

Proper LAN Deployment

Benjamin Brewster

Why You Need to Care

- Because someday you'll have to:
 - Design and deploy a network for your business or home
 - Understand someone else's broken network so you can fix it
 - Automate IT, which requires understanding a typical network



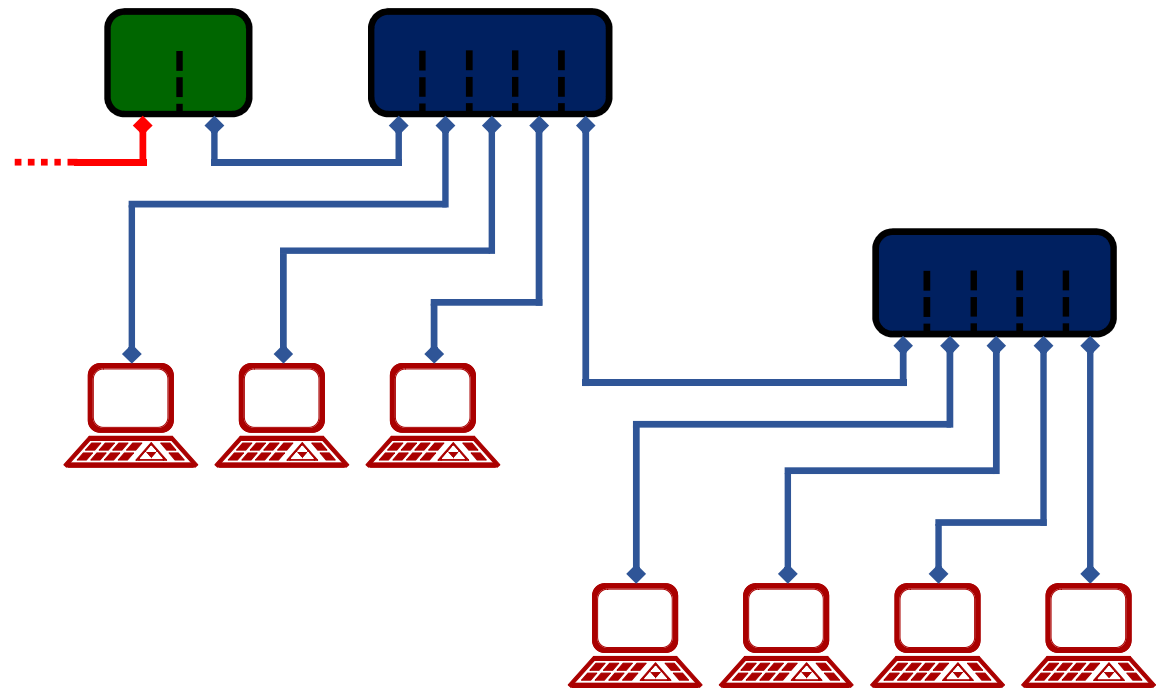
Networking in the Real World

- Network engineers attempt to lay connections across a physical hellscape full of EM, sharp edges, clueless users, hackers, faulty equipment, and lying weasels
- You will see awful things
 - Like that blue Netgear switch I found connecting everything while immersed in mud, outdoors, under a viewing platform, on a coastal cliff
- You will see things that will make you wonder why people haven't been fired, sued, arrested, or defenestrated
 - Like that heavily advertised, password-less WIFI network that connected the general public to the main company server at a tourist destination



An Ideal Network (?)

- Networks can be complicated, but they break down into simple graphs like this
- Even if the cables are running hundreds of feet from room to room, or across the 3rd floor of the dorm
- Note: no loops allowed!



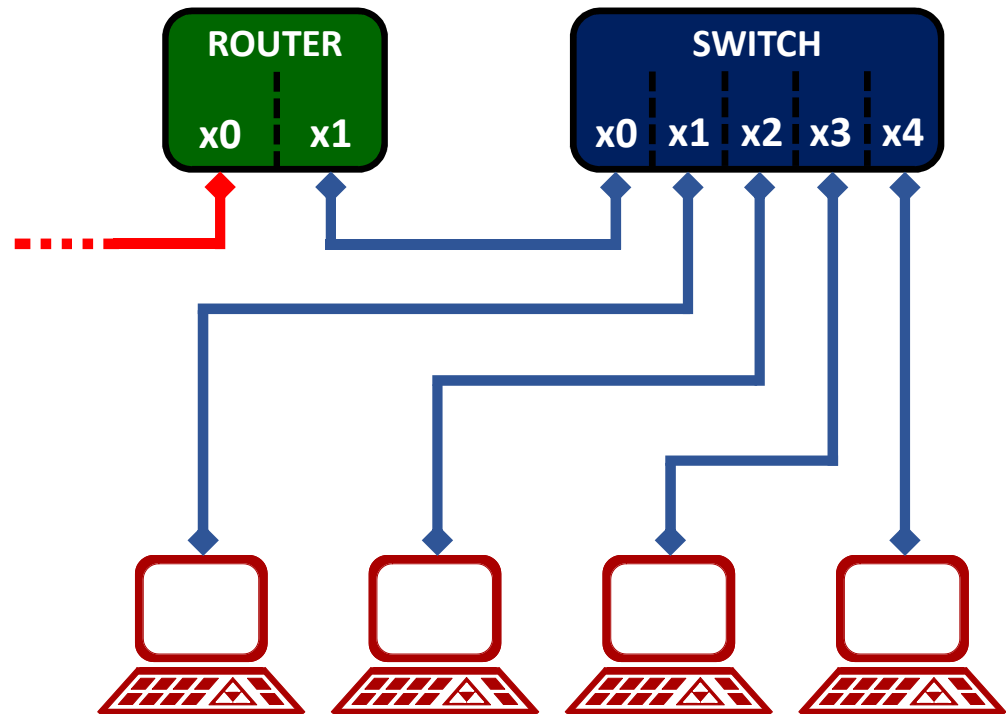
LAN = Local Area Network
WAN = Wide Area Network

← *These terms are
more descriptive
than definitional*



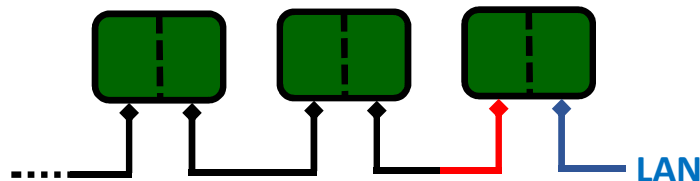
An Ideal Network

- Let's look at an idealized, *practical* LAN with one subnet
- **Routers** interpret between two different network subnets
- **Switches** merely connect devices together & ignore subnet restrictions

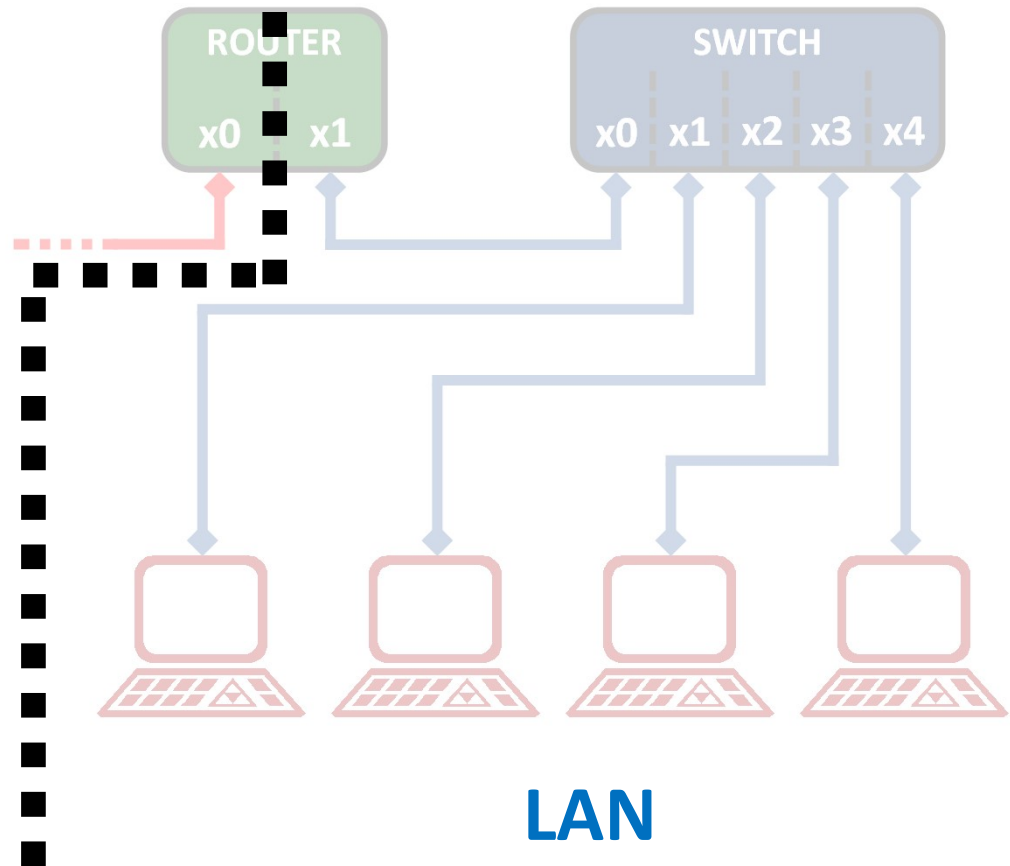


An Ideal Network

- **WAN** (wide area network) means *outside* your **LAN**
- Every **WAN** interface is contained in a subnet on some other router; to the upstream **router**, *our router* is just another device:



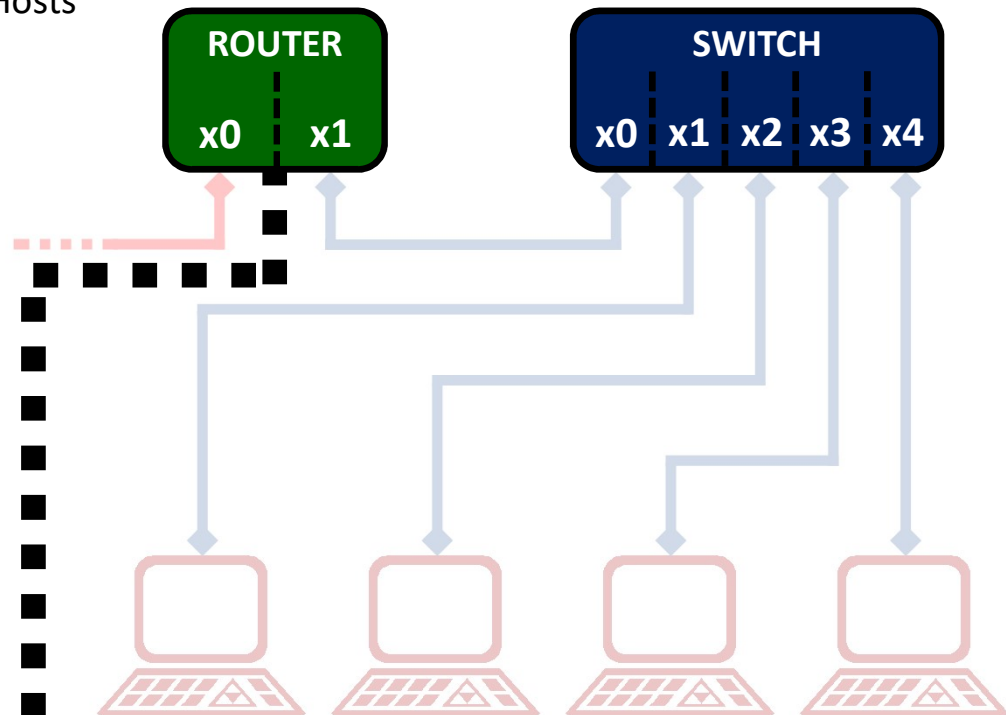
WAN



An Ideal Network

- Each **router** interface:
 - Must be on a different subnet
 - Has an IP address on that subnet
- Unmanaged **switches** do not have IP addresses on any interface: switches gonna switch

WAN
CIDR /30 subnet
2 Hosts



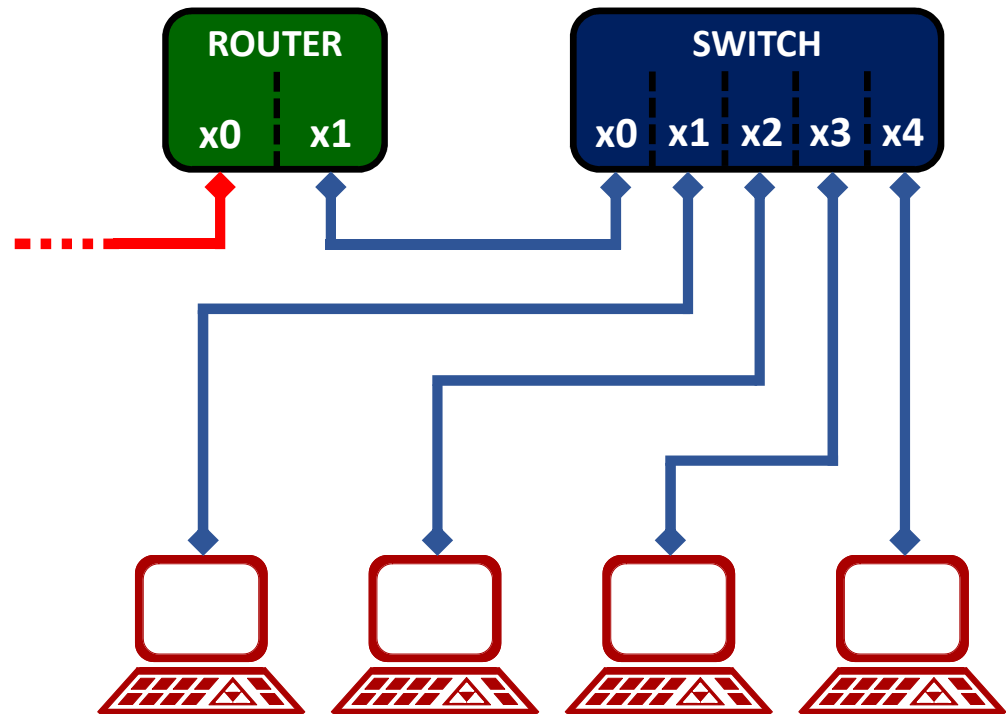
LAN CIDR /24 (Class C) subnet
254 Hosts



Getting IP

- The **LAN**-facing interface of a **router** typically runs a DHCP server in most homes and businesses
- The hosts run a DHCP client to get IP addresses on the subnet
- Both sides of the **router** need to have an IP address assigned:
 - **WAN** side can be either dynamic or static
 - **LAN** side is always static so clients can find it

WAN

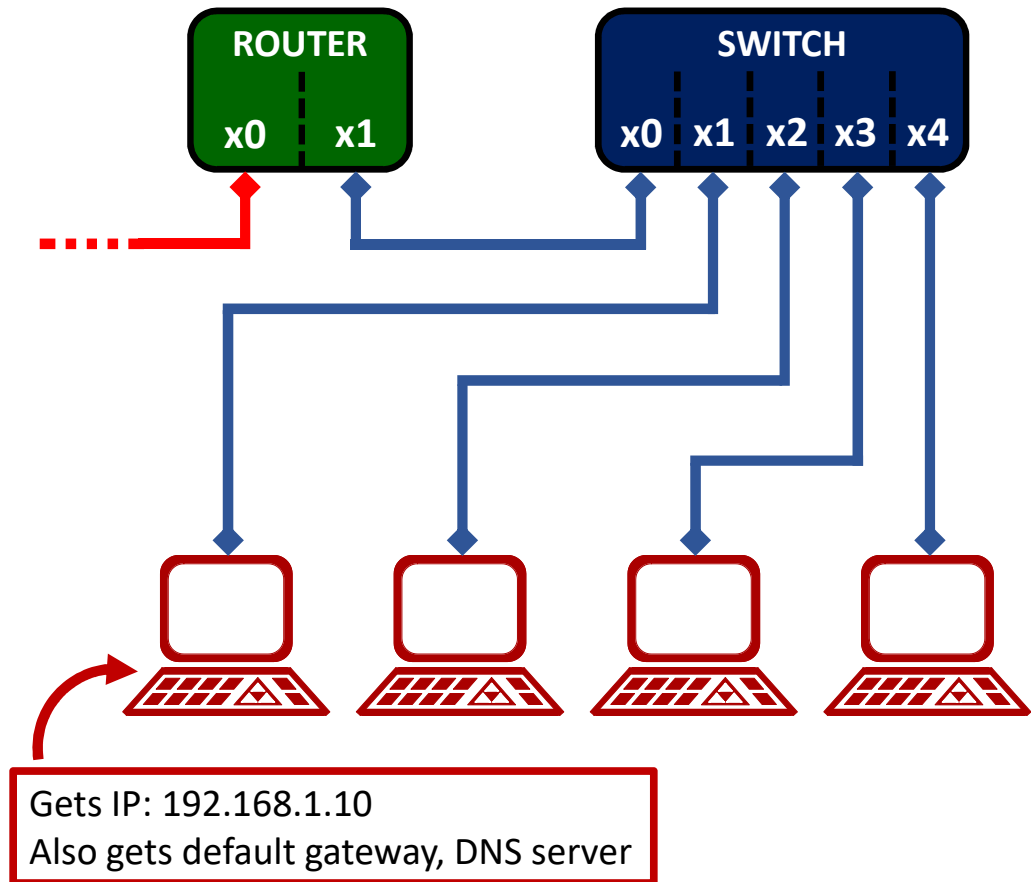


LAN



Sample Network Settings

- **Router** interfaces & data:
 - Default Gateway: 10.0.2.2
 - x0:
 - Network: 10.0.2.0/24
 - IP: 10.0.2.15
 - x1:
 - Network: 192.168.1.0/24
 - IP: 192.168.1.1
 - Runs DHCP server for network, handing out:
 - DHCP start: 192.168.1.10
 - DHCP end: 192.168.1.240
 - Default Gateway: 192.168.1.1
 - DNS Server: 192.168.1.1



Our VirtualBox Network Setup

- Our virtual network will consist of:
 - VirtualBox itself to act as switches and cabling between the hosts
 - VMs for the hosts
 - A VM host running pfSense as the router
 - VirtualBox VirtualBox VirtualBox this software is amazing - we can simulate all the parts of a network!



pfSense

- pfSense is a complete software router that can be installed onto practically any hardware: from IoT-scale, to PCs, to massive purpose-built network devices, like 48-port firewalls
- Robust, stable, in active open-source development, fast, easy to deploy and configure, works out of the box
- Based on BSD, not Linux
- Can use both CLI and web interface to configure



Our VirtualBox Network Setup - Details

SAY

- Pay attention! This is used in the Lab!
- This is our router, note two interfaces on two different networks
- "Attached to" differences:
 - NAT: VB issues an IP to the adapter via internal DHCP
 - Internal Network is internal only: any VMs can talk on that, but there is no connection to the WAN here
- Adapter type specialty: virtio net drivers are optimized for VMs
- The CS312LAN Internal Network is our base switch

DEMONSTRATE

- Boot pfSense_Reference
- Boot CentOS_GUI_Reference on CS312Lan Internal Network
- Show the VirtualBox main screen
- Select "pfSense_Reference"
- Settings -> Network
- Show all settings on Adapter 1 and 2



Our VirtualBox Network Setup - Details

SAY

- In contrast to our router, see that there's only one interface, and it's on the virtual switch

DEMONSTRATE

- Select "CentOS_GUI_Reference"
- Settings -> Network
- Show all settings on Adapter 1 and 2



pfSense Booted

SAY

- Note how there isn't a good way to see detailed settings - you have to do that from the web, unless you're really good with BSD networking commands
- We can verify that we have DNS resolution and networking in one step
- Ping to test DNS and network
- Return to the menu

DEMONSTRATE

- Getting in and out of pfSense VM using Host Key (RCTRL on Windows)
- In pfSense main console menu, see the assigned WAN & LAN addresses
- Menu 8 to get to shell
- # nslookup www.google.com
- # ping www.google.com
- # ping 8.8.8.8
- # exit



CentOS GUI Networking - All DHCP

SAY

- Talk about IP address, default gateway (called "Default Route"), and primary DNS server
- You can see that the information is all set to Automatic via DHCP, so none of this has to be set
- However, we can change to a new address! We don't have to stay on this one

DEMONSTRATE

- In our CentOS GUI VM, click on networking/sound/battery button in upper-right corner, click "Wired Connected", then click "Wired Settings"
- Have "Wired" selected on the left
- Click gear icon in bottom right
- Click IPv4 on left



CentOS GUI Networking - Change to Static

SAY

- However, we can change to a new address! We don't have to stay on this one
- Thanks Linux! I'm never giving you to my grandma
- THAT has an effect
- See that we can still access the web!

DEMONSTRATE

- Change "Addresses" to Manual
- Set:
 - IP: 192.168.1.250
 - Netmask: 255.255.255.0
 - Gateway: 192.168.1.1
 - DNS: 8.8.8.8
- Hit Apply, note that this has no effect!
- `$ sudo systemctl restart network.service`
- Browse teh webz



Rescuing a Device Outside the Subnet

SAY

- Being able to change IP addresses manually like this is handy, because sometimes we need to rescue orphan machines, like this Alpine one
- The Alpine VM starts statically at 192.168.2.200. We can't ping this from our CentOS GUI machine, because this is outside the subnet the CentOS GUI machine is on

DEMONSTRATE

- Start "Alpine_RescueMe" VM
- From CentOS GUI:
- `$ ping 192.168.2.200`
- Set static IP:
 - IP: 192.168.2.250
 - Netmask: 255.255.255.0
 - Gateway: 192.168.2.1
 - DNS: Leave at 8.8.8.8
- Hit Apply
- `$ sudo systemctl restart network.service`
- `$ ping 192.168.2.200`



Rescuing a Device Outside the Subnet

SAY

- Now, we can ping it!
- Let's connect!
- This is where the network configuration is stored
- Currently set up as a bogus static assignment
- Replace the current one with the dhcp config
- This would be setting the assignment however is proper for what you're trying to do
- Now we can access the system on the proper subnet!

DEMONSTRATE

- `$ ping 192.168.2.200`
- `$ ssh root@192.168.2.200` (yes, if asked)
 - `u: root; p: password`
- `$ cd /etc/network`
- `$ ls -pla`
- Examine the three interfaces files!
- `$ cp interfaces.bak.dhcp interfaces`
- `$ reboot`
- Change CentOS back to DHCP IP address
- `$ sudo systemctl restart network.service`
- `$ ping 192.168.1.19` (or whatever it shows)



Playing with pfSense Settings: Admin

SAY

- Let's connect to our pfSense router's GUI config pages and see what we can find
- Connecting to the default gateway's address via HTTP is usually a great way to find the router's config page
- The Assignments page shows us the names of the interfaces as pfSense sees them, and how they are assigned.
- This page shows a ton of stuff for managing the router itself
- Important here is the TCP port, which is occasionally changed to meet some other networking requirement, like a port-forwarding rule
- Never fail silently! This just sets the path of communication up - you set up actual alerts elsewhere.

DEMONSTRATE

- Start Firefox, go to 192.168.1.1
- Log in with admin/password
- Click on Interfaces -> Assignments
- Click on System -> Advanced
- Talk about webConfigurator (the router's web page system) section, TCP port field.
- Explain Notifications tab usage.



Playing with pfSense Settings: Admin

SAY

- DNS settings and the name of the router can be changed here.
- I've also changed the theme to be Dark, since I usually have lights off in my office

DEMONSTRATE

- Click on System -> General Setup



Playing with pfSense Settings: WAN

SAY

- Here, we can change the WAN interface from getting it's config via DHCP, or whether it's statically assigned; both static and DHCP WAN assignments are common

DEMONSTRATE

- Click on Interfaces -> WAN
- Talk about DHCP Client Configuration section, "Reject leases from" field, and the dorm router story.
- Talk about Reserved Networks section, "Block private networks and loopback addresses" field. Handy!



Playing with pfSense Settings: LAN

SAY

- IP config for LAN interface of the router is static so that it can be easily found by devices on the subnet

DEMONSTRATE

- See how IPv4 Configuration Type is set to "Static IPv4"



Playing with pfSense Settings: DHCP

SAY

- We can configure the DHCP settings here
- In pfSense, we can leave the DNS servers fields alone in order to distribute the system default DNS settings. We can override the defaults here.
- Similarly, the Default Gateway field can be overridden.
- The Domain is for allowing those services that need it to know where they are (normally Windows)
- Static ARP makes it so that only the MAC addresses listed below can access the router on this interface, i.e. the ARP table can't be changed.
- This sounds good, but MAC addys can be spoofed.

DEMONSTRATE

- Click Services -> DHCP Server
- Show the Range fields
- Show and explain DNS, Gateway, and Domain name fields.
- Show Static ARP field



Playing with pfSense Settings: UPnP

SAY

- Bonus feature! If you decide to set up pfSense as your router, and you do any gaming, make sure to enable UPnP!
- UPnP allows a device to open ports on the router/firewall and configure port-forwarding rules that point to itself, so that external devices can connect automatically
- If that sounds like a massive security hole, you're right: it's normally something you only find on routers designed for home use.
- It's often not even an option on business-class routers!

DEMONSTRATE

- Click Services -> UPnP



Conclusion

- The network terms and settings we normally concern ourselves with are:
 - WAN
 - Getting an IP and DNS settings for the WAN
 - LAN
 - Defining the LAN's IP network
 - Providing DHCP to that network
- pfSense makes some great router software!
- We'll be talking about WiFi, VPNs, and Firewalls next time

