Flashcards — Modem vs Router

Episode 010 · cut along the lines, or import NetSecViz-010-Flashcards.csv into Anki (Front/Back).

Q What does a modem do?
A Converts your ISP's physical line signal (coax, fiber, or phone) to and from the Ethernet your devices use.

Q What does a bare modem give you?
A A single connection to the internet, and nothing else (no Wi-Fi, no local network).

Q What does 'modem' stand for?
A Modulator-demodulator.

Q What does a router do?
A Takes the modem's one connection and shares it with all your devices, building and guarding the local network.

Q What is the router's WAN port?
A The wide area network side; it plugs into the modem and receives one public IP from your ISP.

Q Name the router's four jobs.
A DHCP (private addresses), NAT (share the public IP), Wi-Fi, and a stateful firewall.

Q What does DHCP do?
A Hands each device on your network its own private IP address.

Q What does NAT do?
A Lets many devices share one public IP by rewriting addresses on the way in and out.

Q Is NAT a security feature?
A No. NAT is address sharing; the protection comes from the stateful firewall alongside it.

Q What does a stateful firewall do?
A Allows replies to connections your devices start, and drops inbound connections nobody inside requested.

Q What is a gateway (combo box)?
A A single unit that is both a modem and a router.

Q Trade-off of a combo box?
A Convenience for control: you cannot upgrade the halves separately, settings are limited, and one failure kills both jobs.

Q What is bridge mode?
A It disables a combo box's router half so you can put your own router behind it.

Q Why is a router a target?
A It is an always-on, internet-facing computer that is rarely patched and often still on its default password.

Q What OS do most routers run?
A Usually Linux.

Q How did Mirai get into routers?
A It scanned the internet and brute-forced Telnet (port 23) using about sixty default logins.

Q What port does Telnet use?
A Port 23.

Q Give two default logins Mirai tried.
A admin/admin and root/1234 (about 60 in its list).

Q What if the default password was changed?
A Newer variants fall back to a known, unpatched vulnerability (CVE) to get in.

Q Do attackers 'break in' to routers?
A No, they log in. The way in is default credentials or a known hole, not a dramatic exploit.

Q What is a botnet?
A A network of hijacked machines all taking orders from one operator.

Q What is a DDoS?
A Distributed denial-of-service: many hijacked devices flood one target with traffic at the same time.

Q What was the 2016 Dyn attack?
A A Mirai botnet flooded Dyn, a DNS provider, taking Twitter, Netflix, and Reddit offline.

Q Why is Mirai still a threat today?
A Its source code leaked publicly in 2016, so new variants keep hijacking routers.

Q Name the four router defenses.
A Change the default password, auto-update firmware, disable remote admin/Telnet/UPnP, and retire end-of-life routers.

Q What should you do with an end-of-life router?
A Retire it. If the manufacturer stopped shipping updates, it will not get safer.

Q Does a botnetted router look broken?
A No. It works normally; the attack traffic is a hidden side job you would not notice.

Q Why does 'distributed' matter?
A Traffic comes from hundreds of thousands of addresses at once, so the victim cannot just block one attacker.

Q Why did hitting Dyn take down other sites?
A Dyn ran their DNS, so their names could no longer resolve to IP addresses.

Q Single most important router fix?
A Change the default admin password. That one step alone stops most of Mirai.

Q What is UPnP and why disable it?
A Universal Plug and Play auto-opens ports on your router; it can punch holes through your firewall, so turn it off unless needed.

Q How does a hijacked router relate to DNS?
A A compromised router can silently change your DNS, sending your whole house to fake sites (see episode 002).