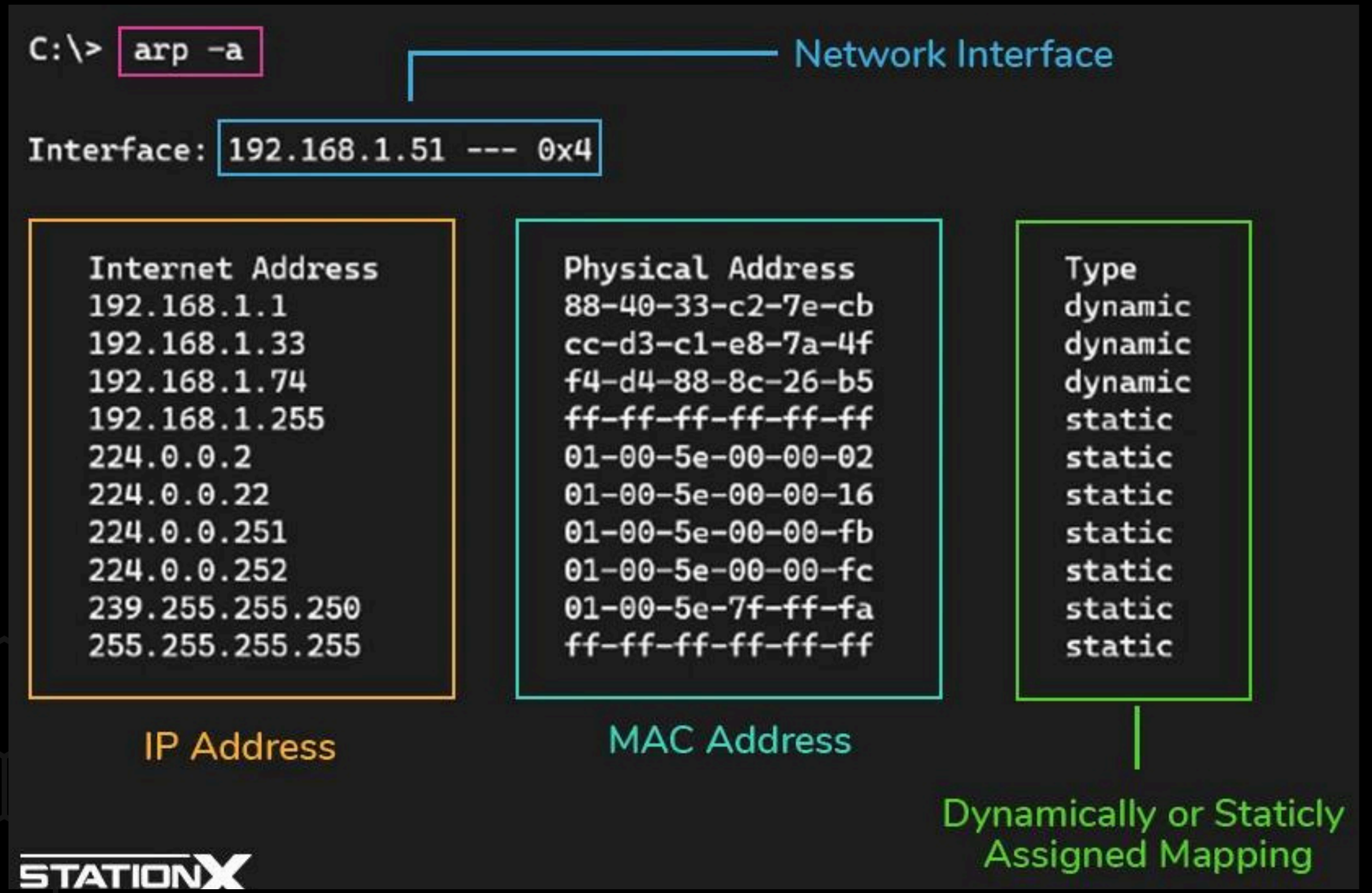
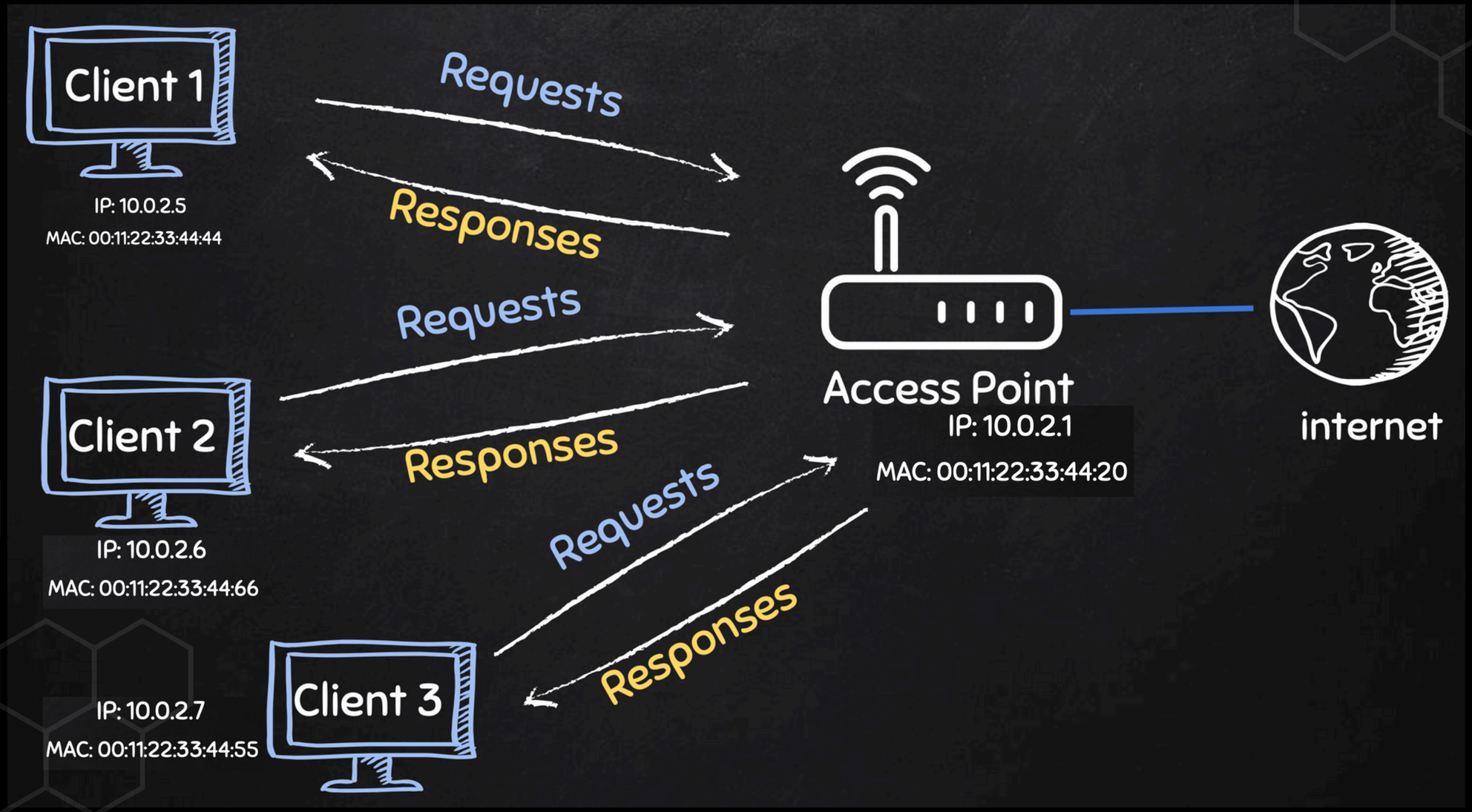
What is Address Resolution Protocol ?

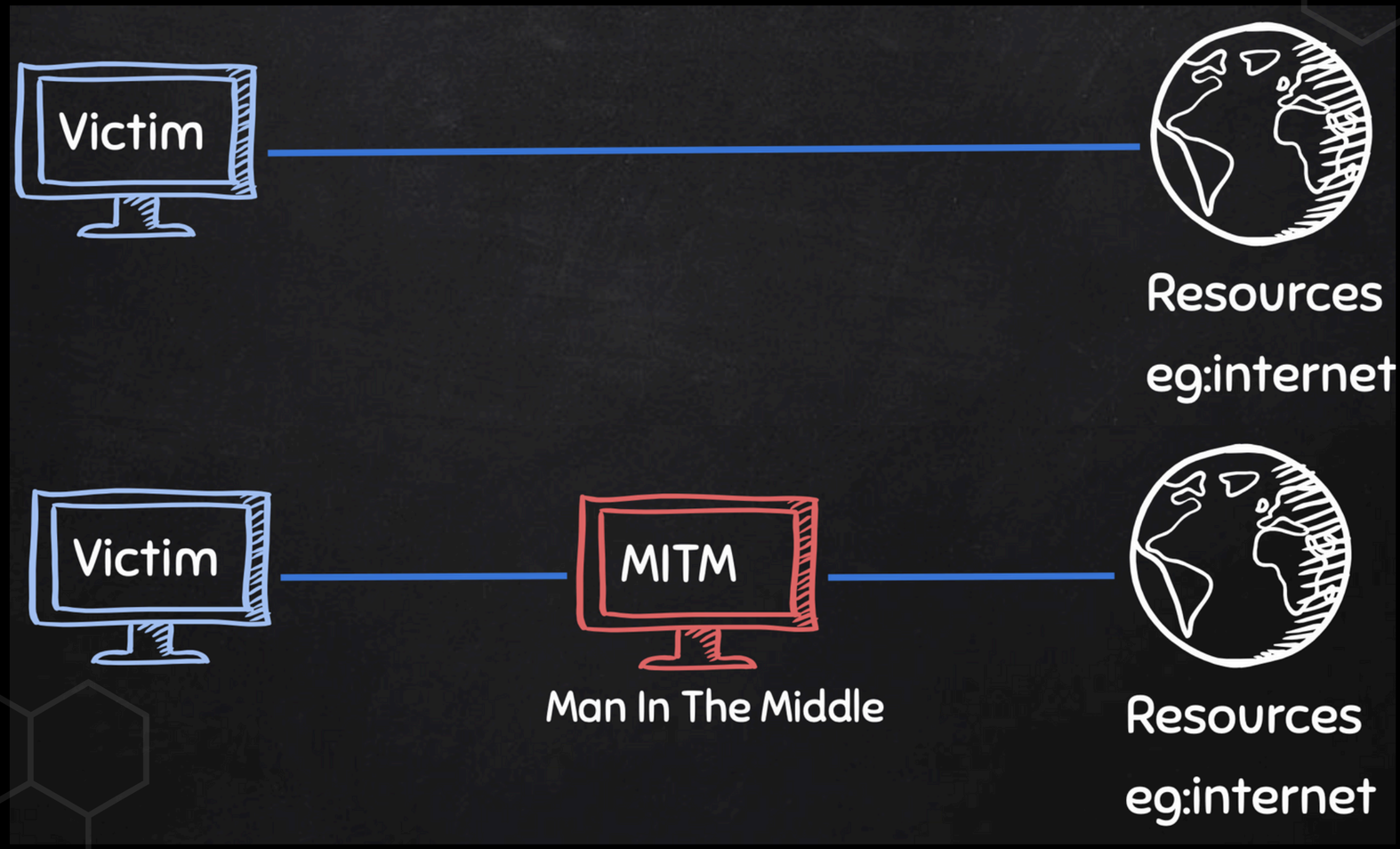
Simple protocol used to map IP Address of a machine to its MAC address.



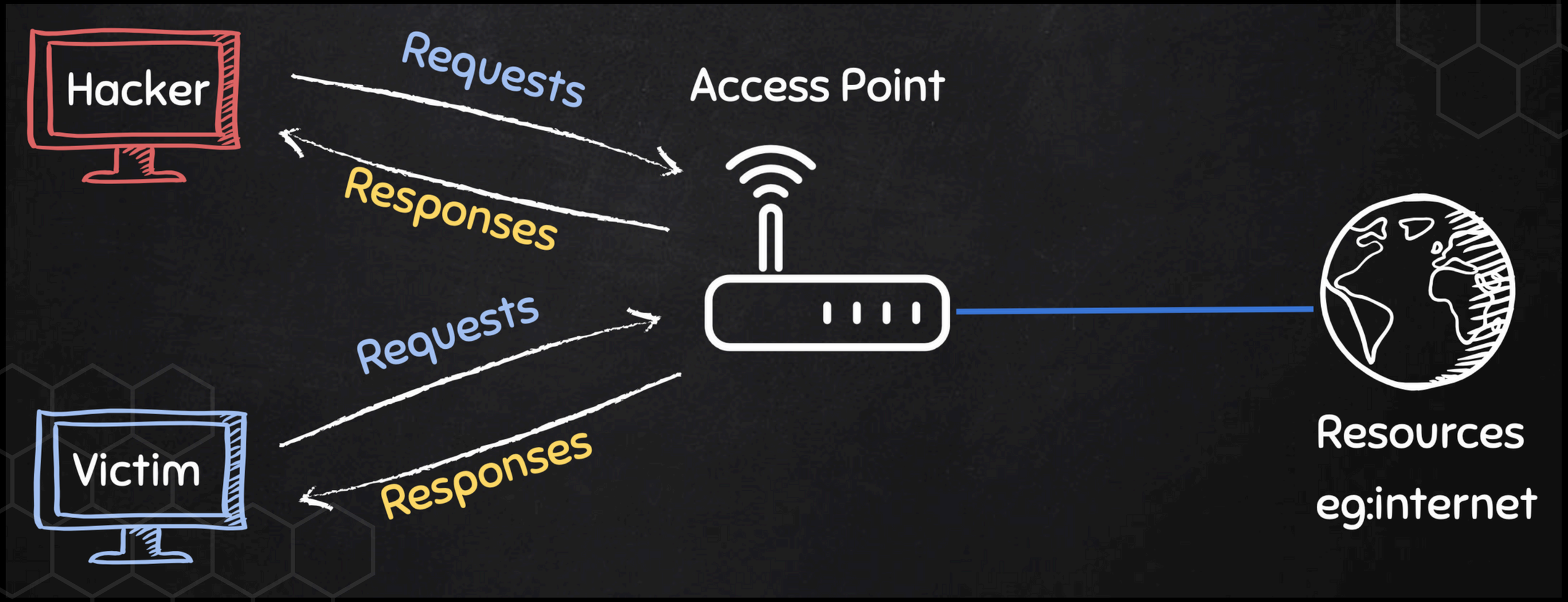
Typical Network

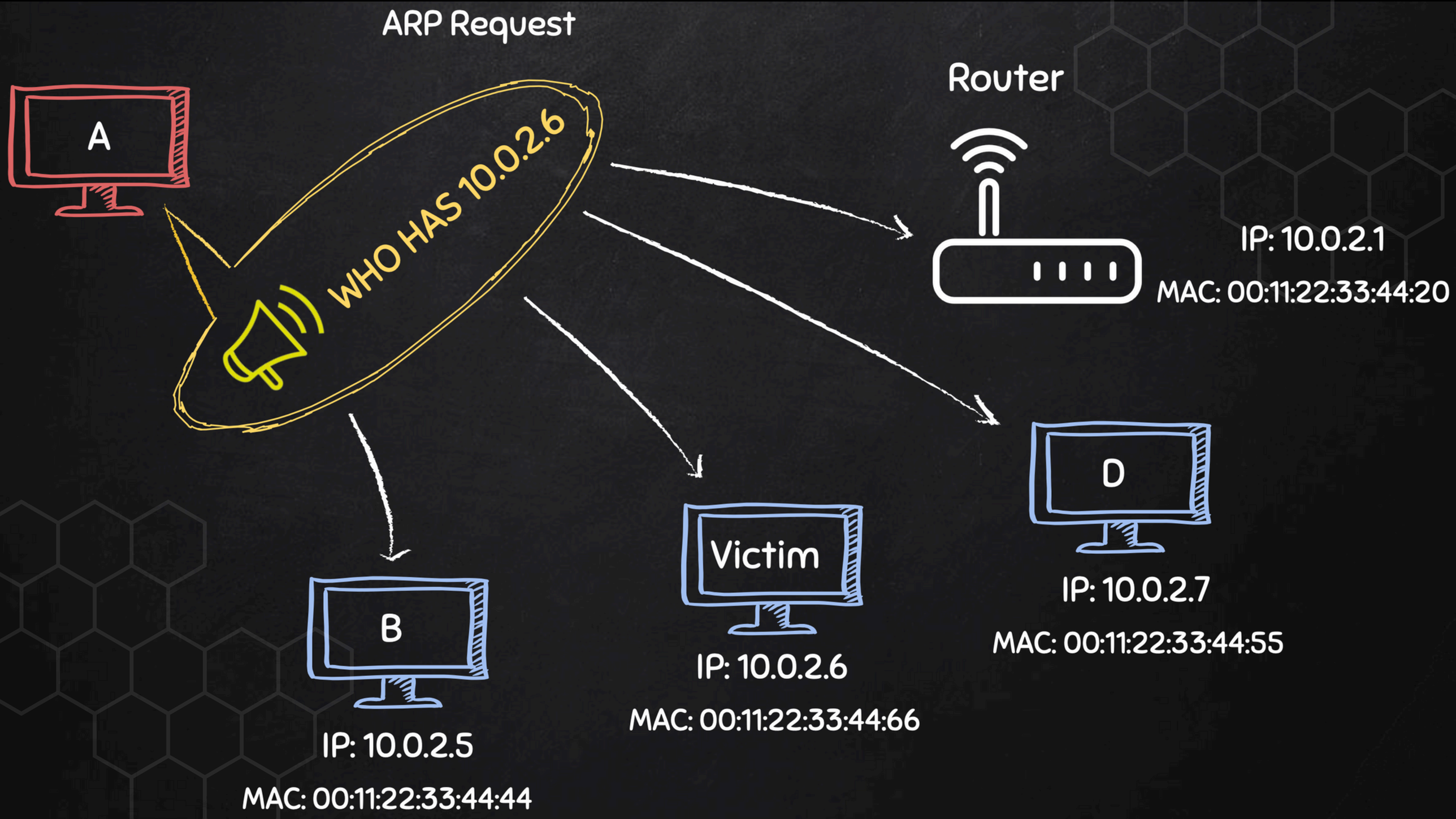


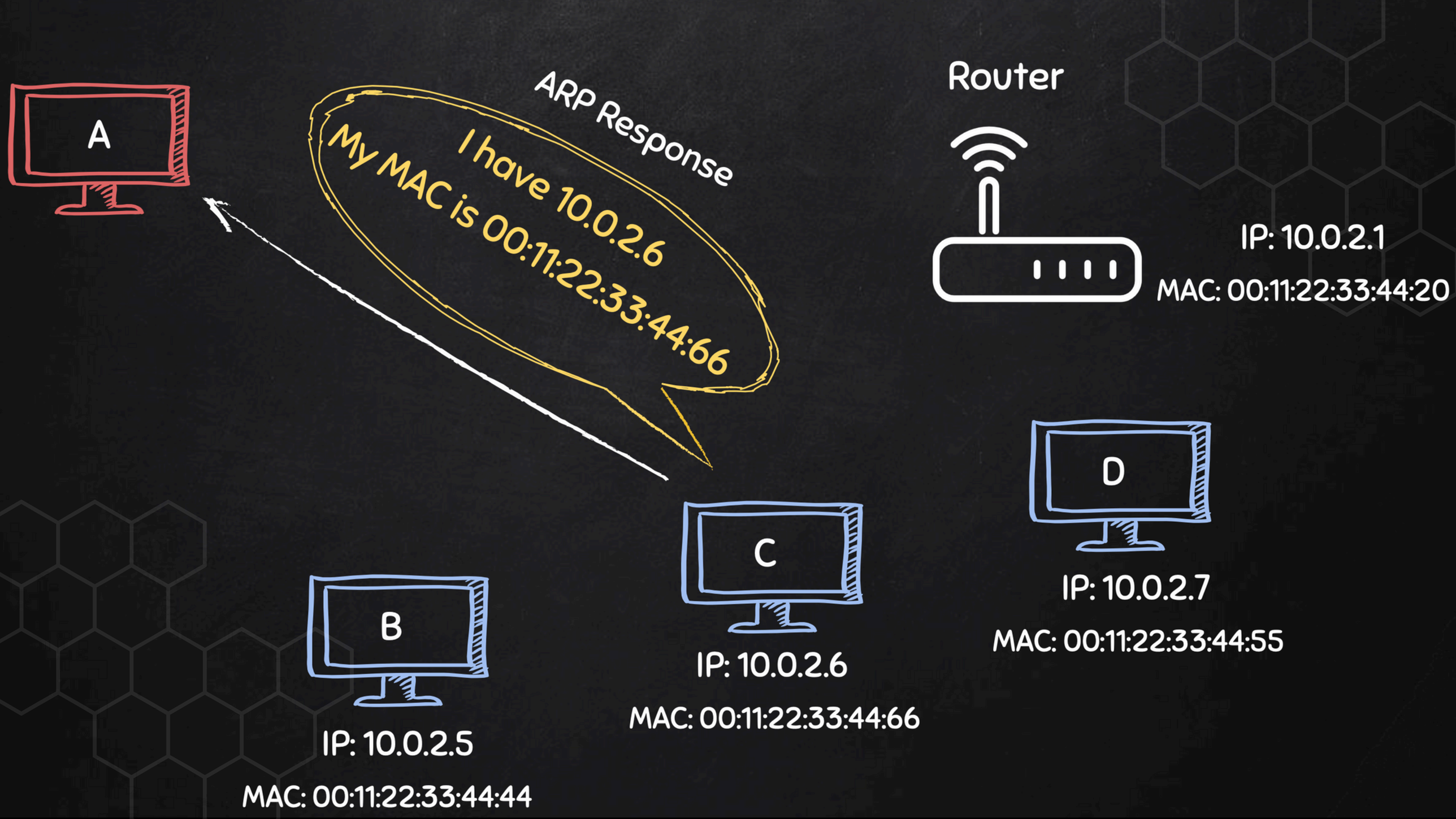
MITM Attacks



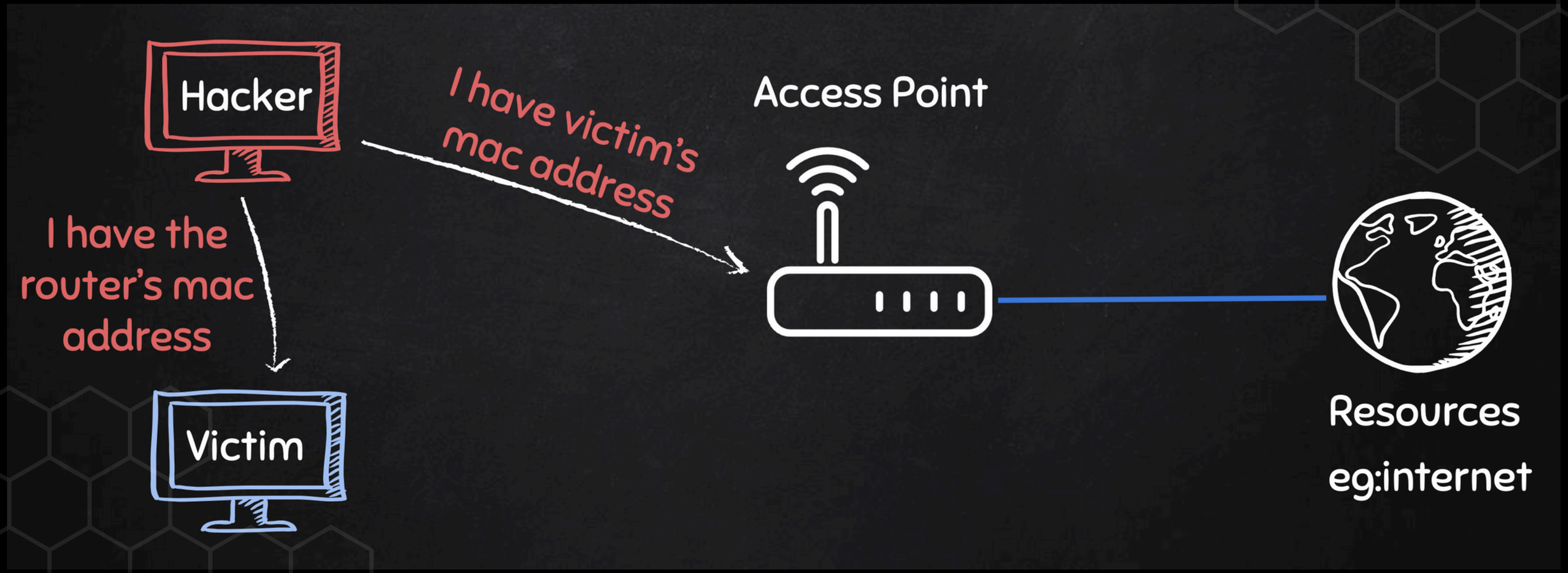
ARP Spoofing



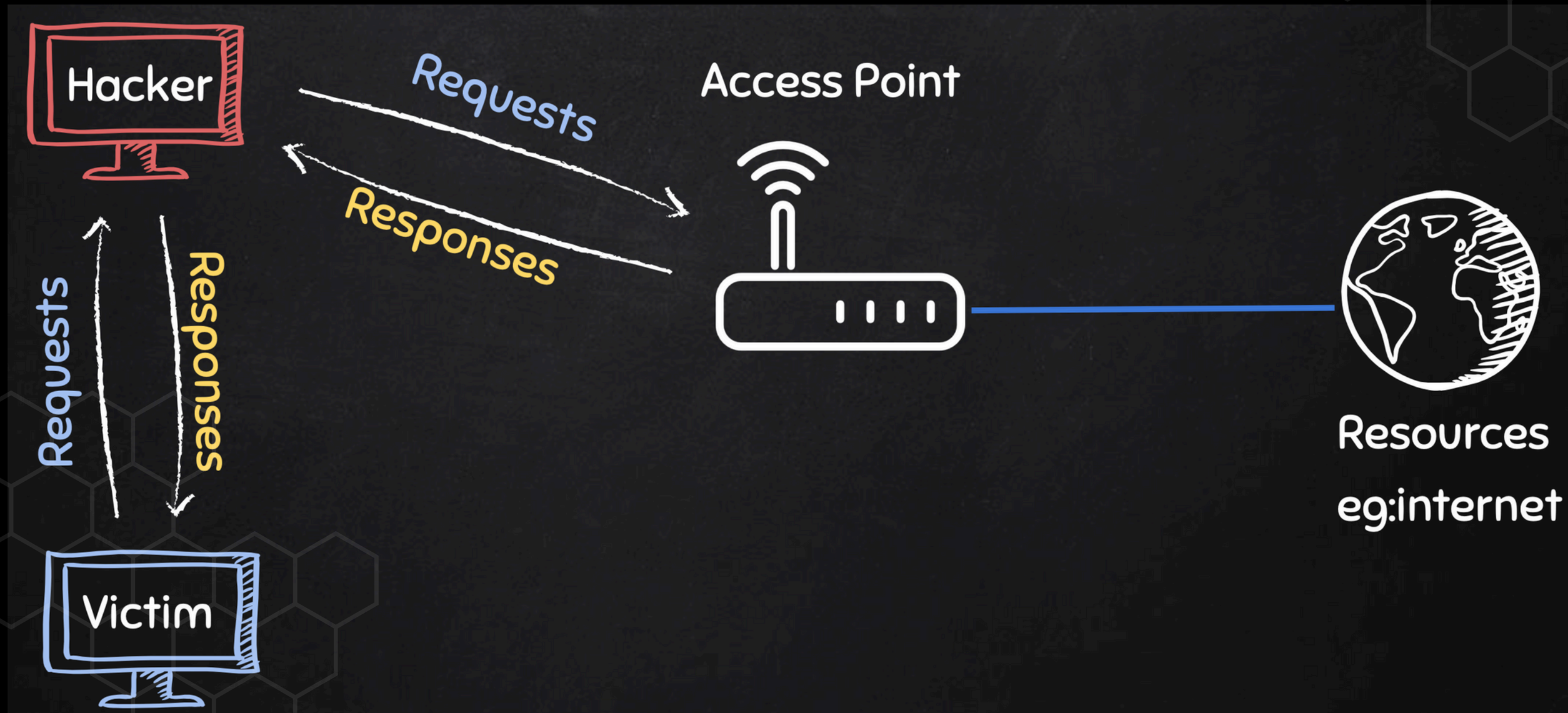

ARP Request
A
WHO HAS 10.0.2.6
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44
Victim
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55


A
ARP Response
I have 10.0.2.6
My MAC is 00:11:22:33:44:66
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55
C
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44

ARP Spoofing



ARP Spoofing



MITM Attacks

Attack Surface : **ARP spoofing**

Attack Vulnerabilities : (ARP)

- Stateless protocol: ARP operates without maintaining connection state.
- Automatic caching: Hosts cache all ARP replies, solicited or unsolicited.
- Overwriting entries: New ARP replies overwrite existing cache entries, even unexpired ones.
- Lack of authentication: ARP has no mechanism to verify the origin of received packets.

MITM Attacks

Attack Anatomy :

- Exploit lack of authentication: Send spoofed ARP messages on the LAN.
- Associate attacker's MAC with target's IP: Trick network into sending target's traffic to attacker.
- Intercept traffic: Receive packets intended for the target host.
- Choose attack vector:
  - Spying: Inspect packets, then forward to actual destination.
  - Man-in-the-middle: Modify data before forwarding.
  - Denial-of-service: Drop some or all intercepted packets.
- Maintain stealth: For spying or man-in-the-middle attacks, forward traffic to avoid detection.

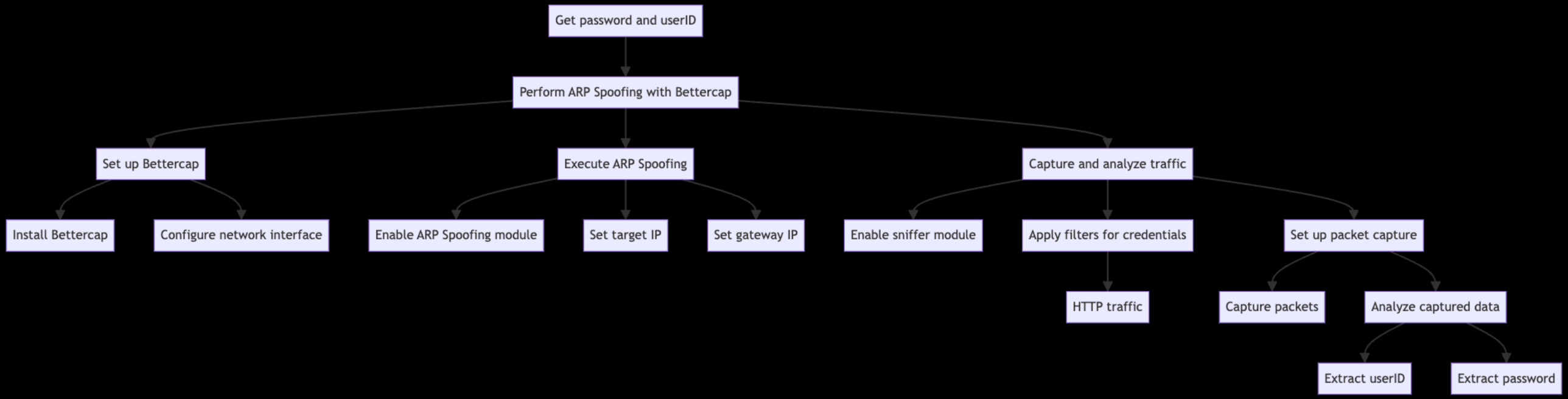
Demonstration Using ButterCap

- Framework to run network attacks.
- Can be used to :
  - ARP Spoof targets (redirect the flow of packets)
  - Sniff data (urls, username passwords).
  - Bypass HTTPS.
  - Redirect domain requests (DNS Spoofing).
  - Inject code in loaded pages.
  - And more!

use:

```
bettercap -iface [interface]
```

Attack Tree


Get password and userID
Perform ARP Spoofing with Bettercap
Set up Bettercap
Execute ARP Spoofing
Capture and analyze traffic
Install Bettercap
Configure network interface
Enable ARP Spoofing module
Set target IP
Set gateway IP
Enable sniffer module
Apply filters for credentials
Set up packet capture
HTTP traffic
Capture packets
Analyze captured data
Extract userID
Extract password

Common Vulnerability Scoring System

Exploitability Metrics:

1. Attack Vector: Network (N)
   - The attack is executed over the local area network.
2. Attack Complexity: Low (L)
   - Relatively simple to perform with readily available tools.
3. Privileges Required: Low (L)
   - Only requires access to the local network, no special privileges needed.
4. User Interaction: None (N)
   - The attack can be carried out without any action from the target user.
5. Scope: Changed (C)
   - The attack impacts not just the targeted system but potentially all network traffic.

Common Vulnerability Scoring System

Impact Metrics:

1. Confidentiality: High (H)
   - Allows unauthorized access to potentially sensitive network traffic.
   - Enables eavesdropping on communications meant for the target.
2. Integrity: High (H)
   - Permits modification of intercepted data before forwarding.
   - Enables man-in-the-middle attacks, allowing alteration of transmitted information.
3. Availability: High (H)
   - Can be used to conduct denial-of-service attacks by dropping packets.
   - May disrupt normal network operations and access to resources.

MITM Attacks
Detection & Prevention

Detection:

- **Analysing arp tables:** Flag sudden or unusual IP-to-MAC mapping changes
- **Multiple IP detection:** Flags multiple IPs associated with a single MAC address
- **Identify Unsolicited Replies:**
  - Look for ARP replies that don't have a matching request in recent traffic
  - Pay attention to replies sent to broadcast MAC address (ff:ff:ff:ff:ff:ff)
- **Wireshark:** This open-source tool can be used to discover ARP spoofing in large network.

MITM Attacks
Detection & Prevention

Prevention:

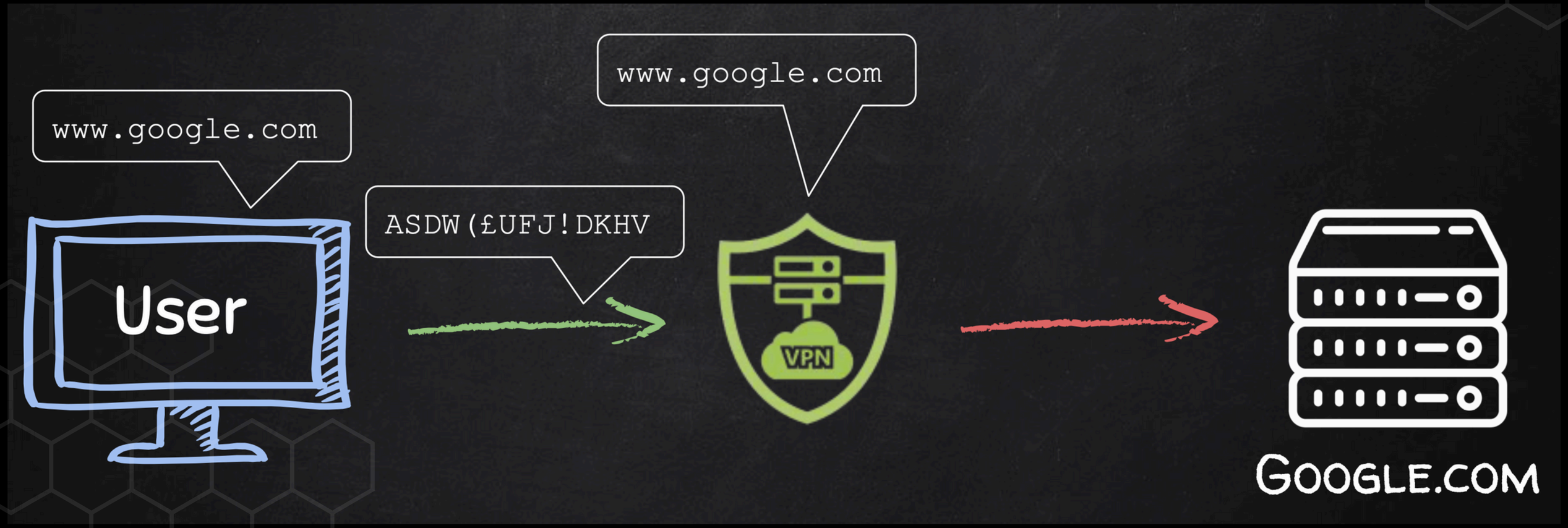
- **Always use HTTPS (HTTP Secure):** Encrypts data between your browser and the web server which Prevents attackers from reading or modifying transmitted data, even if they've successfully executed an ARP spoofing attack.
- **VPN (Virtual Private Network):**
  - Encrypts all network traffic, not just web browsing
  - Creates a secure tunnel from your device to the VPN serve
- **Kernel-level prevention:**
  - Tools like AntiARP for Windows
  - ArpStar module for Linux and some routers
- **Use Linksys routers:** Drops invalid packets that violate mapping, and contains an option to repoison or heal.

Prevention Table:

	Pros	Cons
HTTPS Everywhere	Free	– Only works with HTTPS websites. – Visited domains still visible. – DNS spoofing still possible.
VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free. – VPN provider can see data.
HTTPS Everywhere + VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free

VPN – Virtual Private Network

VPN - Virtual Private Network



VPN – Virtual Private Network

Benefits:

- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.
- Protection from hackers.

VPN – Virtual Private Network

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.
- Use HTTPS everywhere.
- Optional – pay with crypto.