

Evaluation Parts

- 1) Introduction (ARP, ARP Poisoning, attack surface, attack vulnerabilities and attack anatomy)**
- 2) Demonstration (bettercap application)**
- 3) Attack score (Attack Tree, Common Vulnerability Scoring System)**
- 4) Prevention and Detection (HTTPS, VPN)**

MITM ATTACK USING ARP POISONING

TEAM MEMBERS:

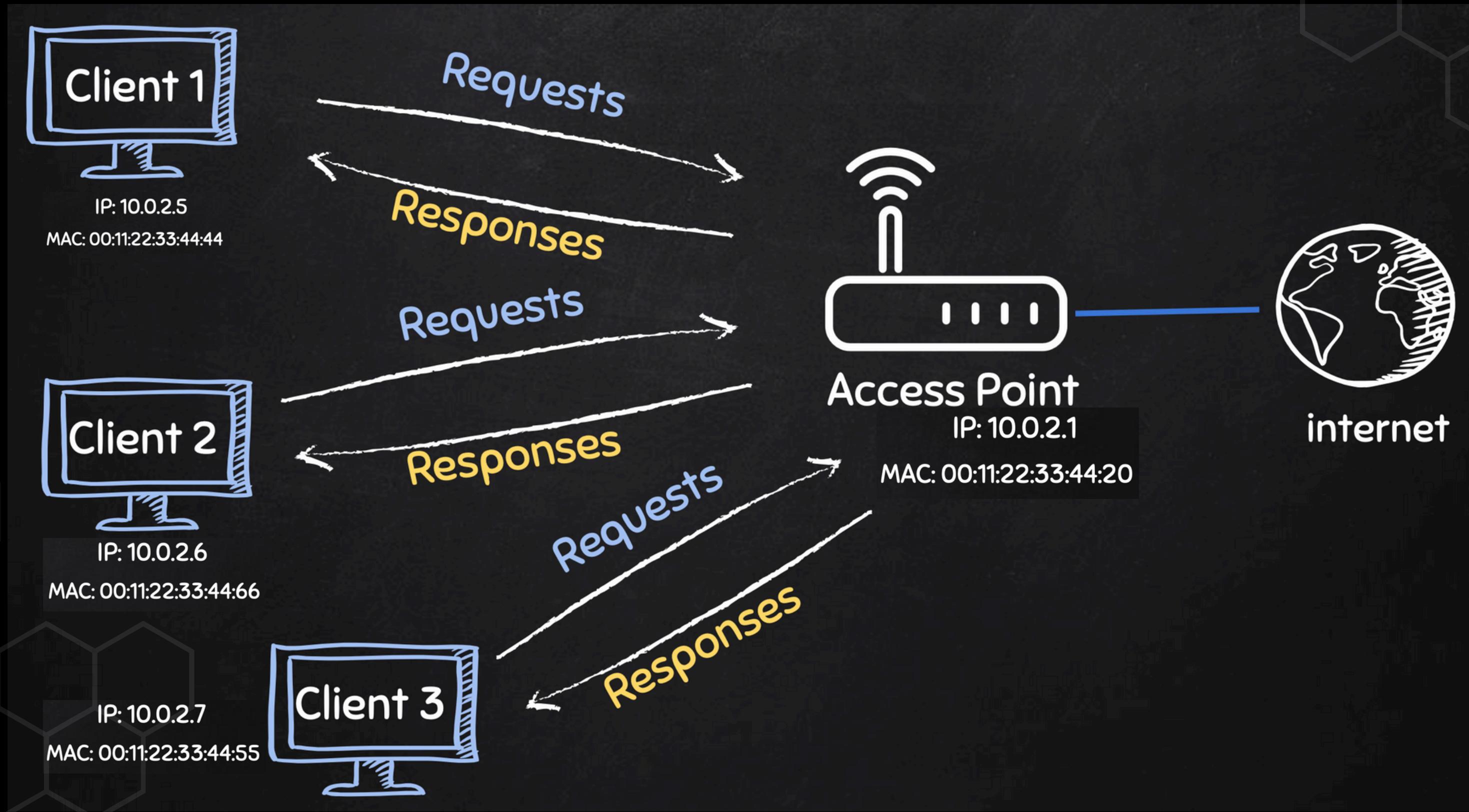
- Adarsh Singh (S20220010004)
- Himanshu Saraswat (S20220010082)
- DHARAWATH NAGESHWARI (S20220010061)
- ASHWIN KUMAR NAIK NENAVATH (S20220010152)

What is Address Resolution Protocol ?

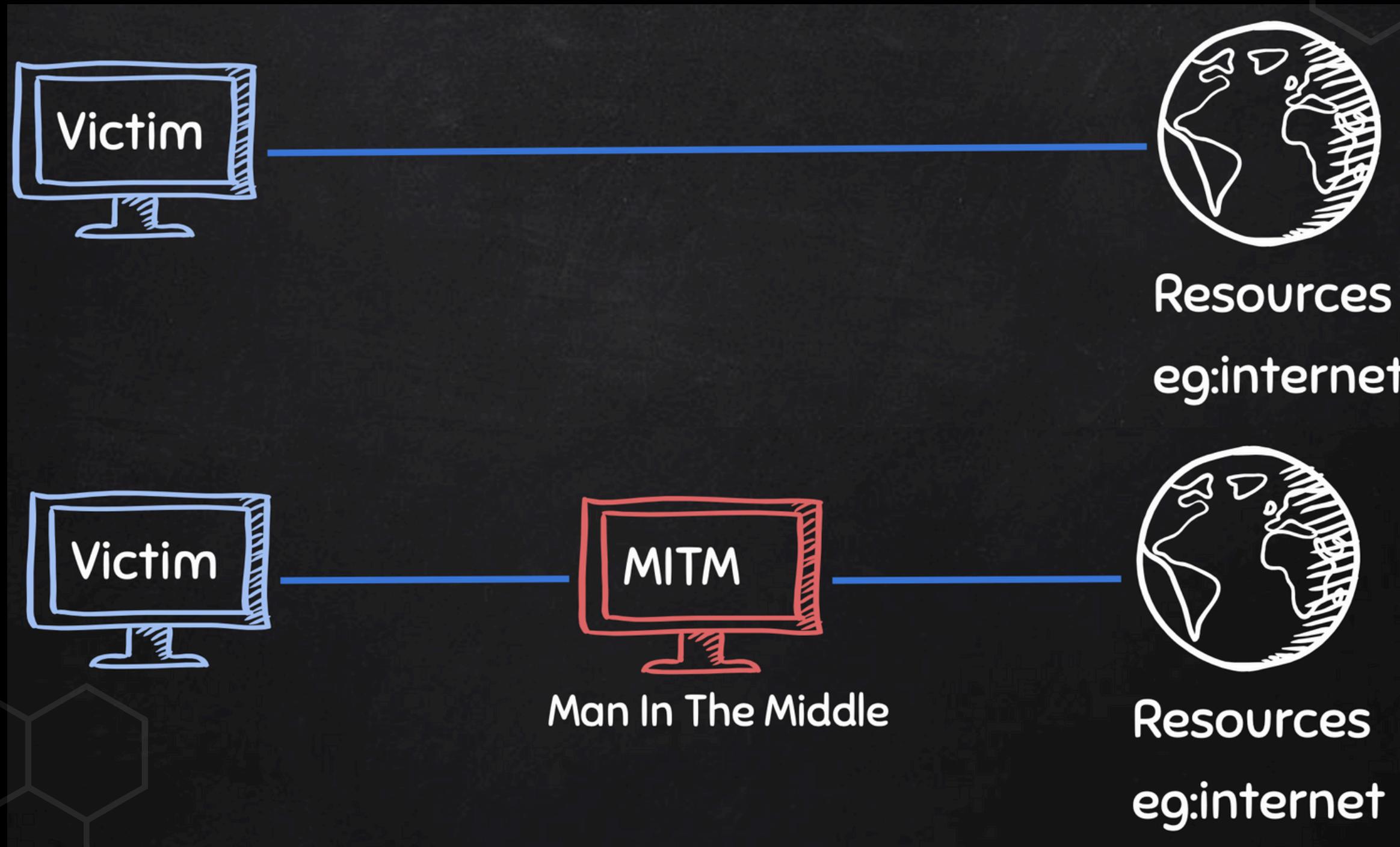
Simple protocol used to map IP Address of a machine to its MAC address.

C:\> arp -a		
Network Interface		
Interface:	192.168.1.51 --- 0x4	
Internet Address		
192.168.1.1		
192.168.1.33		
192.168.1.74		
192.168.1.255		
224.0.0.2		
224.0.0.22		
224.0.0.251		
224.0.0.252		
239.255.255.250		
255.255.255.255		
IP Address	MAC Address	Type
	88-40-33-c2-7e-cb	dynamic
	cc-d3-c1-e8-7a-4f	dynamic
	f4-d4-88-8c-26-b5	dynamic
	ff-ff-ff-ff-ff-ff	static
	01-00-5e-00-00-02	static
	01-00-5e-00-00-16	static
	01-00-5e-00-00-fb	static
	01-00-5e-00-00-fc	static
	01-00-5e-7f-ff-fa	static
	ff-ff-ff-ff-ff-ff	static
		Dynamically or Statically Assigned Mapping

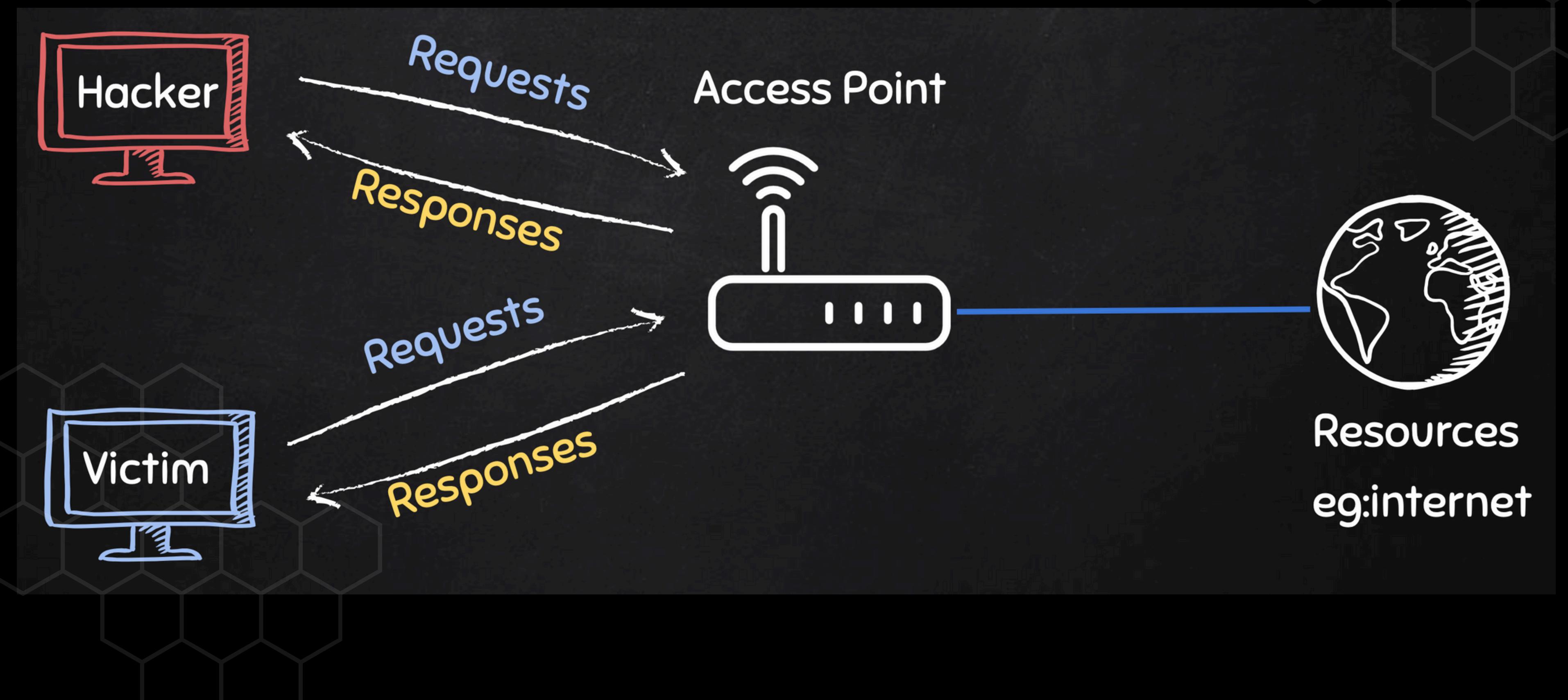
Typical Network



MITM Attacks



ARP Spoofing



ARP Request

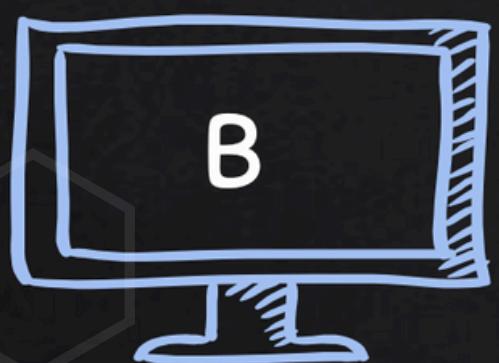


Router



IP: 10.0.2.1

MAC: 00:11:22:33:44:20



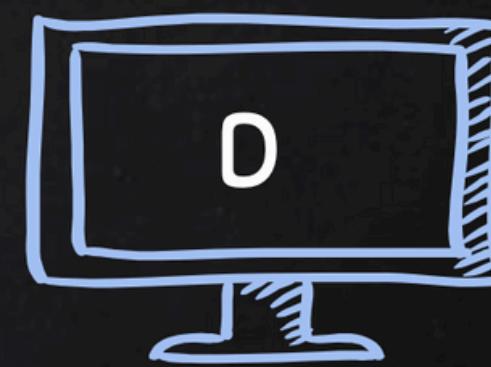
IP: 10.0.2.5

MAC: 00:11:22:33:44:44



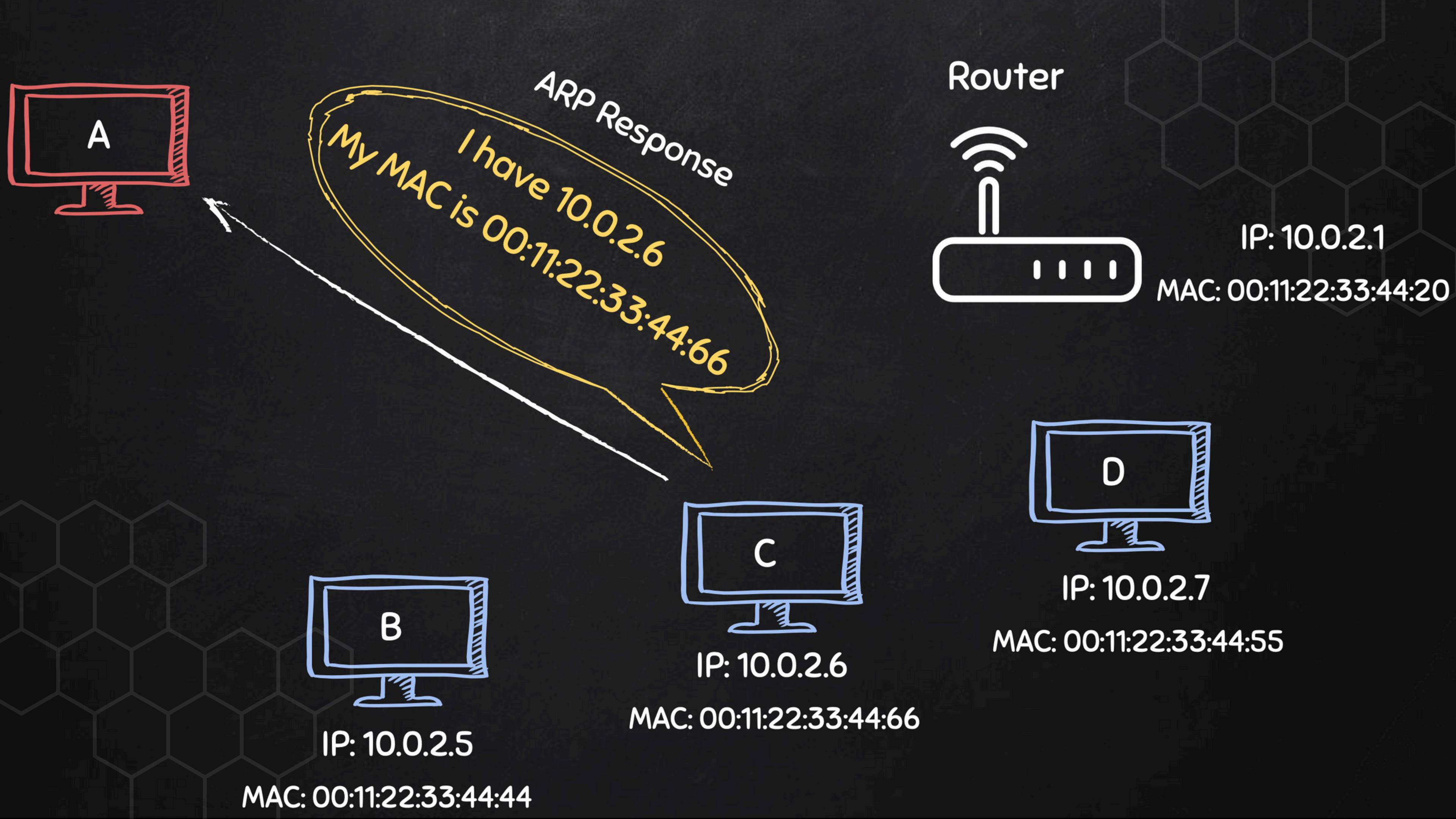
IP: 10.0.2.6

MAC: 00:11:22:33:44:66



IP: 10.0.2.7

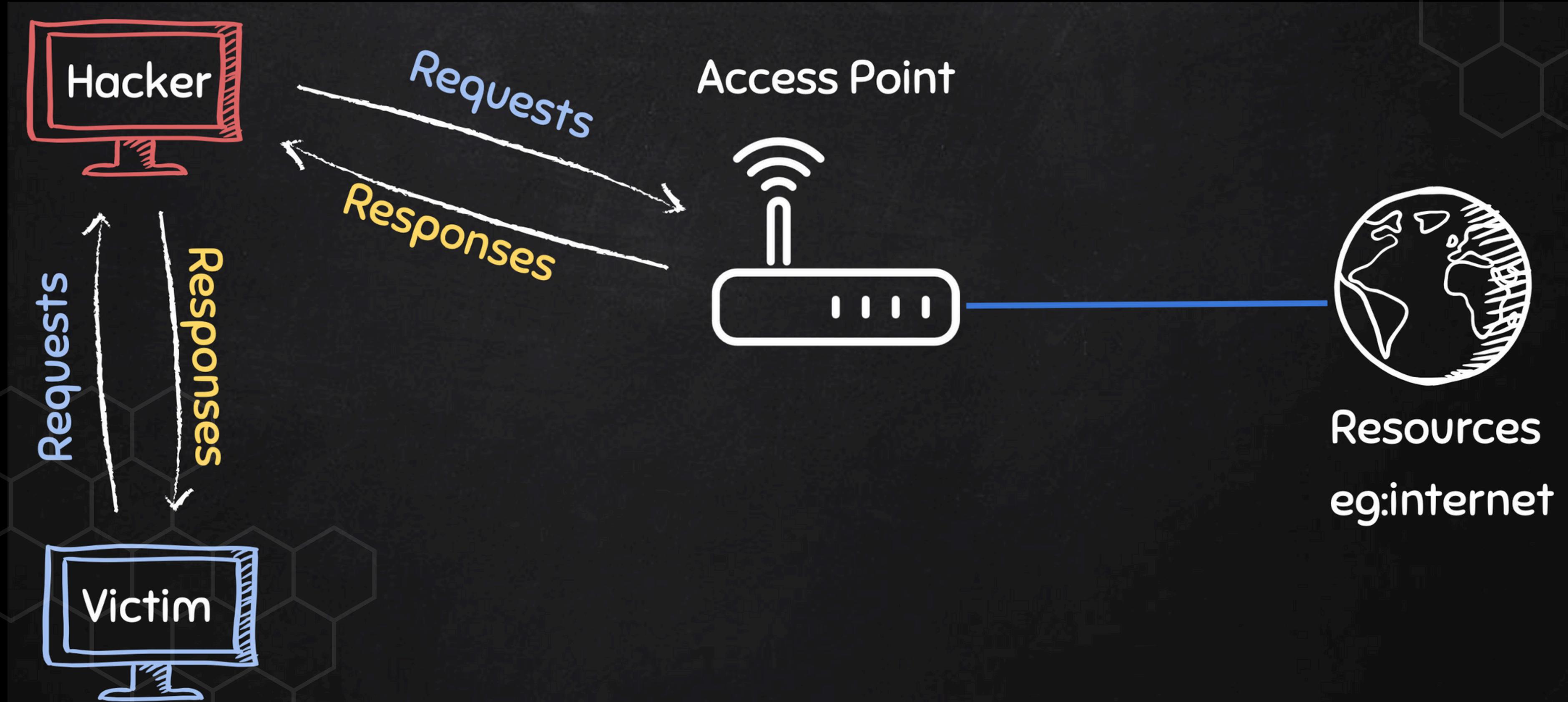
MAC: 00:11:22:33:44:55



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

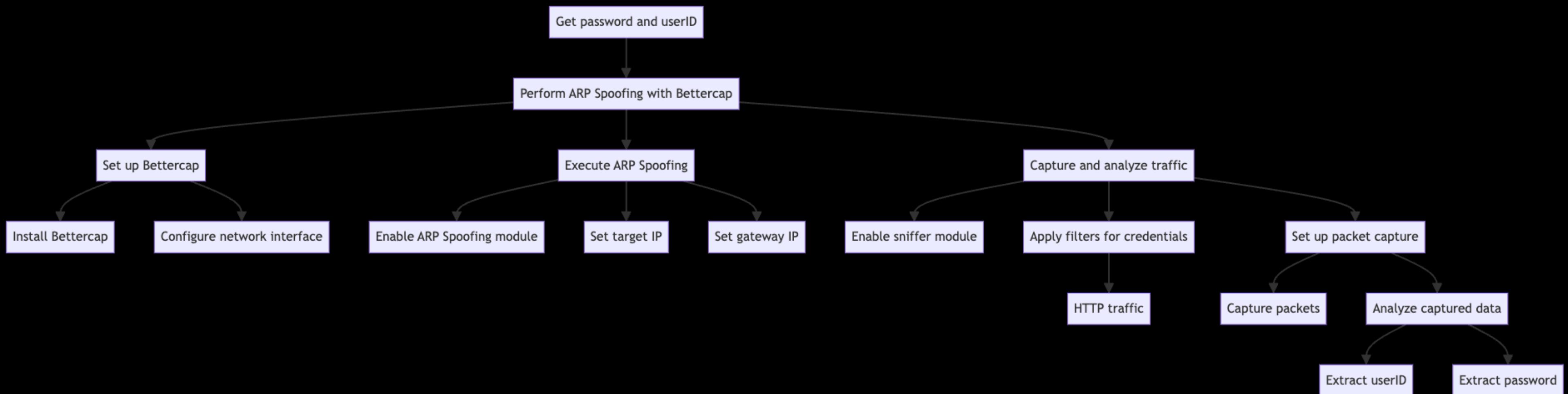
- Framework to run network attacks.
- Can be used to :
 - ARP Spoof targets (redirect the flow of packets)
 - Sniff data (urls, username passwords).
 - Bypass HTTPS.
 - Redirect domain requests (DNS Spoofing).
 - Inject code in loaded pages.
 - And more!

use:

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



Attack Tree



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

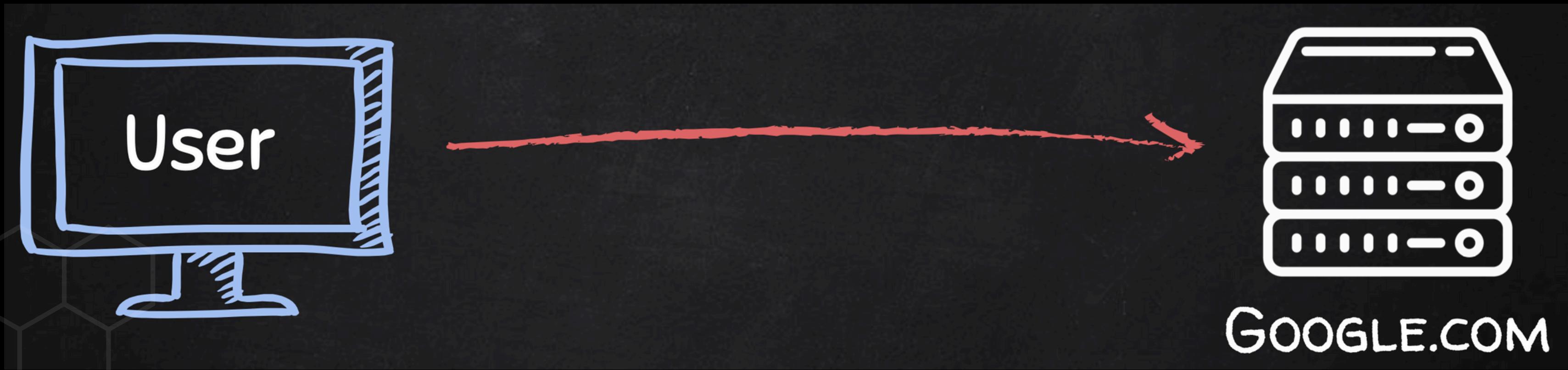
Prevention:

- **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 server
- **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 re poison or heal.

Prevention Table:

	Pros	Cons
HTTPS Everywhere	Free	<ul style="list-style-type: none">- Only works with HTTPS websites.- Visited domains still visible.- DNS spoofing still possible.
VPN	<ul style="list-style-type: none">- Encrypts everything.- Protects from all MITM attacks.	<ul style="list-style-type: none">- Not free.- VPN provider can see data.
HTTPS Everywhere + VPN	<ul style="list-style-type: none">- Encrypts everything.- Protects from all MITM attacks.	<ul style="list-style-type: none">- Not free

VPN - Virtual Private Network



VPN - Virtual Private Network



VPN - Virtual Private Network



Internet

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.