Modem vs Router (and Why Your Router Gets Botnetted)

Episode 010 study guide · Network+ / Security+ · netsecviz.net

In one sentence: *The modem translates your ISP's line into usable internet, the router shares and guards that one connection for your whole home, and because the router is an always-on computer facing the public internet, it is a favorite target for botnets like Mirai.*

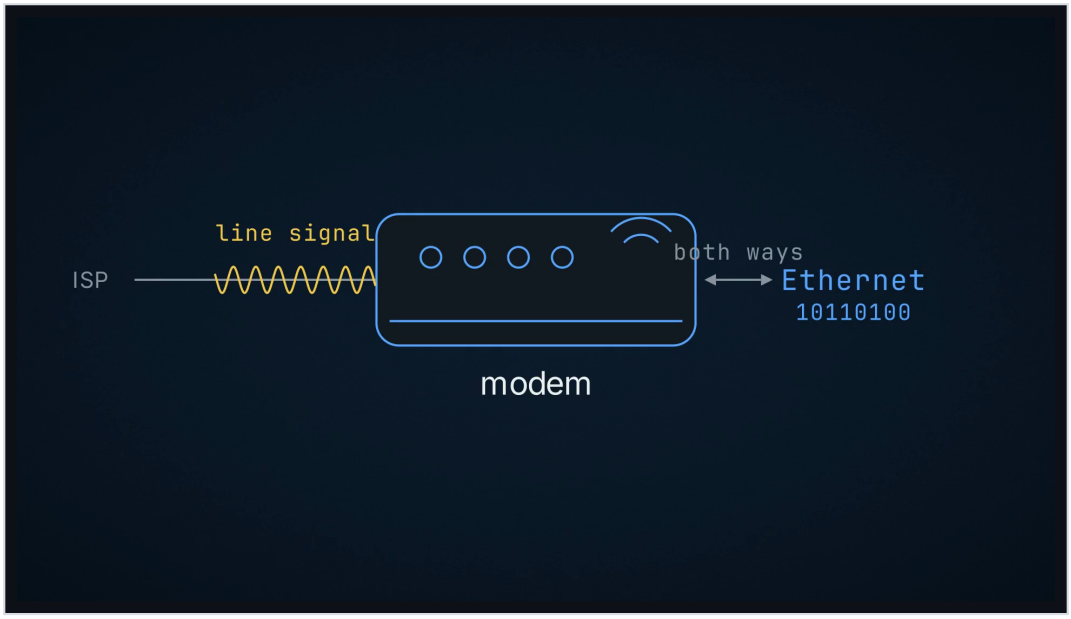
Two boxes sit between your home and the entire internet. Most people cannot say which one does what, or that they are two different jobs even when they live in the same plastic case. This guide walks the mechanism first (modem, router, and the combo box), then the attack: why the router gets hijacked, how the 2016 Mirai botnet did it with nothing more than default passwords, and the short list of settings that stop almost all of it.

Everything here maps to Network+ (device roles, NAT, DHCP, firewalls) and Security+ (botnets, DDoS, IoT hardening).

1. The modem: your translator to the ISP

In one sentence: *The modem converts between your ISP's physical line signal and the Ethernet your devices speak, giving your home a single connection to the internet.*

Modem is short for modulator-demodulator, and that is literally the job. Your internet provider does not deliver data as clean digital bits. It sends it as a signal tuned to the physical line: radio frequencies over a coax cable, pulses of light over fiber, or tones over an old phone line. Your laptop cannot read any of that directly. The modem sits at the boundary and converts between that line signal and the Ethernet your devices actually use, in both directions. By itself, a modem gives you exactly one connection to the internet, and nothing else.



the modem converts the ISP line signal to and from Ethernet.

WHAT TO REMEMBER

Modem = the translator between the ISP's line (coax, fiber, or phone) and Ethernet. One job, one connection.

COMMON MISCONCEPTION

That the modem "gives you Wi-Fi." It does not. A bare modem gives you a single wired connection; the Wi-Fi and the home network come from the router.

2. The router: one connection, shared and guarded

In one sentence: *The router takes the modem's single public connection and turns it into a private network for all your devices, doing four distinct jobs at once.*

One connection is not enough, because you have a dozen devices that all want online at the same time. That is the router. Its WAN port (wide area network side) plugs into the modem and receives one public IP address from your ISP, the single address the rest of the internet sees you as. From there it does four distinct jobs:

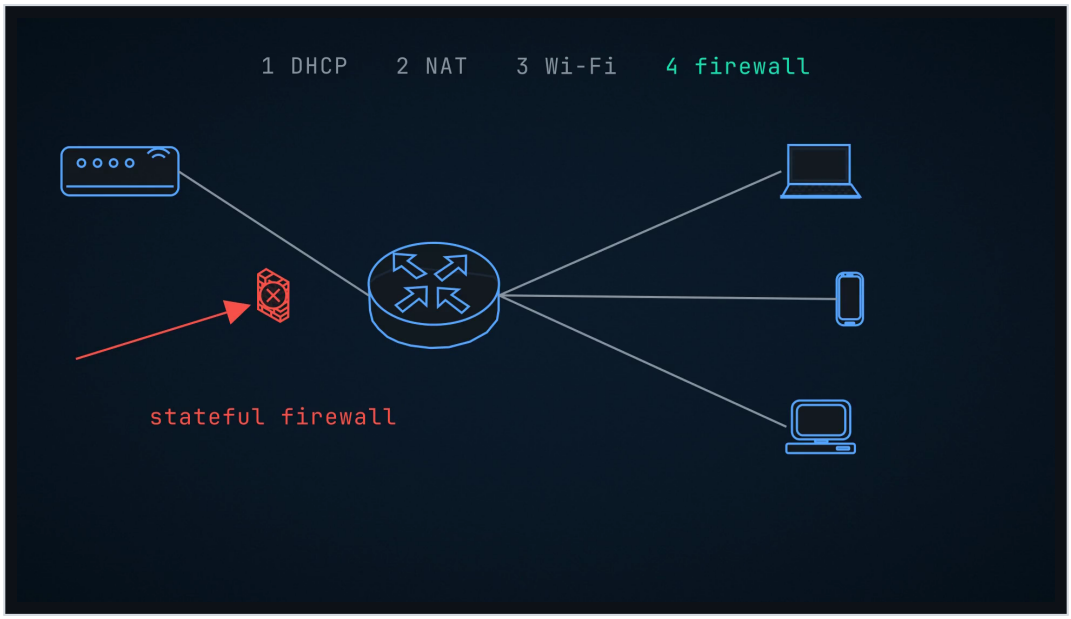
1. It builds your local network and assigns every device its own private address, using DHCP.

2. It lets all of those devices share that one public IP by rewriting addresses on the way in and out, which is NAT.

3. It broadcasts the Wi-Fi.

4. It runs a stateful firewall that, by default, drops connections coming from the internet that nobody inside asked for.

Routing itself just means forwarding each packet toward the right destination. So the modem is the door to the internet, and the router is the hallway, the rooms, and the doorman inside the house.



the router's four jobs, with the stateful firewall dropping unrequested inbound traffic.

WHAT TO REMEMBER

Router = WAN port takes one public IP, then DHCP (private addresses), NAT (share the public IP), Wi-Fi, and a stateful firewall (drops unrequested inbound).

GO DEEPER

"Stateful" means the firewall remembers connections your devices start, so replies to those are allowed back in, while unsolicited inbound is dropped. This default-deny on inbound is why your laptop is not directly reachable from the internet, and it is the first thing that gets weakened when someone opens ports or enables UPnP.

COMMON MISCONCEPTION

That NAT is a security feature. NAT is address sharing; the protection comes from the stateful firewall that usually rides alongside it. Do not rely on NAT alone as a security boundary.

3. The combo box (gateway)

In one sentence: *Most ISPs hand you a single unit that is both a modem and a router, called a gateway, trading control for convenience.*

Most people do not actually own two boxes. Your ISP probably gave you one unit that does both jobs, a modem and a router in a single case, usually called a gateway. It is convenient: one thing to plug in. The

trade-off is control. You cannot replace the modem half or the router half on its own, you usually get a stripped-down settings page, and if the box fails, both jobs fail with it. It is still two devices. They are just sharing a shell.

a gateway is a modem and a router in one case.

WHAT TO REMEMBER

A gateway (combo box) is a modem and a router in one case. Convenient, but less control and a single point of failure.

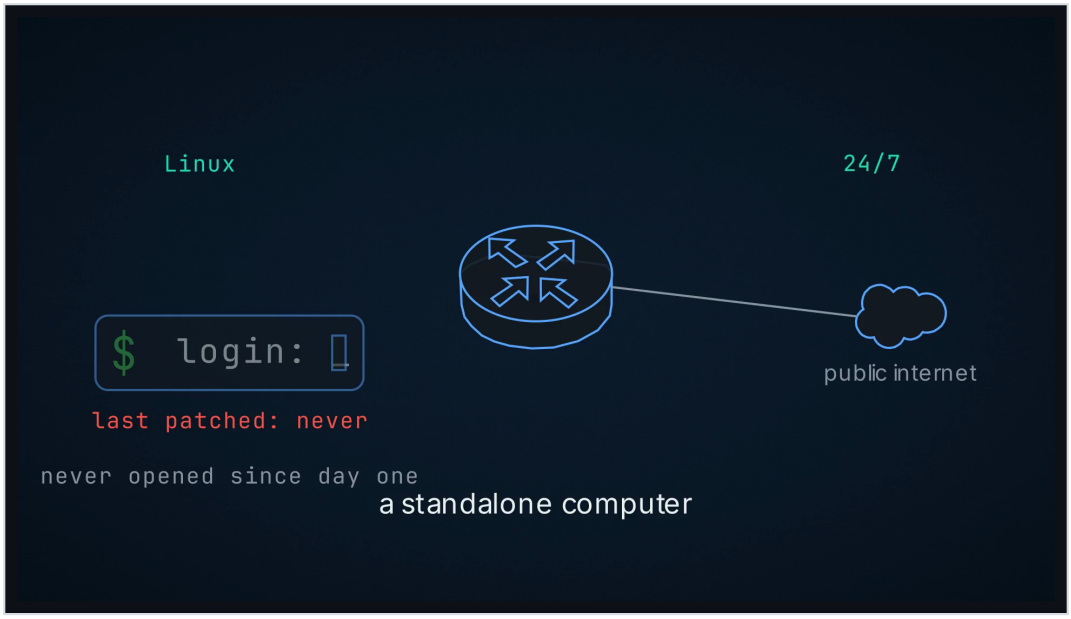
GO DEEPER

Many combo boxes let you switch the router half into "bridge mode," which turns off its routing/NAT/Wi-Fi so you can put your own router behind it. Useful when the ISP unit's firmware is weak or rarely updated.

4. Why your router is a target

In one sentence: *Your router is a standalone computer running an operating system 24/7, wired straight to the public internet, that almost nobody logs into, patches, or thinks about.*

Here is the thing nobody tells you: that router is a standalone computer. It runs its own operating system, usually Linux, twenty-four hours a day, wired straight to the public internet. But unlike your laptop, you never log into it, never patch it, and never think about it. Most people have not opened its settings since the day it was plugged in. A powerful, exposed computer that everyone ignores. Attackers do not ignore it.



the router is a standalone Linux computer, exposed and unpatched.

> **WHAT TO REMEMBER**
>
> The router is an always-on, internet-facing computer that is rarely patched and often still on its default password. That combination is exactly what makes it a target.

5. Mirai and the default password

In one sentence: *Attackers do not break into routers, they log in, using the default passwords the devices shipped with.*

They do not break in. They log in. Back in 2016, the malware called Mirai swept the internet for routers with Telnet open on port 23, then tried about sixty default logins, like admin/admin or root/1234. For most routers, just one works. And when the password does not, newer variants walk in through a known, unpatched vulnerability instead. There is no alarm and no broken lock. Just a login, and the router now belongs to the botnet.

Mirai brute-forces Telnet on port 23 with about sixty default logins.

WHAT TO REMEMBER

Mirai scans the internet, brute-forces Telnet (port 23) with about 60 hard-coded default credentials, and for unpatched devices falls back to known vulnerabilities. The way in is a login, not an exploit.

GO DEEPER

Telnet is an old remote-login service that sends everything, including passwords, in the clear, and many devices shipped with it on by default. That is why it is step one for a scanner. The fix on your side is to disable Telnet and remote administration entirely.

COMMON MISCONCEPTION

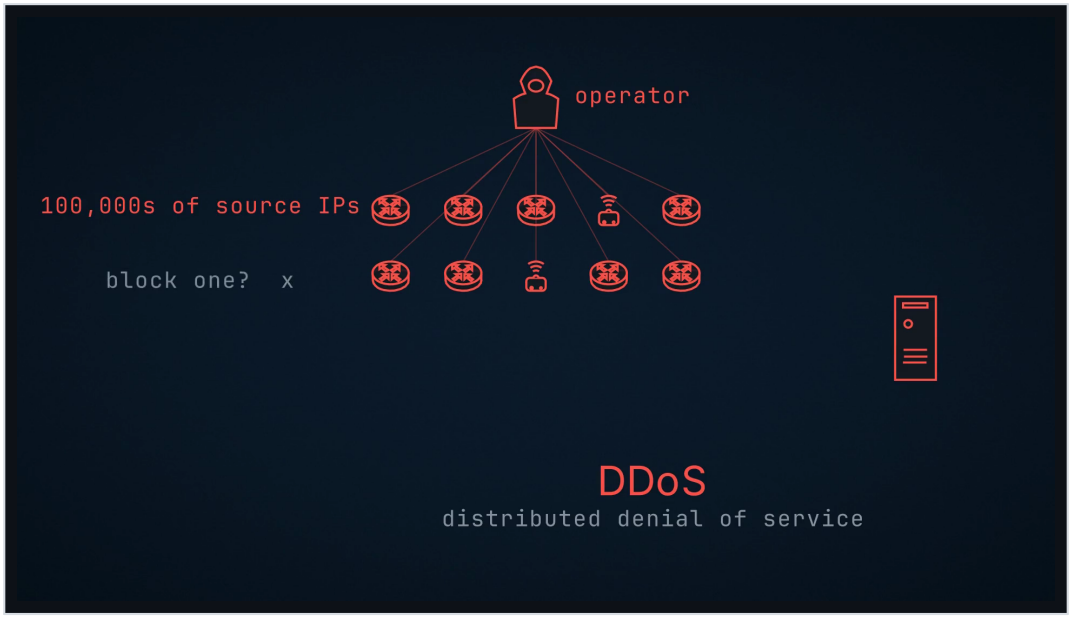
That you have to be a target to be a victim. Mirai does not pick you; it scans the entire internet indiscriminately and takes whatever answers with a default password or a known hole.

6. Botnets and the DDoS

In one sentence: *A botnet is a network of hijacked machines taking orders from one operator, and its favorite weapon is a distributed denial-of-service flood.*

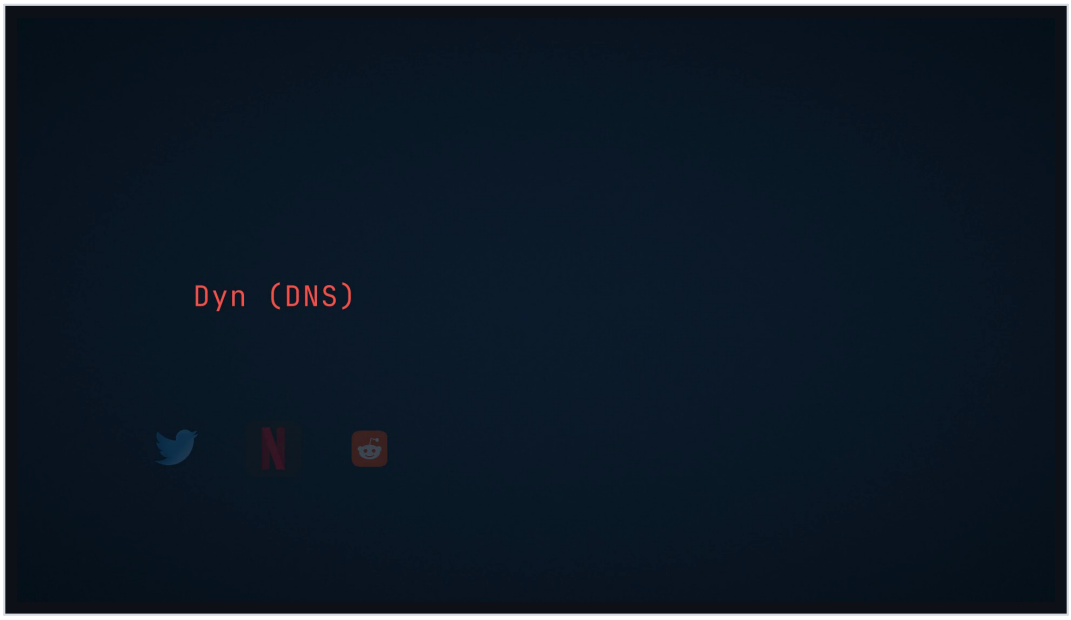
A botnet is a network of hijacked machines all taking orders from one operator. Here is the unsettling part: nothing on your end looks wrong. Your Wi-Fi still works, your router still routes. It is just moonlighting. Then the operator sends a single command, and every device in the botnet floods one target at the same instant. That is a DDoS, a distributed denial-of-service attack. "Distributed" is the load-bearing word: the traffic comes from hundreds of thousands of different addresses at once, so the victim cannot just block one

attacker. These attacks have pushed past a hundred gigabits per second.



one operator commands a botnet to flood a single target from hundreds of thousands of addresses.

In 2016, one Mirai botnet aimed at Dyn, a company that ran DNS for much of the internet. By taking down Dyn, it dragged Twitter, Netflix, and Reddit down with it. Mirai's source code leaked publicly that same year, which is why new variants are still hijacking routers today.



the Dyn attack took DNS offline, and with it Twitter, Netflix, and Reddit.

WHAT TO REMEMBER

Botnet = many hijacked machines under one operator. DDoS = they all flood one target at once, from too many addresses to block. The 2016 Mirai attack on Dyn (a DNS provider) took major sites offline.

GO DEEPER

Because Dyn ran DNS, taking it down did not "hack" Twitter or Netflix directly. It stopped their names from resolving to numbers, so users could not reach them. This is the tie-in to episode 002: a hijacked router can also silently change your DNS and send your whole house to fake sites.

COMMON MISCONCEPTION

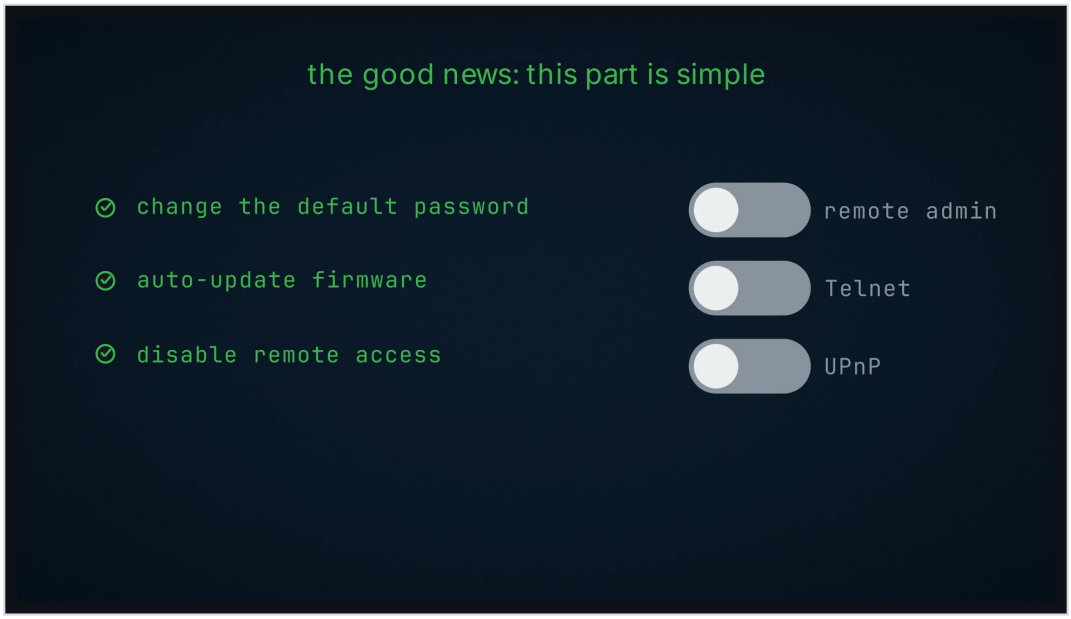
That a botnetted router looks broken. It works normally the whole time; that is the point. The attack traffic is a small side job you would never notice.

7. The fixes

In one sentence: *A short list of boring settings stops almost all of this, starting with changing the default password.*

The defenses are boring on purpose, and they work:

1. Change the default admin password. That one step alone stops most of Mirai.
2. Turn on automatic firmware updates, so known vulnerabilities get patched.
3. Disable remote administration, Telnet, and UPnP unless you actually need them.
4. If your router is old enough that the manufacturer has stopped shipping updates, retire it, because it will not get safer.



change the default password, auto-update firmware, and disable remote admin, Telnet, and UPnP.

WHAT TO REMEMBER

Change the default password, auto-update firmware, disable remote admin / Telnet / UPnP, and replace end-of-life routers. The single highest-impact step is changing the default password.

GO DEEPER

UPnP (Universal Plug and Play) lets devices on your network open inbound ports on the router automatically. Convenient for some games and apps, but it can punch holes through the very firewall that protects you, so turn it off unless you know you need it.

Glossary

- **Modem** Modulator-demodulator; converts your ISP's line signal (coax, fiber, phone) to and from the Ethernet your devices use.
- **Router** The device that shares one internet connection with all your devices and builds the local network.
- **Gateway / combo box** A single unit that is both a modem and a router.
- **WAN port** The wide area network side of the router; plugs into the modem and holds the public IP.
- **Public IP address** The single address your whole home shows to the internet.
- **Private IP address** A local address (like 192.168.x.x) used only inside your network.
- **DHCP** Dynamic Host Configuration Protocol; hands each device its own private address.
- **NAT** Network Address Translation; lets many devices share one public IP by rewriting addresses.
- **Stateful firewall** Filters traffic by connection state; drops inbound connections nobody inside requested.
- **Ethernet** The standard wired signal/format local devices use to communicate.
- **Firmware** The router's built-in software, which needs security updates.
- **Telnet** An old remote-login service (port 23) that sends data in the clear; a common brute-force target.
- **Default credentials** The factory login a device ships with (admin/admin, root/1234), that owners rarely change.
- **CVE** A published, catalogued software vulnerability (for example, in unpatched router firmware).
- **Mirai** 2016 malware that hijacks routers and IoT devices via default passwords and known flaws.
- **Botnet** A network of hijacked devices controlled by one operator.
- **DDoS** Distributed denial-of-service; flooding a target with traffic from many devices at once.
- **UPnP** Universal Plug and Play; auto-opens ports on the router, a common exposure to disable.
- **Dyn** A DNS provider whose 2016 outage from a Mirai DDoS took major sites offline.

Quick self-test

1. What does a modem do, and what does a bare modem give you by itself?
2. Name the four jobs a router does after its WAN port receives one public IP.
3. What is the difference between a modem, a router, and a gateway?
4. Why is a router an attractive target compared to your laptop?
5. How did Mirai actually get into routers in 2016?
6. What does "distributed" add in a distributed denial-of-service attack?
7. Why did taking down Dyn knock Twitter, Netflix, and Reddit offline?
8. List the four defenses, and name the single most important one.

Further reading

- CISA, "Heightened DDoS Threat Posed by Mirai and Other Botnets" (Alert TA16-288A).
- Krebs on Security, "DDoS on Dyn Impacts Twitter, Spotify, Reddit" (October 21, 2016).
- Help Net Security, "New Mirai variants target routers and DVRs" (2026), on variants still active today.
- CompTIA Network+ objectives: NAT, DHCP, firewalls, and network device roles.
- CompTIA Security+ objectives: botnets, DDoS, and IoT/embedded device hardening.