1.5 routers and firewalls

As a computer engineer, you will doubtless be asked to setup a home router for your home or one of your friends (you could even make a job of it).

Definition of terms:

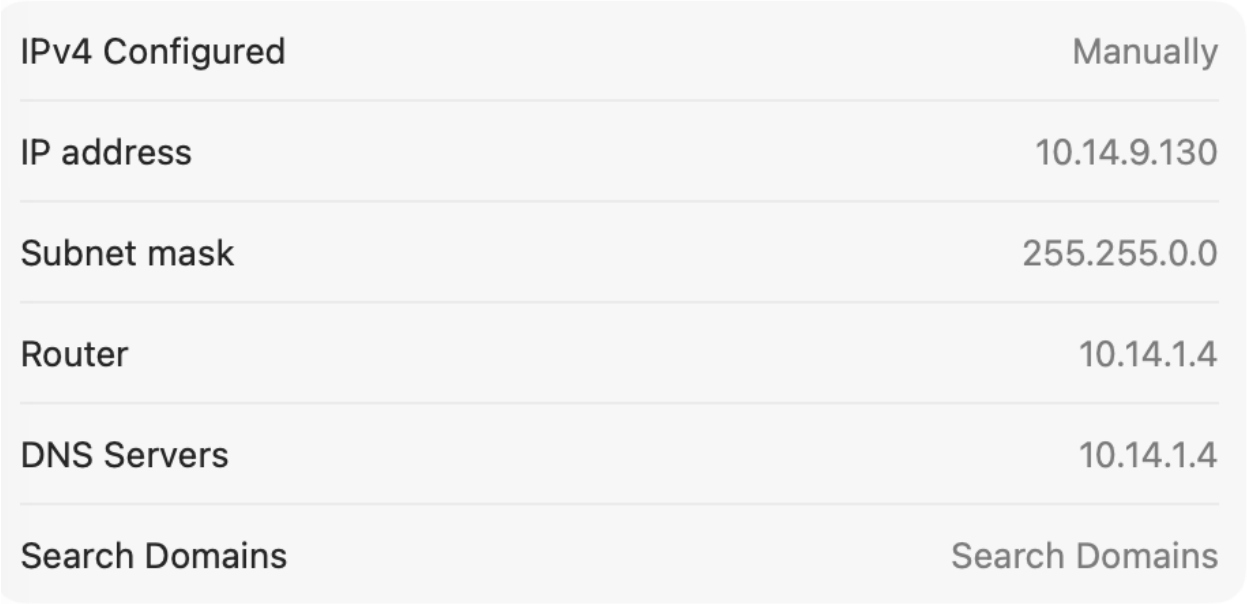
- **Router**: anything that converts one physical form of data transmission like a cable modem or fiber to a wired ethernet network
- **Access point:** a wifi station that broadcasts your INTERNAL network for users in your home
- **Switch**: anything that connects parts of a wired network to another part, like a hub, only smarter, some routers have a few ports built in, which you can see below
- **Firewall**: a special part of most routers that blocks invaders but can also be seen as a "bouncer" at a bar, letting in some people and not others
- **WAN** is the wide area network, or the internet in our case
- **LAN** is the local area network, your home network that we need to keep safe

Some terms to review first:

Internet terms:

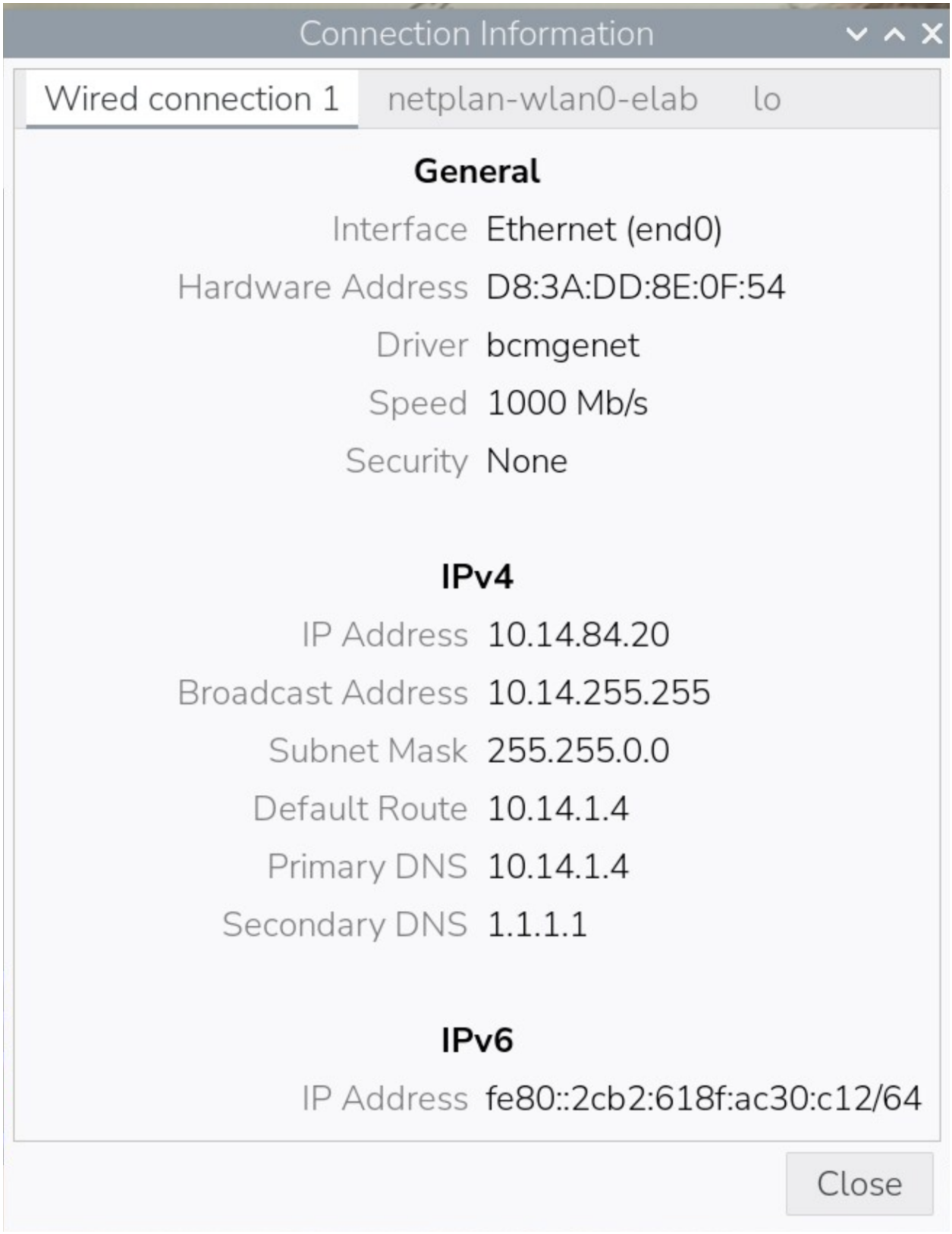
- Your computer needs 4 things to be able to get onto the internet:
- **IP address**, example 10.14.88.83
- **Subnet mask**, example 255.255.0.0
- **Gateway/router,** example 10.14.1.3
- **Domain name serve**r (DNS), example 10.14.1.4

Look up your network settings on whatever device you are on, you should see all of these
Mac: look under system preferences, network:



Screenshot 2026-04-22 at 3.31.30 PM.png

Pi: look for up and down arrows on the upper right, select "advanced options" and "connection information"



Screenshot 2026-04-22 at 3.31.03 PM.png

Here's what each one does:

IP address:

All traffic on the internet or local area network (LAN) is in the form of packets of information, like mail envelopes with a letter inside. Each letter you mail has two important things: the address you want it to go to, and the message inside the envelope.

- TCP/IP is the format of these, which stands for Transmission control protocol and internet protocol.
- The TCP part is the message, and the IP part is the envelope, with an IP address on it.
- Check the IP address of your machine:
- From the GUI: open system preferences, network
- From the terminal: type ifconfig
- Your computer may have an address in the form 10.14.253.x, this means you are "leasing" an address from the system (more below)

Subnet mask:

- Imagine you want to stay in one of two large 254 room hotels. One has long hallways, and very few floors, the other has many floors, but short hallways.
- If you want to sleep, you don't want many people walking down the hall in front of your room. You want many floors with fewer rooms per floors.
- This is what subnet masking does on a network. Each of the four segments can hold 254 addresses.
- At home, you probably have a network that looks like this:
- IP: 192.168.1.49
- mask: 255.255.255.0
- router: 192.168.1.1
- dns: 192.168.1.1

This means that the last zero can hold up to 254 addresses (from 192.168.1.1 to 192.168.1.254)

- HPA has this sort of mask:
- 255.255.0.0
- which means that
- 10.14.0.0
- is the elab, which can have 254 x 254 addresses
- It makes for a quieter network, also providing some security as others cannot see you easily.

Router/gateway:

This is the gateway for all of your traffic, usually the access point at your home. The technical difference between these words is that a router routes traffic between two networks of the same type (like ethernet), while a gateway is between different types of networks (like a cable modem or DSL gateway).

A firewall is just a gateway that has an outside part and an inside part.

Your gateway may also distribute IP addresses inside your network. At home this will likely look like 192.168.1.x, where at the elab, our network leases addresses in the form 10.14.253.x.

To scan these addresses here, you can use nmap 10.14.253.0/24

Domain name server:

- This is the computer on your network or outside that translates names into numbers, like a digital phone book.
- Try this in terminal:

nslookup elab.hpa.edu

1. when you get the address, write it down
2. open a browser
3. go to elab.hpa.edu
4. now go to the numbers you wrote down.
5. Try this with another name, either on campus or off
6. you are asking our domain name server (DNS) to resolve the name into a number
7. this also works in reverse, from numbers to names
8. using ARIN.net you can find the location of IP addresses outside your network

----tools to use to check your network configuration, or fix a broken one-------

NSLOOKUP:

- Say you want to find out the name of something, or the IP address from the name.

- try this:
- nslookup
- (you will get a funny > sign)
- type:
- server 10.14.1.4
- type:
- elab.hpa.edu
- what do you get?
- where is this machine?
- Try again using 8.8.8.8 as the server (this may be blocked by our system)

The best use of this is to find out what OTHER people might call a machine.

- We have several DNS servers at the elab, the main one is at 10.14.1.4
- Others to try:
- 4.4.4.4
- 8.8.8.8 (google)

- you can get out by typing
- exit
- or control-z (halt)

Ping and traceroute:

- Imagine you want to find out if a machine is responding (you can block this by using "stealth mode")
- In terminal ping one of the IP addresses in your class
- ping an address out on the internet
- what is the difference?

now try this:

traceroute www.apple.com

- It should give you a trace of the path your connection took.
- Try this with other addresses on and off campus.

A **router** is a device that physically separates two networks. If the router can also filter traffic in and out of your network, it is also a **firewall**
You will setup a firewall here, and your friends will try to "break in".
Thinking of a selective club or restaurant: there would be the bouncer (usually a very big person guarding the door) who lets some traffic (people) in.
The bouncer can also get messages out of the restaurant to the outside, and when the message returns, they can pass it back inside.

Router setup:
We will first be using the TP-Link Archer C9 home router/access point for your network.
Why?
It should be similar to most home routers you will setup for yourself or your friends.
Industrial ones for colleges and such may have more options, but the fundamentals are the same.
We have others for you to learn on as well, so you will be able to make many $$$ if you want to charge folks...

Here's what it looks like:



- start with the ports: blue is the WAN (wide area network) you connect to the internet
- yellow are the LAN (local area network) ports for your network.
- the usb port is for external storage
- note the antennas, most routers will have many of these, or they may be built in

Setup:

- the WAN for your router will be the HPA elab network, in the form 10.14.254.x, connected to the blue port
- your router will borrow an address from the elab for the day, which is called DHCP, just as your laptop, iPad or phone borrows an address when you come into the elab
- the LAN side of the router (yellow ports, pick one) should be in the format 192.168.1.x and will usually be the first in this subnet or 192.168.1.1.
- the domain name server is usually baked into the router, so same address
- the router will also give out DHCP address to the LAN side, so you will connect your pi to the LAN side with a wire, and your laptop to the router using the wifi network of the router/access point
- make sure the router is completely erased, and start from scratch, connecting as above and see what addresses you have
- go to the admin page and change the wifi network name and password (keep these secret)

Inbound port mapping:
Suppose you want to have a web server in your home, but you don't want everyone in the world to get into your computer.
A firewall can be setup to pass inbound traffic on certain ports, in our case port 80 (web) and port 443 (secure web).
We want to be very safe with your computer so first of all, create a temporary web server on your laptop. Enter the following in terminal on your laptop:

python -m http.server 8000

Now go to your browser and type in http://localhost:8000
What do you see?

Repeat using http://127.0.0.1:8000
What now?

We want to pass inbound visitors (the bouncer again) to your inside web server.
Locate the pages that say inbound port mapping.
Enter the port 8000 and the IP address your laptop now has from the router wifi
apply and save

From a computer elsewhere in the elab, go to the outside address of your router on a browser, using the same port:
10.14.254.x:8000

See?
Wow! you just setup a network with a server at your house!
Could this work for hosting a minecraft server?

Next: only letting your friends into your wifi, even if someone gives them your secret password!

Challenges:

1. connect a router to the internet (WAN) and a wired computer (LAN) including power and admin user
2. setup a basic wifi network with password
3. show how to monitor who is using your wifi network
4. setup restrictions on your network using MAC addresses (like they do in the dorms)
5. setup port forwarding from the WAN side to your pi web page (port 80)
6. setup port forwarding from the WAN side to your pi port 8000 running python3: python3 -m http.server

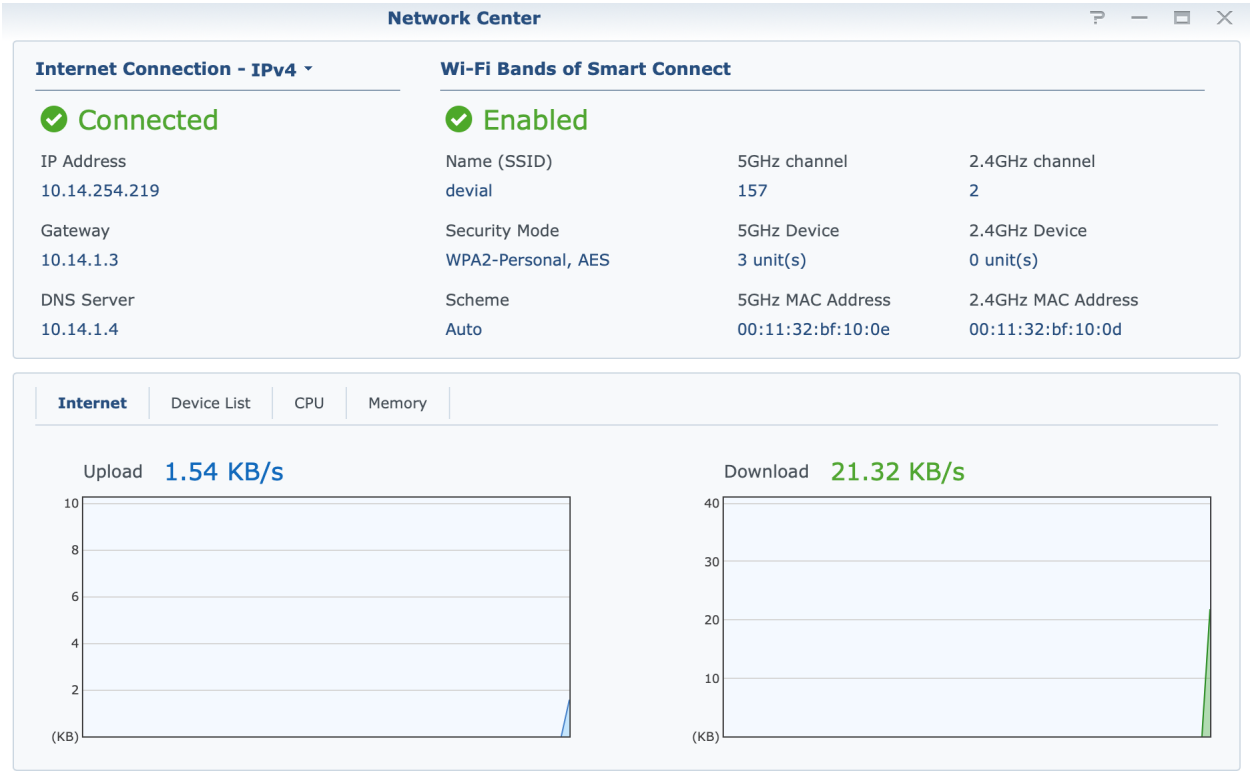
Homework: 4.27.26

1. Looking at this diagram, where do you connect the internet?



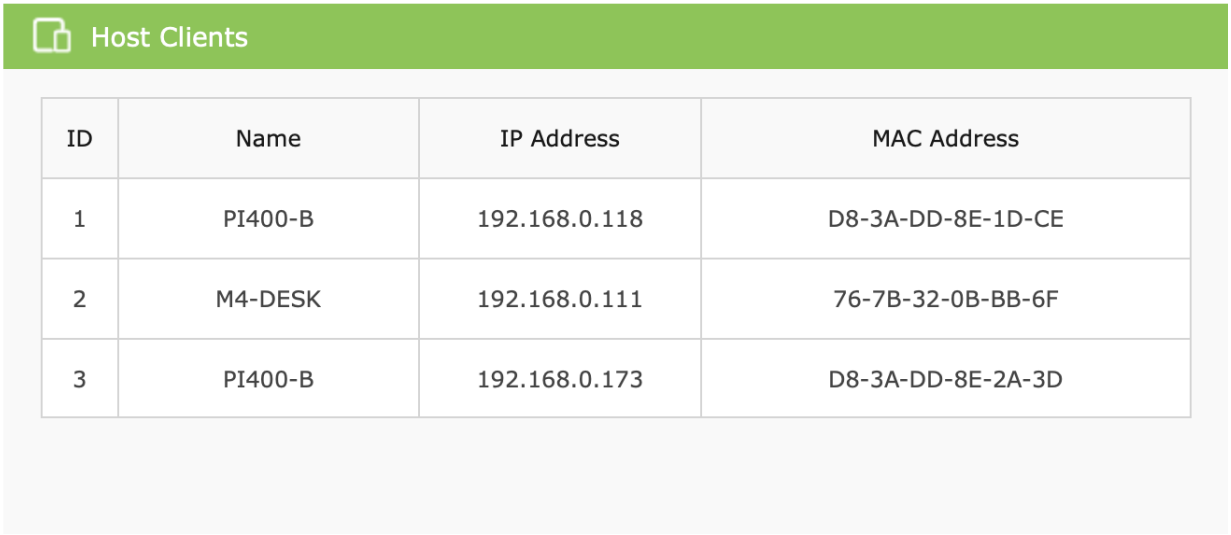
Screenshot 2025-09-03 at 4.37.41 PM.png

2. What is the outside address for this router?



Screenshot 2026-04-27 at 3.16.59 PM.png

3. what is the MAC address for the computer that is not a PI?



Host Clients

ID	Name	IP Address	MAC Address
1	PI400-B	192.168.0.118	D8-3A-DD-8E-1D-CE
2	M4-DESK	192.168.0.111	76-7B-32-0B-BB-6F
3	PI400-B	192.168.0.173	D8-3A-DD-8E-2A-3D

Screenshot 2026-04-27 at 3.15.02 PM.png

4. If you were a hacker, how would you know that #1 and #3 are Pi-400 from their MAC address? (hint: copy the MAC address into https://www.wireshark.org/tools/oui-lookup.html)

Migrated from Apple Server Wiki. Original page ID: x6e0d8v3_

Revision #2
Created 2026-09-29 15:59:39 UTC by Admin
Updated 2026-09-29 16:22:25 UTC by Admin