How Does the Internet ACTUALLY Work?

A clear, practical walkthrough of packets, TCP/IP, DNS, routers, modems, physical signals, and what happens when you load a website.

The big idea
The internet is a system for moving small pieces of digital information across interconnected networks. Protocols give those pieces addresses, rules, and reliable delivery.

How does the Internet ACTUALLY work?

1. How Two Computers Communicate

- All computers have something like a digital address, called an **IP address**. This is how they find and talk to each other.
- When one computer wants to send data to another, it breaks the message into small chunks called **packets**.
- Each packet travels across the network and gets reassembled at the other end.
- The computers follow a set of rules (called **protocols**) to make sure everything is delivered correctly. The most important ones are **TCP** and **IP**.

What is TCP and how does it work?

TCP (Transmission Control Protocol) is a set of rules that two devices follow to send data reliably.

What it does:

- Makes sure data **arrives in the right order**
- Resends anything that gets **lost or damaged**
- Prevents sending data too fast and overwhelming the other side

How it works (simplified):

1. **Handshake:** Your laptop says "Hello" (`SYN`), the server replies "Hello back" (`SYN-ACK`), and your laptop confirms with "Okay, let's go" (`ACK`). Now they trust each other and start talking.
2. **Sending data:** Your laptop sends packets with parts of the website request. Each packet has a number so the server knows how to reassemble them.
3. **Acknowledgment:** The server replies, "Got it!" after each chunk. If it doesn't reply, your laptop resends that packet.

4. **When done:** They agree to stop (using a "FIN" flag) and close the connection cleanly.

Why we need TCP:

The internet can be messy — things get dropped or arrive out of order. TCP keeps everything correct, complete, and clean.

What is the IP Protocol and how does it work?

IP (Internet Protocol) is responsible for **delivering packets to the right address**, kind of like the postal service.

What it does:

- Adds the **source and destination IP addresses** to every packet
- Helps routers along the way figure out **where to send the packet next**
- Doesn't care about the data inside — just the delivery

How it works:

- When your laptop wants to send a packet, it wraps it in an **IP header**.
- The header includes: Your public IP (where it's from), the website's IP (where it's going), and a few other things like how long it can travel before being dropped (TTL).
- Every router along the path reads the destination IP and sends the packet one step closer to that target.

IP is like the address label on a package. It gets your data where it needs to go — but it doesn't care if the package is broken or if it's late. That's TCP's job.

2. Your Laptop and the Router

- Your **laptop** connects to your **router**, usually through Wi-Fi.
- The router gives your laptop a local IP address, like `192.168.1.5`.
- This local address only works inside your home network.
- When your laptop wants to access a website, it sends the request to the **router**.

3. The Router and the Internet

- The **router** is connected to a **modem**, which connects to your **Internet Service Provider (ISP)** — like Comcast, Verizon, etc.
- The ISP gives your home network a **public IP address** — this is how the outside world sees you.
- The router takes your laptop's request and sends it out into the internet using this public IP.

  (How does the sending out work?)

3. Finding the Website (DNS)

When you type a website like `www.example.com`, **your laptop doesn't know its IP address**, so it needs to find out.

But — and this is key — **your laptop does not directly talk to the DNS server on the internet.**

Instead:

1. Your **laptop sends a DNS query to your home router** (using your local IP, like `192.168.1.1`).
2. Your **router** then **forwards that request to a DNS server** — usually one from your ISP or something like Google DNS (`8.8.8.8`) or Cloudflare (`1.1.1.1`).
3. The **DNS server** responds with the IP address of the website, like `93.184.216.34`.
4. The **router** passes that response back to your laptop.

Full Explanation (Step by Step):

1. Your laptop wants to load `www.example.com`

It doesn't know the IP, so it sends a **DNS request packet** to the router.

2. The router forwards the DNS request

The router sends the request to the DNS server (usually via your ISP), asking "What IP address matches `www.example.com`?"

3. The DNS server responds

It replies with something like:

→ "`www.example.com` = `93.184.216.34`"

4. The router gives that IP to your laptop

Your router doesn't do anything else with it. It **passes that DNS response packet** back to your laptop.

At this point, your **laptop now knows** the IP address of the web server.

5. NOW your laptop creates the real website request

Your laptop says:

> *"I want to connect to 93.184.216.34 and get the web page."*

It creates a new **HTTP (or HTTPS)** request packet with the website's IP address as the destination. This is not part of the DNS process — this is the actual website request.

6. The router forwards that website request

The router does not open or understand the packet's contents — it just sees:

- Source: your laptop
- Destination: `93.184.216.34`

So the router sends that packet out to the internet via your ISP.

7. The server sends back the website data

The response from the website comes back in **packets** (HTML, images, CSS, etc.) to your public IP address.

8. The router sends those response packets to your laptop

The router sees that the data is meant for your laptop (using NAT and port tracking), so it delivers it there.

6. What Is in a Packet? (Simple Explanation)

A **packet** is like a digital envelope. It has two main parts:

Packet Header:

This is information about the packet, like:

- Who it's from (your IP address)
- Who it's going to (website IP)
- What type of data it has (web, video, etc.)
- What order it's in (packet 1 of 100, etc.)

Packet Payload:

This is the actual content being sent. For example:

- A part of a web page
- A piece of a YouTube video
- A request to open a specific website

If you're using **HTTPS**, the payload is **encrypted**, so nobody can read it except the server.

7. The Server Responds

- The web server sees the request, finds the page you want, and sends the data back in **more packets**.
- These packets follow the same path back through the internet to your router.
- The router then sends them to your laptop.

8. Your Laptop Reassembles the Packets

- Your laptop collects all the packets.
- It puts them in the right order using the info in the headers.
- It checks to make sure none are missing or broken.
- This is handled by the **TCP protocol**.

9. Your Browser Displays the Website

- Once all the packets arrive, your browser reads the data.
- It turns the code (HTML, CSS, JavaScript) into the visual website you see.
- Images, fonts, and videos might need extra packets, which the browser asks for automatically.

But, how does it work in the physical world?

Big Picture: The Internet Is Made of Cables

The internet is mostly **physical infrastructure**:

- Underground and underwater **fiber optic cables**
- Copper cables (older or for short distances)
- Routers, switches, and data centers that connect them

Those cables **literally carry your packets as electrical or light signals**.

1. Your Laptop connects to your Router

- Usually through **Wi-Fi** or **Ethernet**
- The data is just **electrical signals** (Ethernet) or **radio waves** (Wi-Fi)
- These signals contain the binary data of your packets: 1s and 0s

2. Your Router connects to a wall socket

- That wall socket is wired to your **modem**
- The modem is the bridge between your home network and your ISP's network

What Is a Modem?

A **modem** is a device that stands between your **home** and your **Internet Service Provider (ISP)**.

The word "modem" comes from:

Modulator / Demodulator

That means:

- It **modulates** (changes) digital data into signals (light or electrical) to send it over cables
- And it **demodulates** signals it receives into digital data your router and devices can understand

Real-Life Example

When you get internet from your ISP, they **send data to your house** over:

- Coaxial cable (like for cable TV)
- DSL phone line
- Fiber optic cable

But your **router and devices don't speak that language**. They speak pure digital.

So the **modem is like a translator** between your ISP's system and your home.

Modem vs Router (Important Difference)

Device	What It Does
Modem	Connects your home to the internet (via your ISP)
Router	Shares that internet connection with all your home devices

Sometimes they're **combined into one box**, which is why it seems like the router just connects to the wall and gets internet. But technically, the **modem does the connection**, the **router does the sharing**.

3. The Modem converts digital data to a signal your ISP understands

Depending on your internet type, this conversion is different:

Internet Type	Signal Type	Cable Type
Cable (Coax)	RF signals (radio frequency)	Coaxial cable
DSL	Electrical signals over phone lines	Twisted-pair copper
Fiber	Pulses of **light** (laser or LED)	**Fiber optic cable**

4. The signal travels through the cable to your ISP's equipment

- This is usually a big cabinet in your neighborhood called a **local exchange, node**, or **DSLAM**.
- From there, it connects to **bigger routers and fiber optic cables** owned by your ISP.

So How Does a Packet Become a Real Signal?

A **packet** is just a chunk of digital data (1s and 0s).

To send it over a cable:

Step-by-step signal translation:

1. The packet data (binary: 101101010...) is passed to your modem.
2. The modem turns those bits into **modulated signals**: For coax or DSL, it turns them into varying voltages or radio frequencies; for fiber, it turns them into **light pulses** (light = 1, no light = 0).
3. These signals travel through the cables to the ISP.
4. At the ISP, another modem or optical receiver **reverses the process**: It reads the signal, rebuilds the binary data, and reassembles the packet.
5. The ISP's router then forwards that packet toward its destination on the internet.

How the Internet Communication Happens When You Load a Website:

1. **Laptop sends a DNS request to the router:** "What's the IP address of `www.example.com`?"
2. **Router forwards DNS request to your ISP:** Your ISP either answers from its cache or forwards the request up the DNS hierarchy (to big DNS providers like Google DNS, Cloudflare, etc.).
3. **DNS server finds the IP address:** It looks up `www.example.com` → `93.184.216.34` (example IP).
4. **ISP sends the IP address back to the router:** Router receives the IP and passes it back to your laptop.
5. **Laptop creates the actual website request:** Sends an HTTP/HTTPS request packet destined for `93.184.216.34`.
6. **Router forwards the request to the ISP:** ISP sends it over the internet through many interconnected networks.

7. **The website's server receives the request:** Processes it and sends the website data back in packets.
8. **Packets travel back to your ISP and then your router:** Router receives the packets and sends them to your laptop.
9. **Laptop reassembles the packets:** Using TCP to check order, completeness, and errors.
10. **Web browser displays the website:** HTML, images, scripts load, and you see the page.