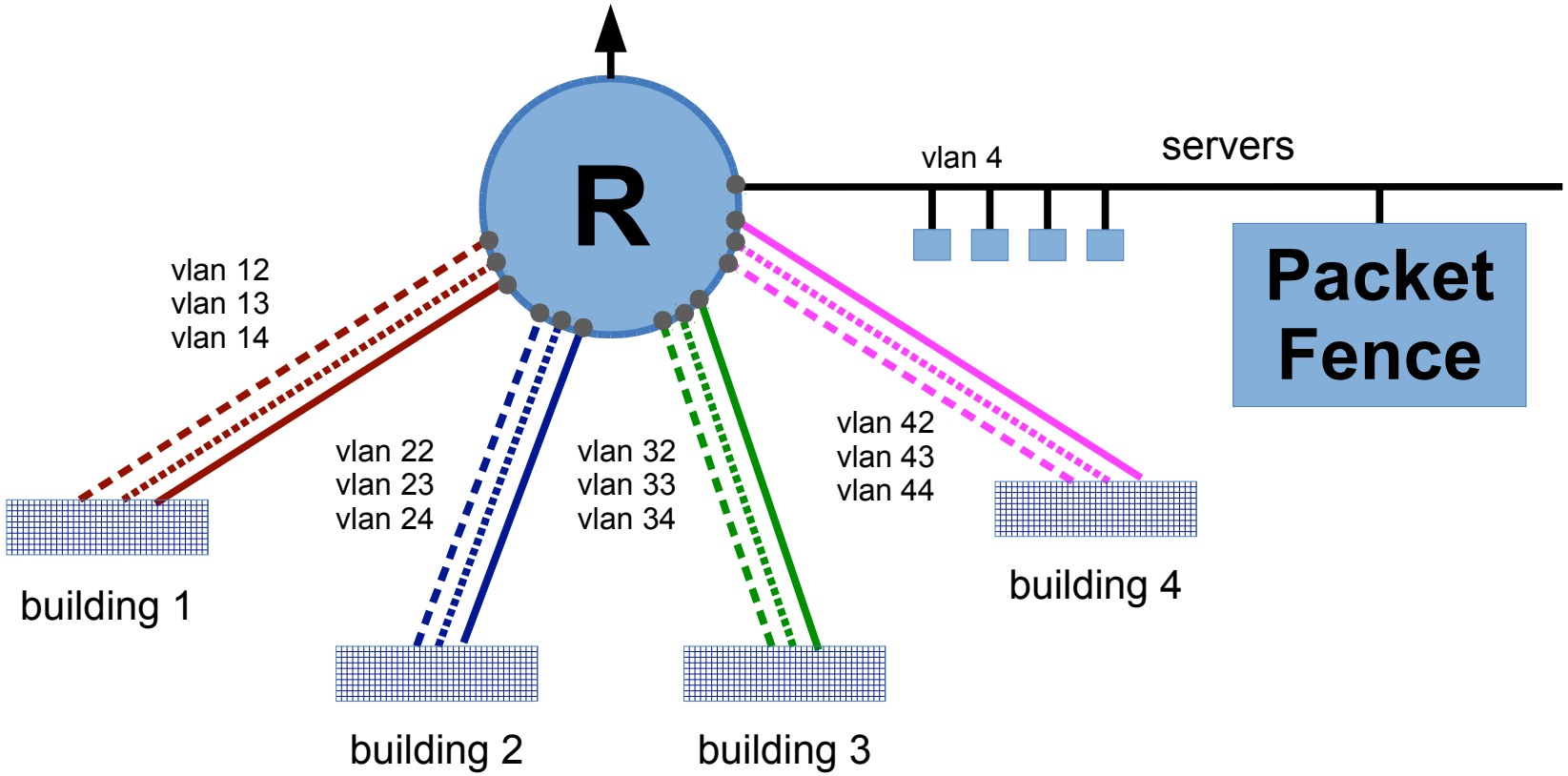
Inline enforcement

- PacketFence becomes a one-legged router
- PacketFence is choke point and SPOF
- PacketFence does not (yet) support IPv6 for inline enforcement
- Core network device may be switching on some VLANs and routing on others

VLAN Enforcement (preferred)

- Each building needs:
  - its own data VLAN (standard campus design)
  - its own registration and isolation VLANs
- PacketFence sits on the server network and is out-of-line

VLAN Enforcement



VLAN Enforcement

- PF is DHCP server for reg and isol VLANs
  - DHCP helper needs to point to PF server
- Set ACL on reg/isol VLANs which blocks all traffic except to/from the PF server
- If your edge switches can do layer 3 ACLs so much the better (a.k.a. "vlan-isolation")
  - blocks peer-to-peer traffic on the VLAN
  - on isolation VLAN, helps prevent infected machines infecting each other

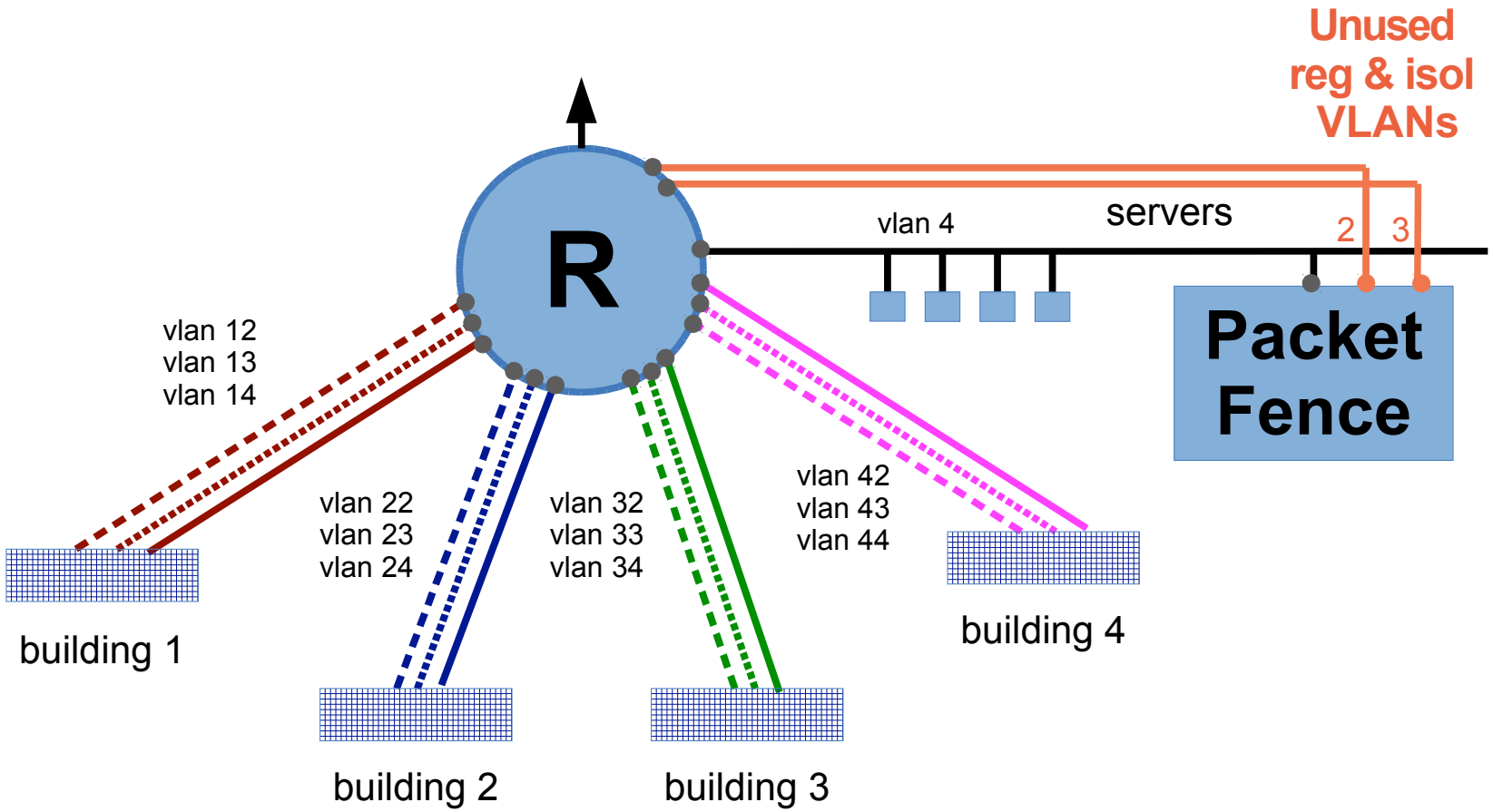
VLAN Enforcement

- PacketFence is configured with the management IP of each managed switch
- For each switch, told which VLANs to use for reg/isol/data
- Configured *not* to manage trunk ports (i.e. switch to switch links, and ports with dumb switches downstream)
  - PF calls them "uplink ports"

Configuration note

- Web configurator will force you to create registration and isolation interfaces *on the PacketFence server itself* - even though you won't use them
  - (Perhaps they expect you will span them across the campus? No thank you!)
- These interface IPs can still be the targets for DHCP helper and DNS from your reg/isol nets

VLAN Enforcement



Both inline and VLAN enforcement

- If you have some managed switches and some dumb switches
- Building aggregation switch needs to be VLAN-capable
- Downstream dumb switches configured on access ports on the *inline* VLAN
- Four VLANs per building - complicated :-)
  - Oh, and PacketFence supports VOIP VLANs too

Possible VLAN / addressing plan

- Lots of VLANs, so make a repeatable and consistent scheme
- Following page is just a suggestion
- Feel free to adapt, drop the bits you don't need, or just make your own
- For IPv6, you can just put the VLAN ID as the fourth word
  - pr:ef:ix:**vlanid**::/64

Plan for building X

- Allocate a /20 for each building, e.g. 10.90.0/20

```
Vlan xx0    10.90.0.0/24    Spare
Vlan xx1    10.90.1.0/24    Wired Inline
Vlan xx2    10.90.2.0/24    Registration
Vlan xx3    10.90.3.0/24    Isolation
Vlan xx4    10.90.4.0/24    Wired Data Managed
Vlan xx5    10.90.5.0/24    Spare
Vlan xx6    10.90.6.0/24    Spare
Vlan xx7    10.90.7.0/24    Spare
Vlan xx8    10.90.8.0/22    Wireless Routed (802.1x)
Vlan xx9    10.90.12.0/22   Wireless Inline
```

(Building 0 = NOC/server room. Generate configs for your network devices using a script)

MAC detection

- The MAC detection VLAN should be completely isolated
- You can use the same VLAN ID everywhere (e.g. VLAN 4000) but don't enable it on any trunk ports

DHCP notes

- PacketFence is the DHCP server for the registration and isolation VLANs
- Keep your existing DHCP for live subnets
- PacketFence will also keep track of the live IP addresses assigned to users
- Add PF's management IP address as the last "ip helper-address" on each live subnet
  - pfdhcplistener process will pick it up

Other considerations

- Maybe not all networks need to be PF controlled
  - Dorms only? Not staff offices?
  - Shared PC labs better to have domain logins?
- VLAN enforcement scales better and is easier to roll out incrementally
- Upgrade your edge switches to managed!
  - and check the model you buy is supported by PF