Advanced Networking and Wireless

Benjamin Brewster

Why You Need to Care

- Because someday you'll have to:
  - Design and deploy a network for your business or home
  - Set up a nested router situation, where separate routers control different networks
  - Deploy WAPs in a complicated or already-congested building
  - Set up a VPN that encrypts traffic
- No hands-on, follow-along-with-me stuff today

Firewalls

- Firewalls protect your data and your services
- Note that firewalls don't/can't interfere with traffic that isn't hitting them - so traffic solely through unmanaged switches never hits the firewall!
- This is forgotten more often than you might think in network design

Firewalls

- The term "firewall" can mean many things, but it usually means a device that processes packets.
- Processing could mean allowing the packet through, allowing the packet through with modifications, or denying (dropping) the packet

- Some devices scan the *contents* of those packets, not just the address information in the header
  - So-called Deep Packet Inspection means that the firewall can look for registered virus binaries, forbidden keywords, spam, etc. inside the packets

Firewalls

- Some network devices can be programmed to be anything: router, switch, DHCP/DNS/other server, VPN end-point, firewall, etc.,
- Confusingly, the device could be *called* any of these

- This is typical in big-name boxes
  - Cisco
  - Juniper
  - Watchguard
  - HP
  - Dell
  - pfSense (company name is netgate)

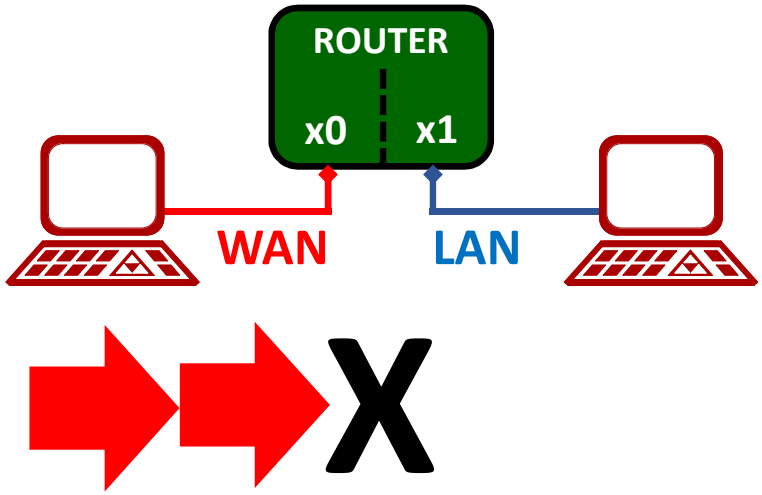
Firewall Technologies

- Two technologies are usually used together to authorize packets through and point them to the correct place:
  - Firewall Rules
  - Network Address Translation (NAT)

- These technologies can be operated on schedules and can shape traffic/provide Quality of Service (QoS)
  - e.g. From 9am to 5pm, prioritize video chat and downloads, from 5pm to 9am, prioritize gaming traffic above all else

Firewalls

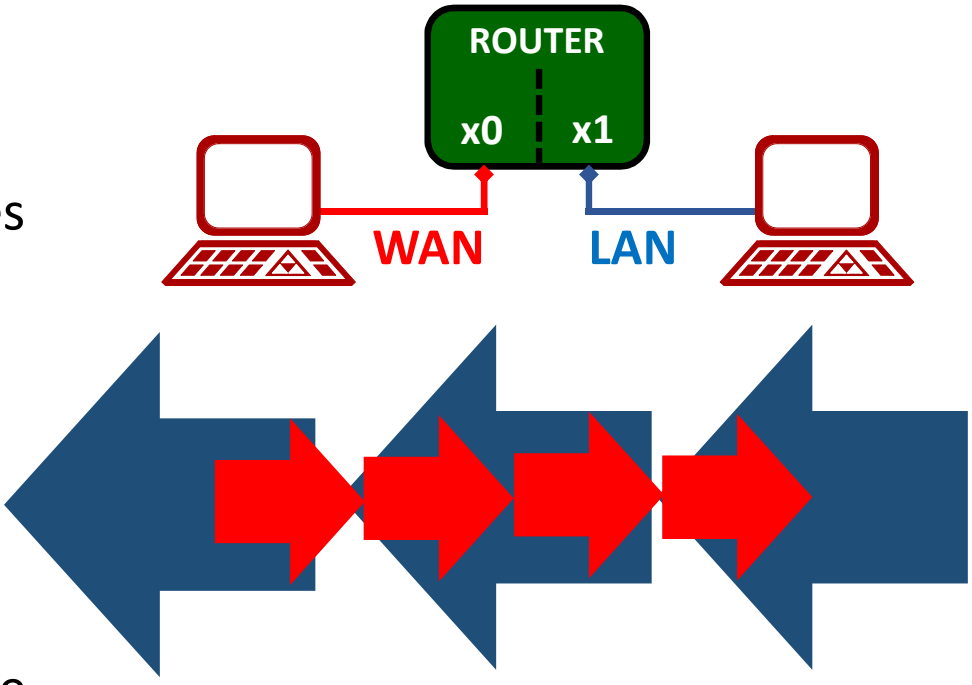
- NAT allows port-forwarding for incoming connections
- Recall that unless a **LAN** device makes a connection outbound *first*, **WAN** devices do not know where to find **LAN** devices (i.e. which port to use)
- Incoming traffic addressed to unregistered/unused ports is normally blocked by Firewall Rules
- NAT rules allow **WAN** devices to make first-contact with **LAN** devices



Initiating connection from WAN is blocked by Firewall Rules, as an open port wasn't targeted

Firewalls

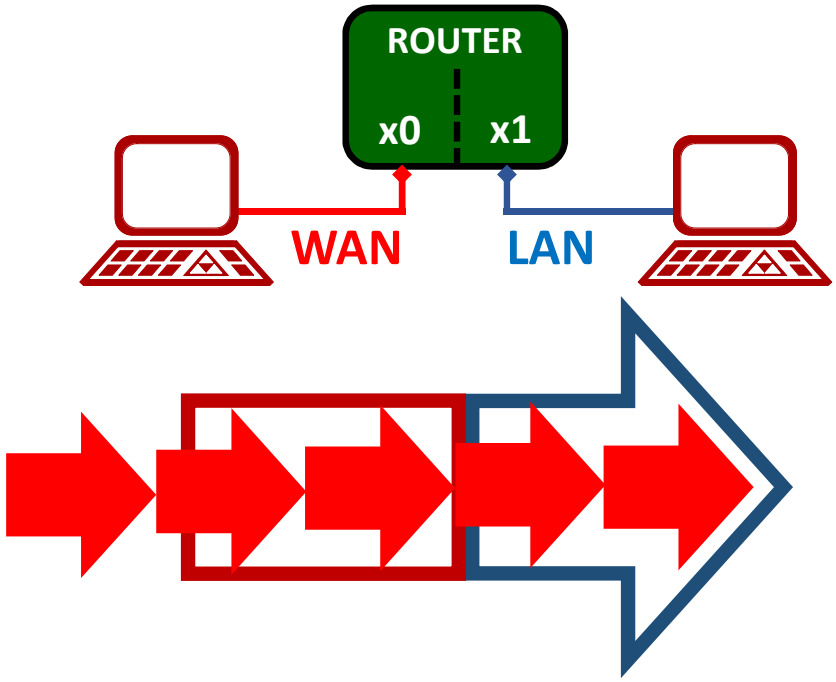
- NAT allows port-forwarding for incoming connections
- Recall that unless a **LAN** device makes a connection outbound *first*, **WAN** devices do not know where to find **LAN** devices (i.e. which port to use)
- Incoming traffic addressed to unregistered/unused ports is normally blocked by Firewall Rules
- NAT rules allow **WAN** devices to make first-contact with **LAN** devices



Outbound connection from LAN device creates NAT mapping so that traffic back from WAN can find target LAN device

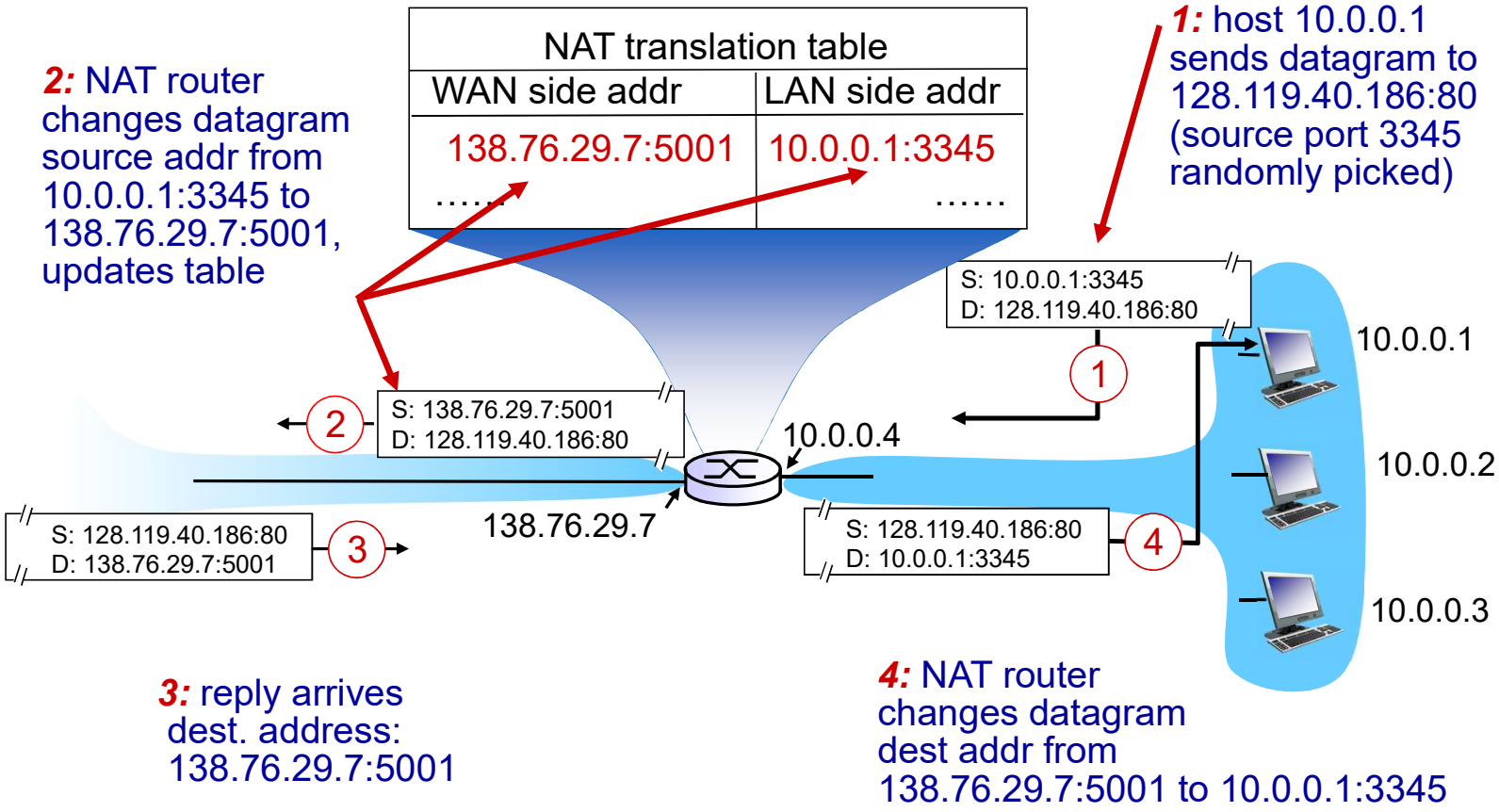
Firewalls

- NAT allows port-forwarding for incoming connections
- Recall that unless a **LAN** device makes a connection outbound *first*, **WAN** devices do not know where to find **LAN** devices (i.e. which port to use)
- Incoming traffic addressed to unregistered/unused ports is normally blocked by Firewall Rules
- NAT rules allow **WAN** devices to make first-contact with **LAN** devices



Port-forwarding NAT rule provides pathway for originating WAN connections to target a pre-determined LAN device

NAT example from networking class



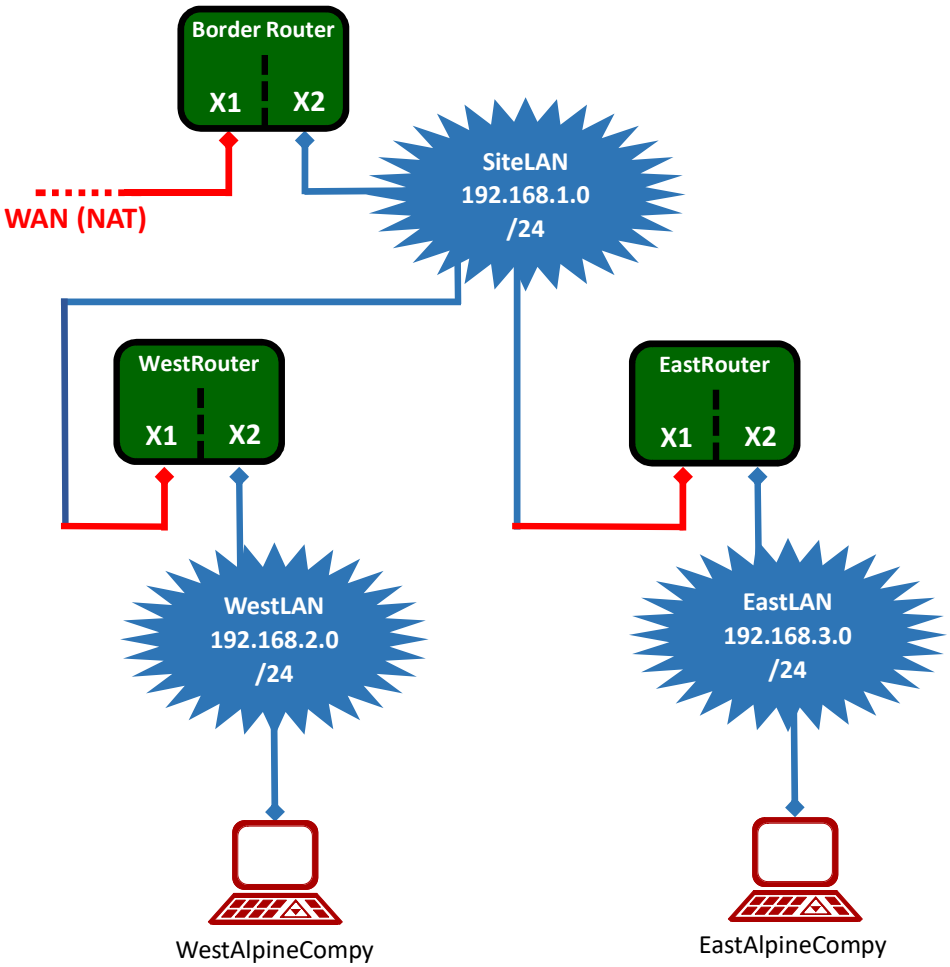
NAT Justified

- Why NAT?
  - Out of IP addresses for LAN devices to all have unique ones
  - To hide internal devices and provide some obfuscation of them

- If you don't need those (for example you're already inside a NAT router's control), you don't need NAT

Our Advanced Lab Network

- A border router, and two internal routers
- All on separate, private subnets
- Note that NAT is enabled on the internal routers, yet is unnecessary
- This is common in practice because it's the default configuration!



pfSense as Border Router/Firewall

Say

- Let's look at some of the features of the Firewall in pfSense

Demonstrate

- Boot:
  - Lab5_BorderRouter
  - Lab5_WestRouter
  - Lab5_EastRouter
  - Lab5_WestAlpineCompy
  - Lab5_EastAlpineCompy
  - CentOS GUI Reference VM, on "SiteLAN" Internal Network

- Firewall rules are processed from top to bottom
- Note how no Allow rules are present, and there are even explicit blocks in place to prevent private and bogon networks
- Note how everything is allowed on the LAN

- With Firefox, connect to Lab5_BorderRouter at 192.168.1.1
  - u: admin; p: password
- Click on Firewall -> Rules -> WAN
- Click on Firewall -> Rules -> LAN

What Devices Are Connected?

Say

- As we look at more complicated connection scenarios, we need to know what is connected to our border router
- This list shows when they connected, what their address is, and what their hostname is.
- All DHCP servers have this feature!
- One common desire is to have a server, computer, or other device always have the same IP address. Problem is, if you set it statically on the device, then it can't be plugged in anywhere: it'll just not work on other networks
- Instead of this, you can give it a static mapping, so that whenever its MAC address shows up, it gets the same IP address, and yet always to get one wherever it plugs in. You can also thus manage its DHCP settings from the DHCP server, instead of the box

Demonstrate

- Click on Status -> DHCP Leases
- To do this, you would click the "Add static mapping" button in the Actions list in the row of the VM device you want to set
- Show the static leases for this router at the bottom, and on the Services -> DHCP Server page

pfSense as Internal Router/Firewall

Say

- Now let's connect to the West Router
- Reset the networking state so that it picks up a DHCP address from the West Router
- Firewall rules are processed from top to bottom
- Note that packets from so-called private networks (192.168.X, 10.X, etc.) are usually dropped by default. For this example, since we're going to be nesting routers with private networks, I've removed this rule from this firewall
- Note that I've added an accept ICMP rule to the WAN, so we can ping the router from the WAN, and we can SSH to this router from the WAN
- Any incoming packets that don't match *any* of these rules are dropped; this is typical behavior: rulesets are usually ordered whitelists

Demonstrate

- Switch the Internal Network of the CentOS GUI VM to be "WestLAN"
- `$ sudo systemctl restart network.service`
- With Firefox, connect to Lab5_WestRouter at 192.168.2.1
- Click on Firefox -> Rules -> WAN

pfSense as Internal Router/Firewall

Say

- Note no changes to the LAN: anything still goes!

Demonstrate

- Click on Firewall -> Rules -> LAN

pfSense as Internal Router/Firewall

Say

- See how the port-forward is set up as part of NAT: this allows us to ssh to either the router OR a machine inside the firewall
- I chose to set port 2222 as the port that WAN devices could target the internal WestAlpineCompy at with SSH connections
- Such packets will be translated such that their destinations will be rewritten as the static IP'd WestAlpineCompy, with the port re-written as 22, which is where WestAlpineCompy is listening for SSH connections

Demonstrate

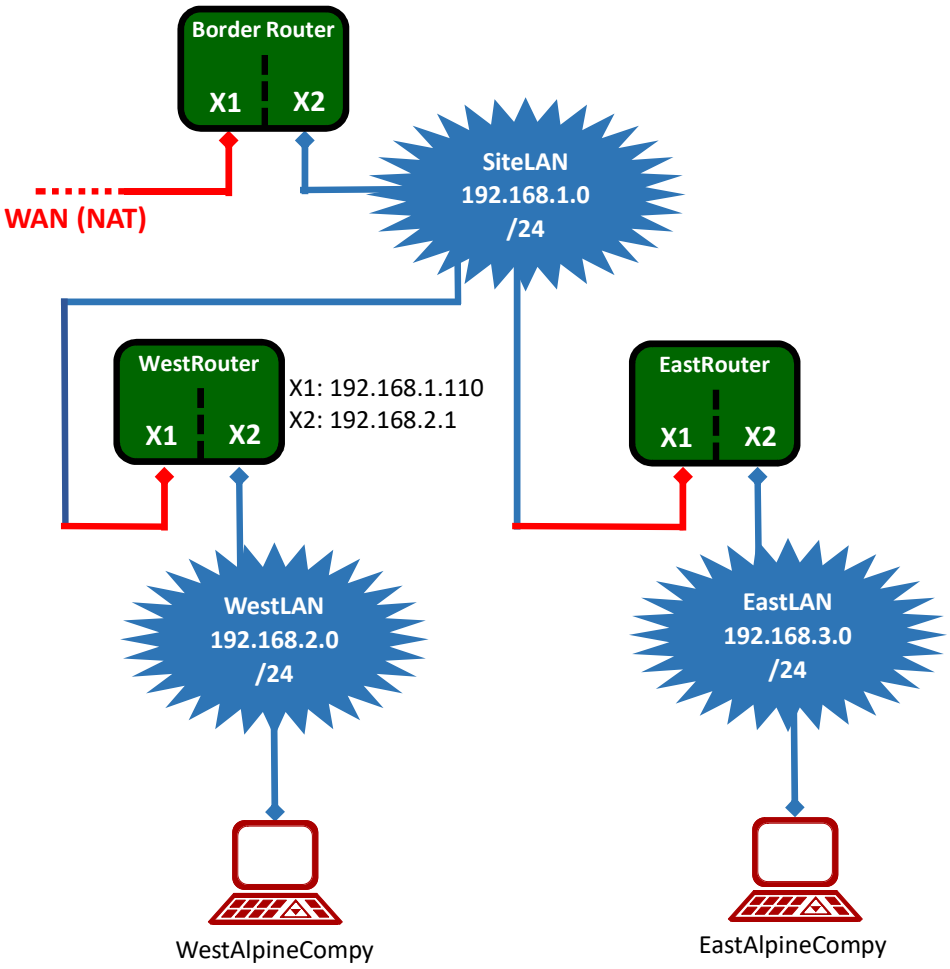
- Click on Firewall -> NAT

- Connects to the WestRouter's SSH server
- Connects to the WestAlpineCompy

- On EastAlpineCompy:
- `$ ssh admin@192.168.1.110`
- `$ ssh root@192.168.1.110 -p 2222`

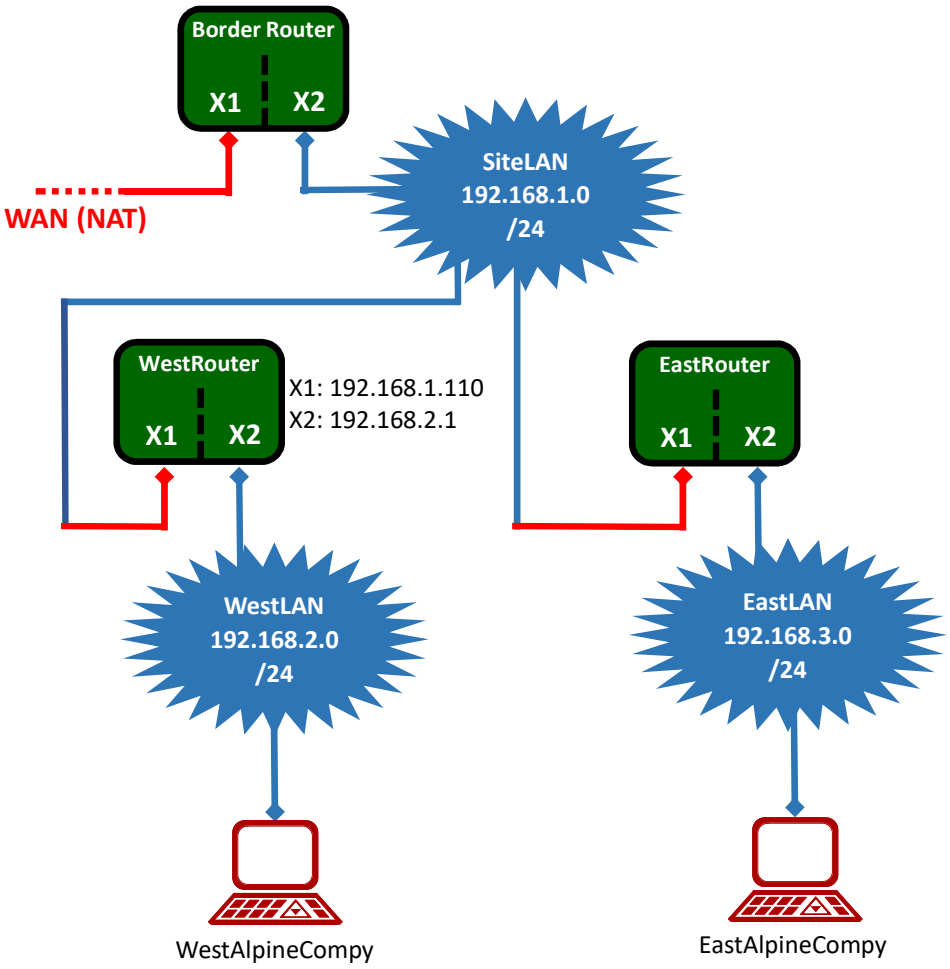
Consequences: Routing, NAT, and VPNs

- All packets out of WestRouter's X1 appear to have come from 192.168.1.110:X, and must target that SAME address and port to re-enter… but where are the LAN devices really??



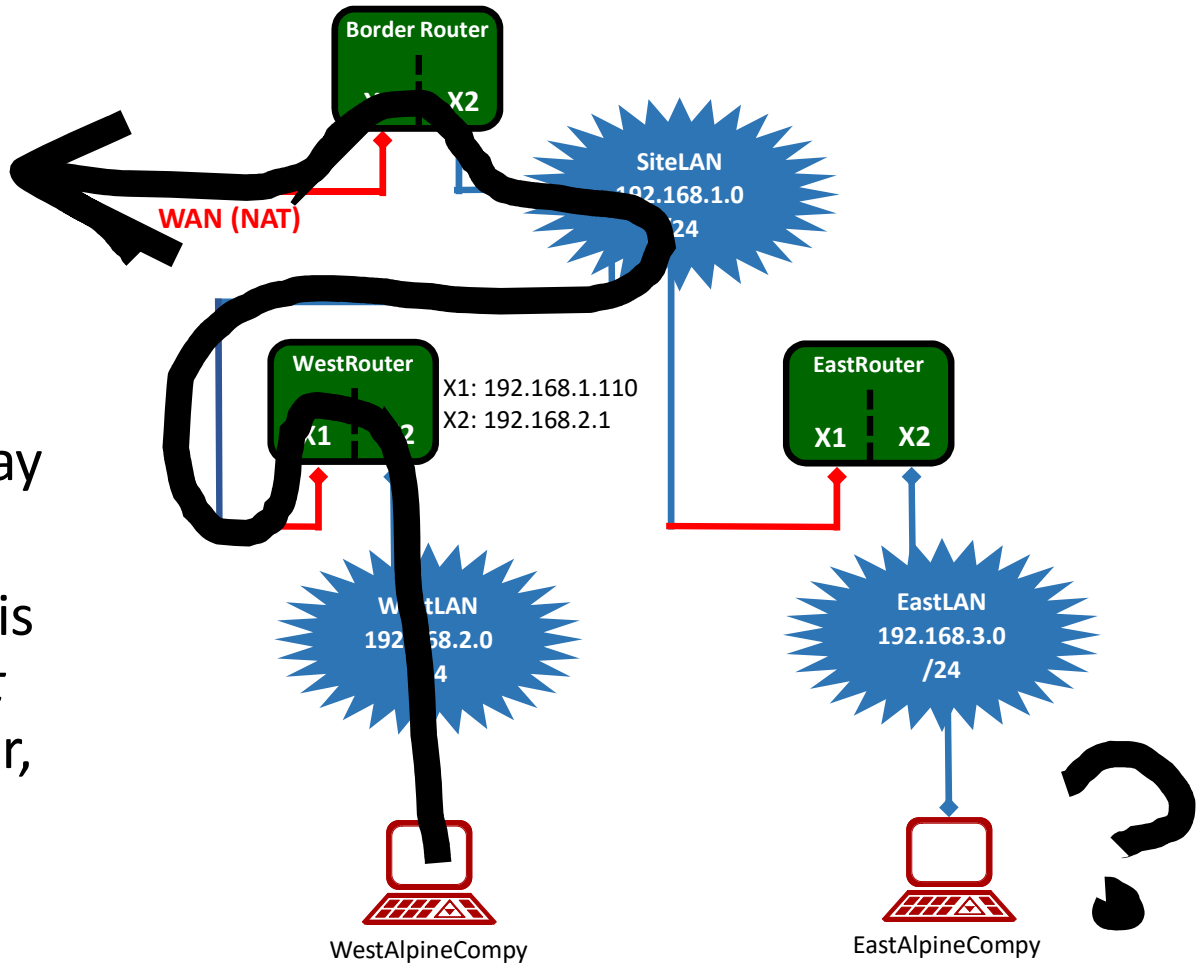
Consequences: Routing, NAT, and VPNs

- Traditional routing is used internally in place of NAT, because we aren't going to run out of IP addresses in here
- All addresses are left alone, anyone can target anyone! Except…



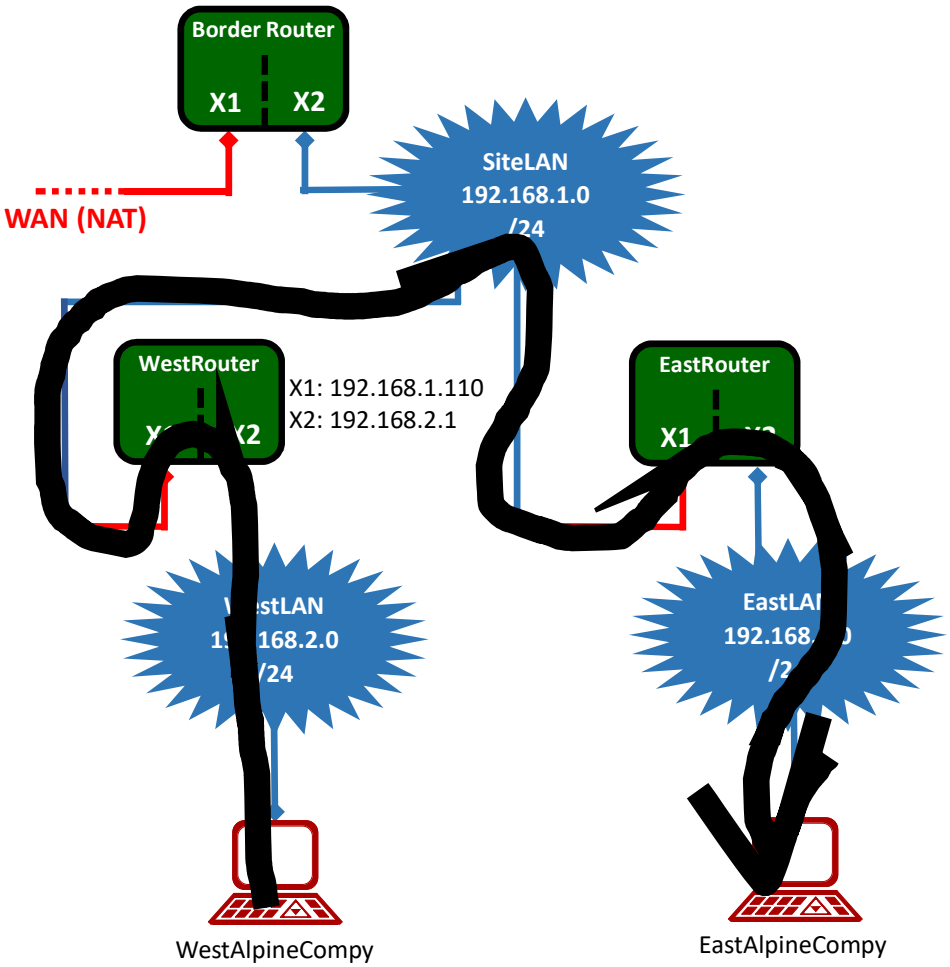
Consequences: Routing, NAT, and VPNs

- Since WestAlpineCompy's **LAN** network is 192.168.2.0, and the *default* **WAN** gateway is WestRouter…
- And SiteLAN's **LAN** network is 192.168.1.0, and the *default* **WAN** gatway is BorderRouter, then neither of those know where to find EastLAN!



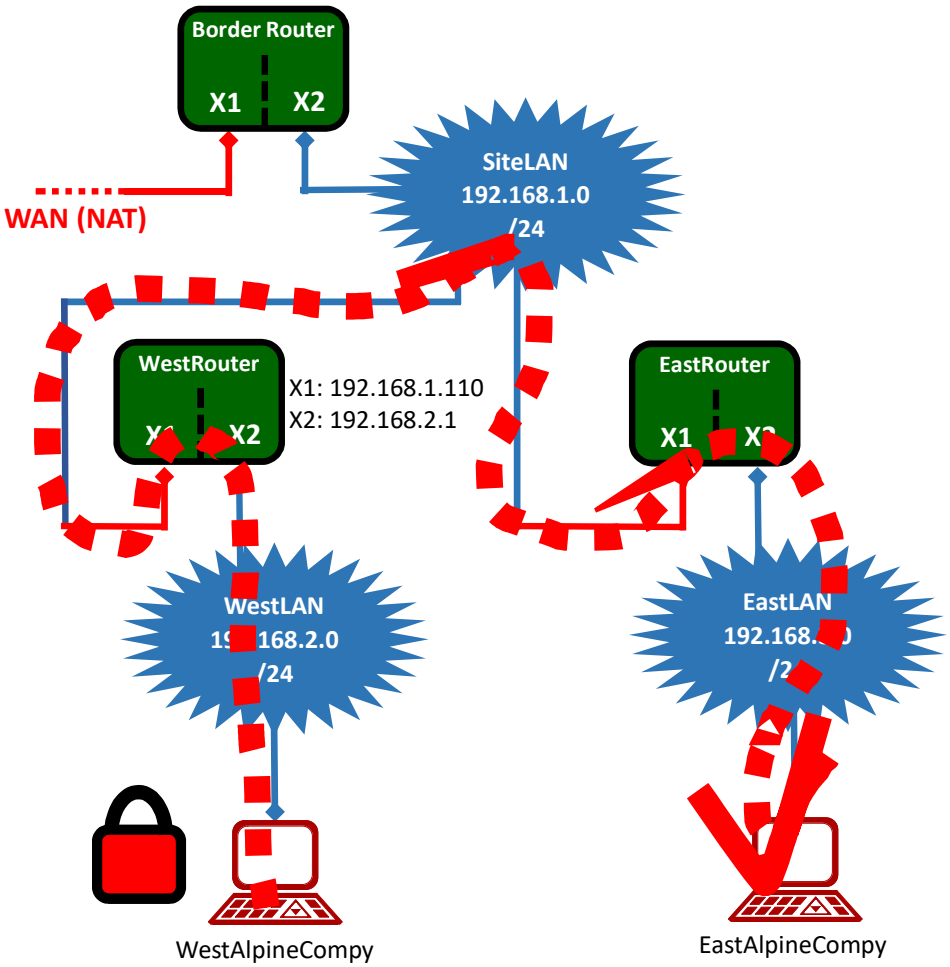
Consequences: Routing, NAT, and VPNs

- Thus, a route is set up in WestRouter's routing table that maps 192.168.3.0 through the **WAN** interface of EastRouter
- This becomes a second (non-default) gateway for WestLAN: anything destined for 192.168.3.0 is sent to the EastRouter's **WAN** interface, instead of BorderRouter

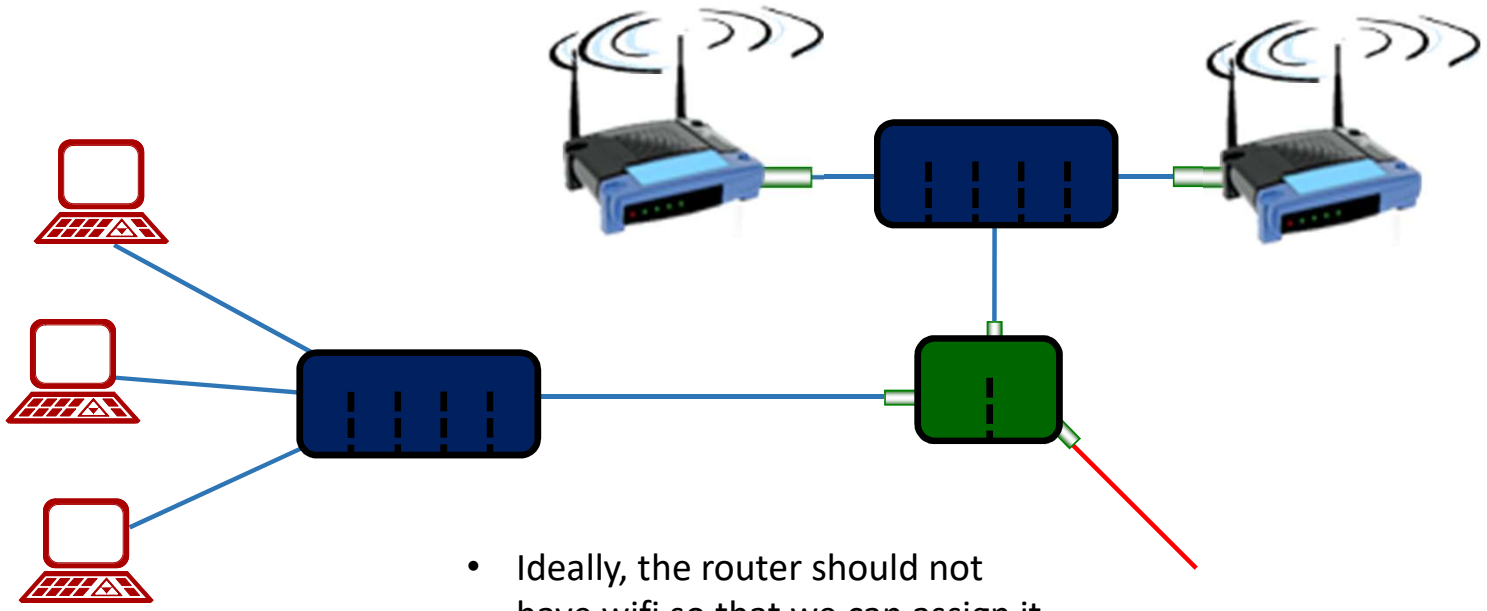


Consequences: Routing, NAT, and VPNs

- A VPN encrypts all data between two IP endpoints, and gives the two endpoints direct access to each other's networks
- With WestRouter and EastRouter X1 **WAN** interfaces as endpoints, all traffic between them becomes encrypted
- NAT breaks this, since routes don't mix with NAT
- These three concepts are the subject of the Lab

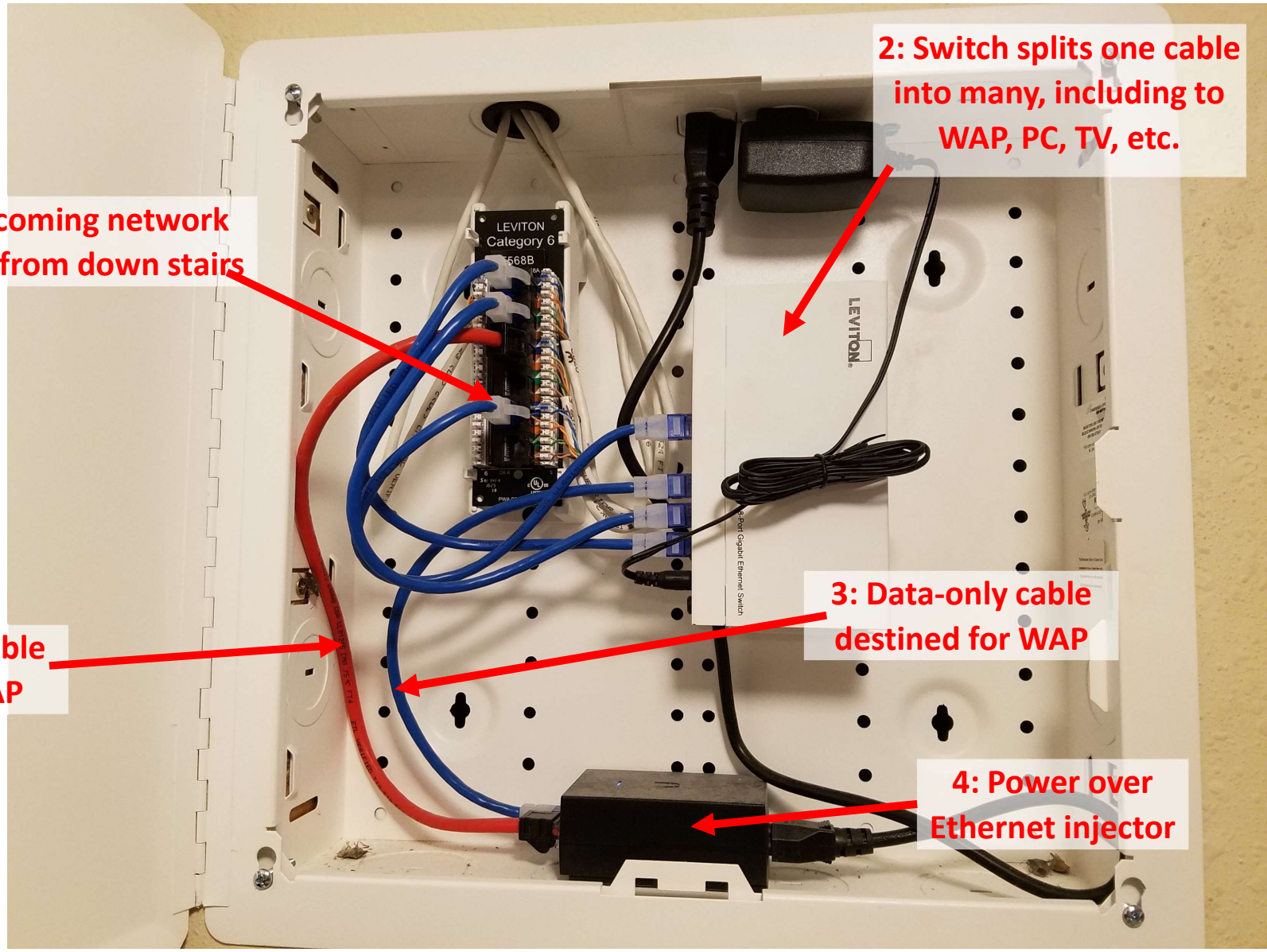


Wireless Access Point (WAP) Deployment



- Ideally, the router should not have wifi so that we can assign it from a central authority
- Maybe connected with PoE

Network Cabinet on my 2nd Floor



1: Incoming network cable from down stairs

2: Switch splits one cable into many, including to WAP, PC, TV, etc.

3: Data-only cable destined for WAP

4: Power over Ethernet injector

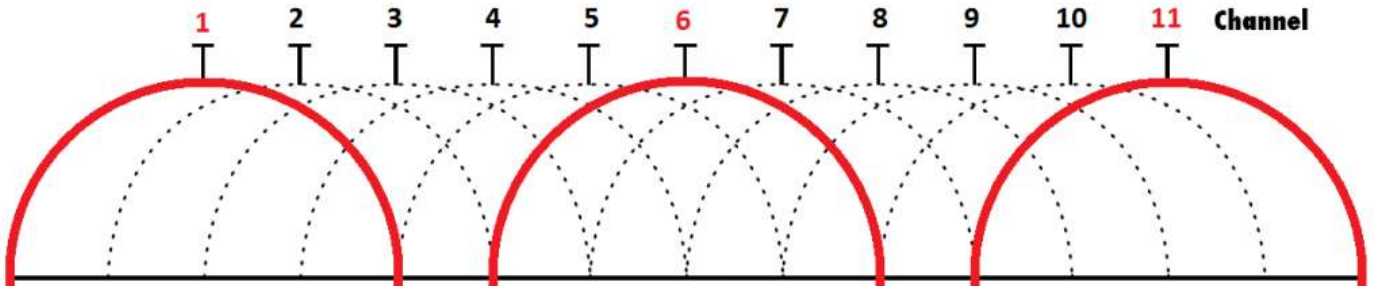
5: Data+Power cable destined for WAP

The WAP, a Ubiquiti UAP-AC-PRO-US

- 802.11ac
- 2.4 & 5GHz
- Outdoor rated,
- ~$130-170

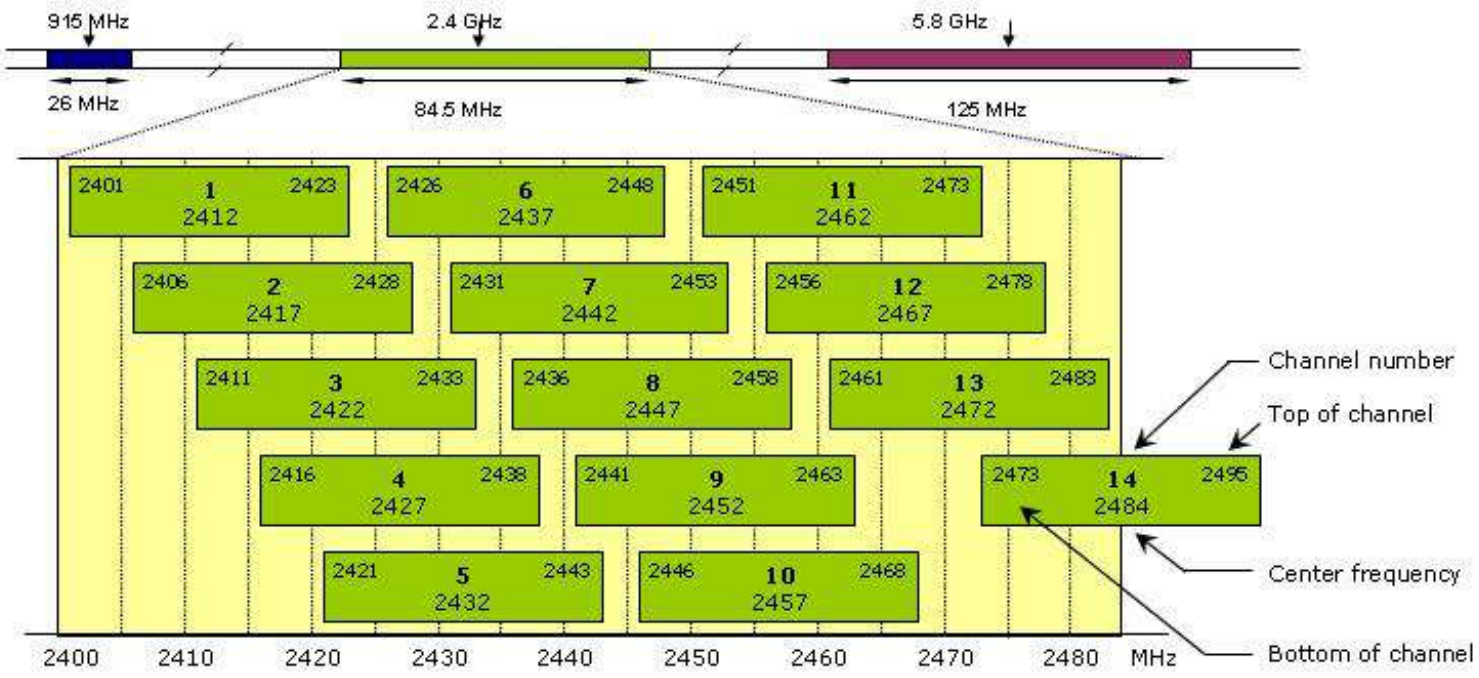
802.11 / WiFi

- Choose encryption of data to and from WAP, usually WPA2 + AES these days
- 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - Administrator chooses frequency for WAP, or the WAP can auto-hop based on measured interference
  - Interference can come from any other source of same frequency



https://igscomputers.co.uk/how-to-choose-the-right-wi-fi-channel-and-avoid-interference/

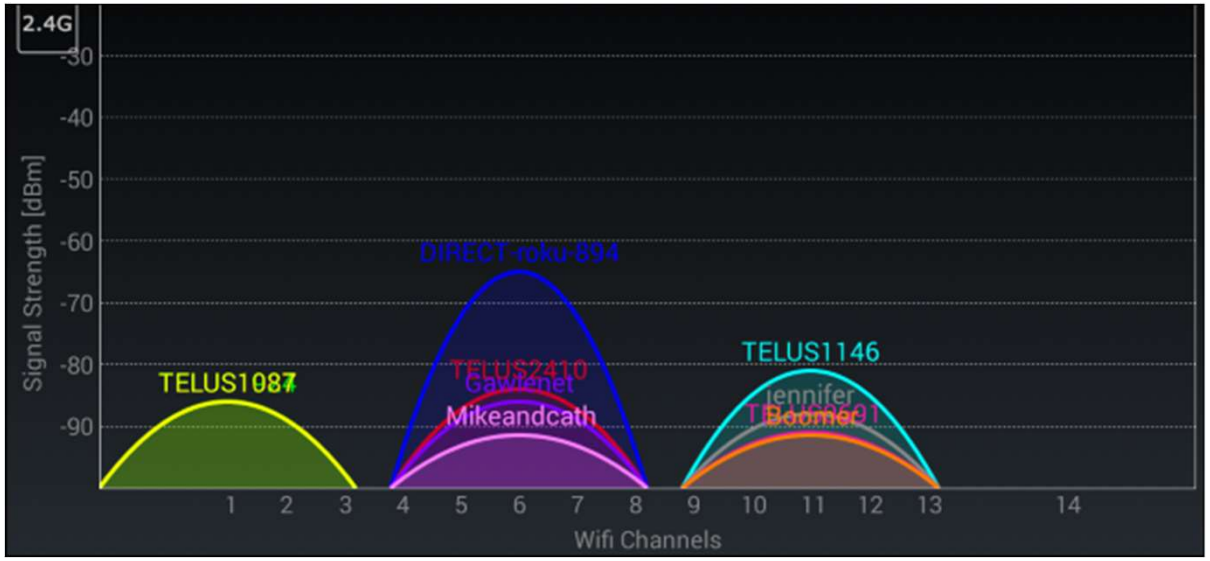
WiFi Channel Selection - Interference



https://photosync-app.com

WiFi Channel Selection - Interference

- It is worse to use the non-big three (1, 6, 11), even if they're full!
- Collisions happen on BOTH ends, and the result is a lower transmission rate

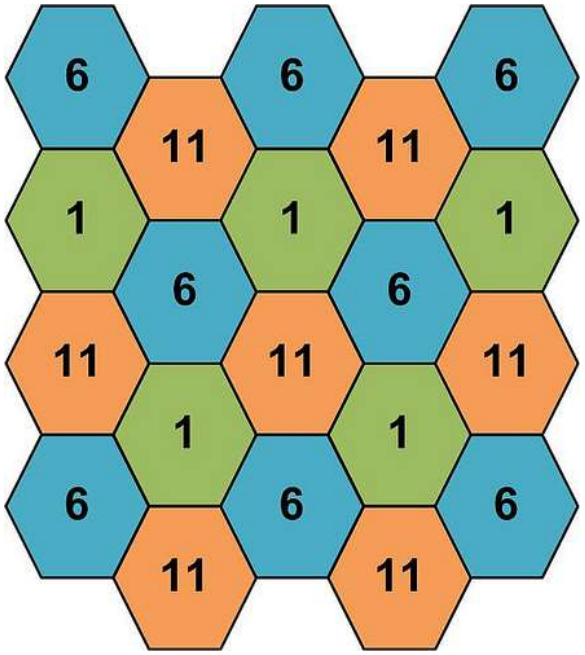


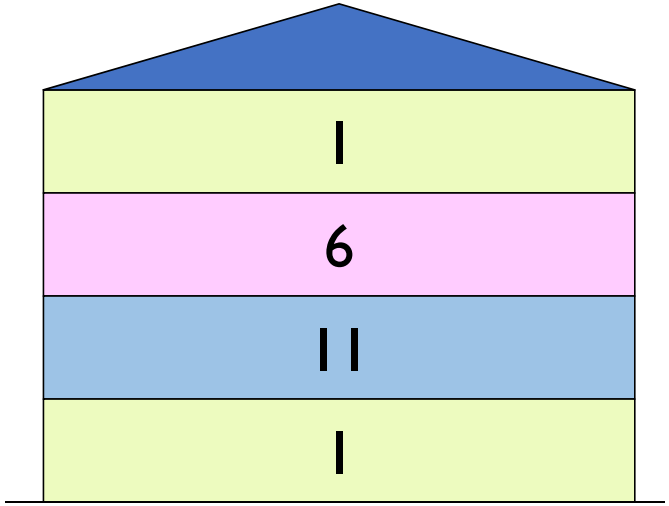
http://www.howtogeek.com/197268/how-to-find-the-best-wi-fi-channel-for-your-router-on-any-operating-system/

WAP Placement

- When placing wireless access points in a building, use a method that:
  - Centralizes the WAPs physically (i.e. make sure the radio energy isn't wasted)
    - Like SLC
  - Don't block them with metal
    - Like Church
  - Separates the channels from overlapping (as much as possible)
  - Uses the same SSID (network name) and password
  - Turn off low data rates if possible:
    - Some WAPs offer low data rates, which makes devices “stick” to them as they move around, which prevents devices from associating with closer, better WAPs
    - In some cases, using different SSIDs will help the users to know which WAP they’re connected to, if stickiness is a problem

WAP Placement





http://forum.projetoderedes.com.br/viewtopic.php?t=775

Conclusion

- Network engineering is a fascinating career
- Remember that NAT and Routes don't mix
- Every router's WAN is some other router's LAN
- Plan where WAPs should go to maximize their effectiveness