

Homework — Networking Infrastructure

Estimated time: ~45 min · No code required · A browser, your home router, and optionally a free download

Three tool-tour exercises. The goal is to turn the abstract picture from the theory page into things you can actually observe: your own connection type, the SOHO world inside your home router, the scale of a data-center campus, and what the Tor anonymizer looks like from the outside. No installs are required for Tasks 1 and 2. Task 3 involves downloading Tor Browser — a free, widely-used application that you can uninstall when you're done.

Before you start

Keep a short notes file (or a piece of paper) open. For each task, jot down the answers to the lettered questions. You are not turning this in — the notes are for you to check that you actually *saw* the things the lesson is about, not just read about them.

The three tasks

Task 1 — Your connection and your router

First, find out what kind of connection you have and poke around the SOHO device that manages it.

1. Open speedtest.net and run a test. When it finishes, note the **ISP name**, the **connection type** if shown (Fiber, Cable, DSL, Cellular), and your **download / upload speeds**.
2. Now open ipinfo.io in a new tab. Write down your **public IP address** and the **org / ISP line**. Does it match what Speedtest reported?

3. Open your **home router's admin page**. The address is almost always `192.168.1.1` or `192.168.0.1` — type it directly into your browser's address bar (not a search engine). Most routers use `admin / admin` or `admin / password` as the default login; check the label on the bottom of the router if that doesn't work.
4. Once inside, explore the settings menus until you find and note down **three SOHO features** mentioned in the lesson. Common examples to look for:
- **DHCP** — usually in a "LAN" or "Local Network" section; shows the range of private IPs being handed out.
 - **NAT** — often visible as "WAN IP" vs your devices' "LAN IPs"; that gap is NAT in action.
 - **Wi-Fi bands** — note whether you see 2.4 GHz, 5 GHz, or 6 GHz listed.
 - **Connected devices** — a list of every device on your network and its private IP.
 - **Firmware version** — note it. Is there an update available?

Self-check — answer all three:

- **(a)** What ISP and connection type does Speedtest report?
- **(b)** What is your public IP, and does the ISP label on ipinfo.io match?
- **(c)** Name three SOHO features you found in the router admin UI (you don't need to change anything, just note what you saw).

✓ You have found where the boundary between “private home network” and “public internet” lives, and you’ve seen that your router is doing more than just “providing Wi-Fi.”

Task 2 — The data-center world from Google Maps

One of the sharpest ways to feel the scale difference between SOHO and data-center networking is to look at the physical footprint.

1. Open [Google Maps](#) and search for "**Google Data Center Council Bluffs Iowa**". Switch to **Satellite view**. Zoom out until you can see the full campus — the grey rectangular buildings with their characteristic cooling equipment on the roof.

2. Use the map's **measure distance** tool (right-click on the map → "Measure distance") to estimate the rough **length and width of the campus** in metres or feet.
3. Compare that to the floor plan of your home or apartment. The data-center campus is, typically, the size of several city blocks.
4. Now open the Wikipedia article: en.wikipedia.org/wiki/Google_data_centers. Read the first two paragraphs only. Note one fact that surprised you.

Self-check — answer all three:

- **(a)** Roughly how large is the Google Council Bluffs campus? (Your best estimate from the satellite view is fine.)
- **(b)** One fact from the Wikipedia article that surprised you.
- **(c)** Can you spot the *cooling towers* on the satellite image? (Hint: they look like large rectangular structures with fan housings on top, often beside the main buildings.) Why do you think a data center needs so much cooling infrastructure?

✓ You have a physical mental image for the “data center” world — it is not a server room in an office basement.

Task 3 — See Tor in action

This task demonstrates what the theory page explains about anonymizers: your apparent IP address changes to an exit-node IP in a country you may not be in.

1. Download **Tor Browser** from torproject.org/download. It is a free, open-source application maintained by a non-profit. No account or sign-up required.
2. Open Tor Browser and wait for it to connect to the Tor network (it shows a progress bar; usually 10–30 seconds). When connected, it opens to the Tor start page.
3. In Tor Browser, navigate to ipinfo.io. Note the **IP address**, the **country**, and the **ISP / org** shown. These are the details of a Tor *exit node* somewhere in the world — not your home IP.
4. Open your normal browser (Chrome, Firefox, Safari, Edge) in a separate window and also navigate to ipinfo.io. Compare the two IP addresses side by

side.

5. Optional: click the **New Circuit for this Site** button in the Tor Browser toolbar (the broom icon or the lock icon in the address bar). Reload ipinfo.io. Notice that the exit-node IP has changed again.

Self-check — answer all three:

- **(a)** What country did your Tor exit node appear to be in?
- **(b)** Does the org / ISP line on the Tor IP look like a commercial VPN provider, a hosting company, or something else? What does that tell you about who runs Tor exit nodes?
- **(c)** Pages loaded noticeably slower in Tor Browser than in your normal browser. In one sentence, why? (Hint: count the hops.)

Uninstall note

Tor Browser is a self-contained application — it does not install anything into your system or modify your other browsers. You can delete it like any other application when you are done.

What “done” looks like

You're done when, in your notes, you have:

- Your ISP name, connection type, public IP, and three SOHO features from Task 1.
- A rough campus-size estimate and one surprising data-center fact from Task 2.
- Your Tor exit-node country, an observation about who runs exit nodes, and a one-sentence explanation of why Tor is slower from Task 3.

The aim was never to make you a network engineer in 45 minutes. It was to make the words “SOHO router,” “data center,” and “anonymizer” refer to things you have actually *seen*, not just read about. The next time someone mentions a “VPN” or asks why a data center needs an entire city block of cooling, you will have a picture.

Where this goes next

Lesson 09 moves from the physical and logical network into security: how attackers move through networks, what firewalls and intrusion detection systems do, and how zero-trust architecture changes the perimeter model. The networking concepts from this lesson — VLANs, VPNs, traffic monitoring — reappear there as the things defenders are protecting and measuring.