CSE 406 Project

ARP DoS via Gratuitous ARP storm

Members:
2005074 – Dipanta Kumar Roy Nobo
2005090 – Tawkir Aziz Rahman

Made with GAMMA

Understanding ARP Gratuitous Storm Attacks and Defence

This presentation will explore the vulnerabilities of the ARP protocol, detail attack methods like gratuitous ARP storms, and outline essential defence strategies to secure local networks. We'll cover the attack's impact and practical mitigation techniques.

What is ARP and Gratuitous ARP?

ARP Protocol

ARP (Address Resolution Protocol) is fundamental for IPv4 networks, mapping IP addresses to physical MAC addresses. This mapping allows devices to locate each other on a local network segment.

Gratuitous ARP

A gratuitous ARP is an unsolicited ARP reply, broadcast by a device to announce its IP-to-MAC address mapping. It's used for legitimate purposes like updating ARP caches or detecting IP conflicts.

Stateless Nature

A key vulnerability of ARP is its stateless nature; devices accept ARP replies and update their caches without verifying if a request was ever made, making them susceptible to malicious updates.

Made with GAMMA

ARP Gratuitous Storm Attack Explained

An ARP gratuitous storm attack involves an attacker flooding the local network with fake, unsolicited ARP replies. These malicious packets contain falsified IP-to-MAC mappings, causing network devices to update their ARP caches incorrectly.

1

Flooding the Network

The attacker sends a high volume of gratuitous ARP replies, rapidly saturating the network.

2

Cache Poisoning

Network devices, including switches and hosts, receive these fake replies and overwrite their legitimate ARP cache entries with the attacker's MAC address associated with various IPs.

3

Traffic Redirection

Consequently, traffic intended for legitimate devices (e.g., the default gateway) is redirected to the attacker's machine, enabling Man-in-the-Middle (MITM) attacks.

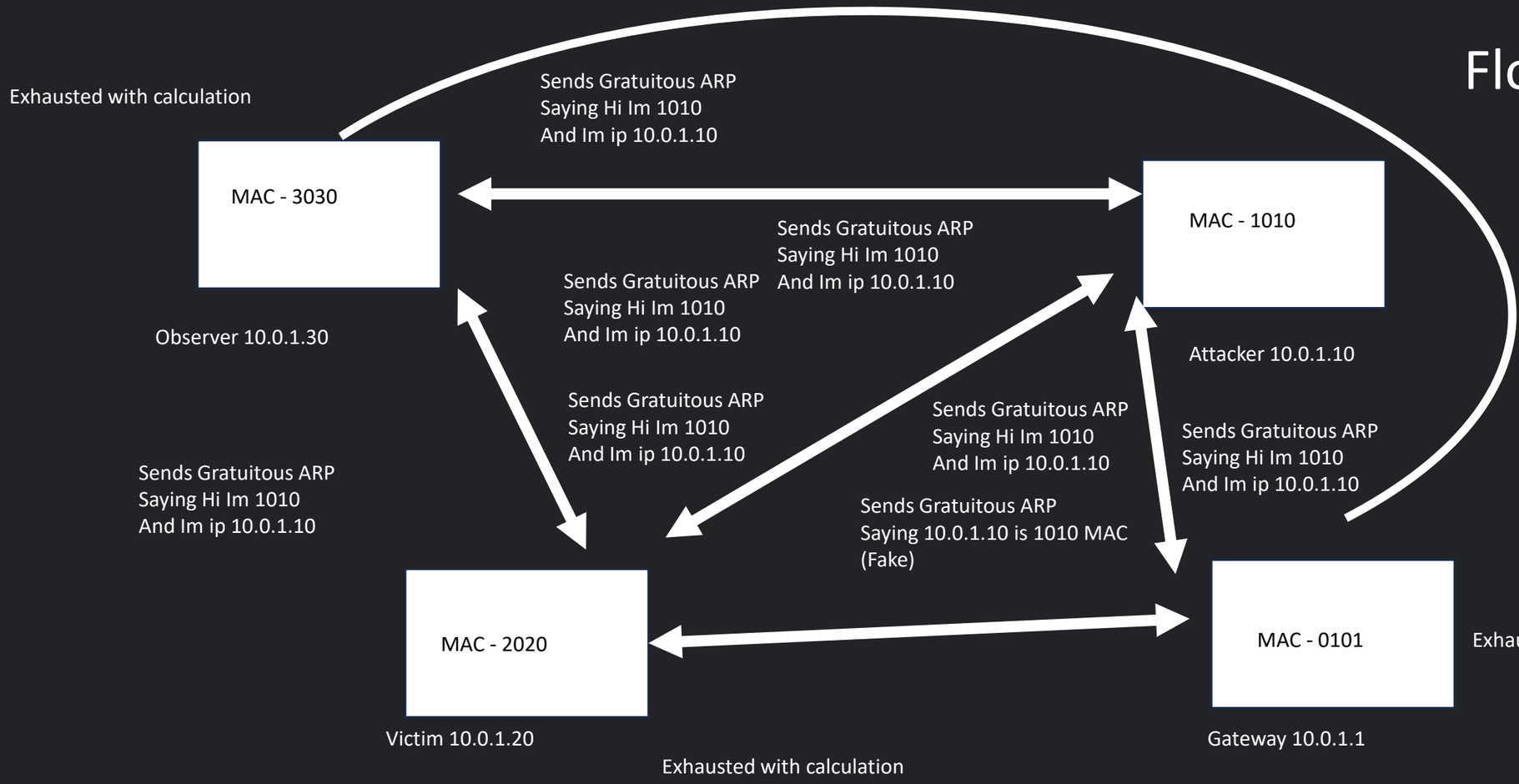
4

Denial of Service (DoS)

The sheer volume of forged ARP traffic can overwhelm network devices and hosts, leading to network disruption and denial of service.

Made with GAMMA

Flooding attack



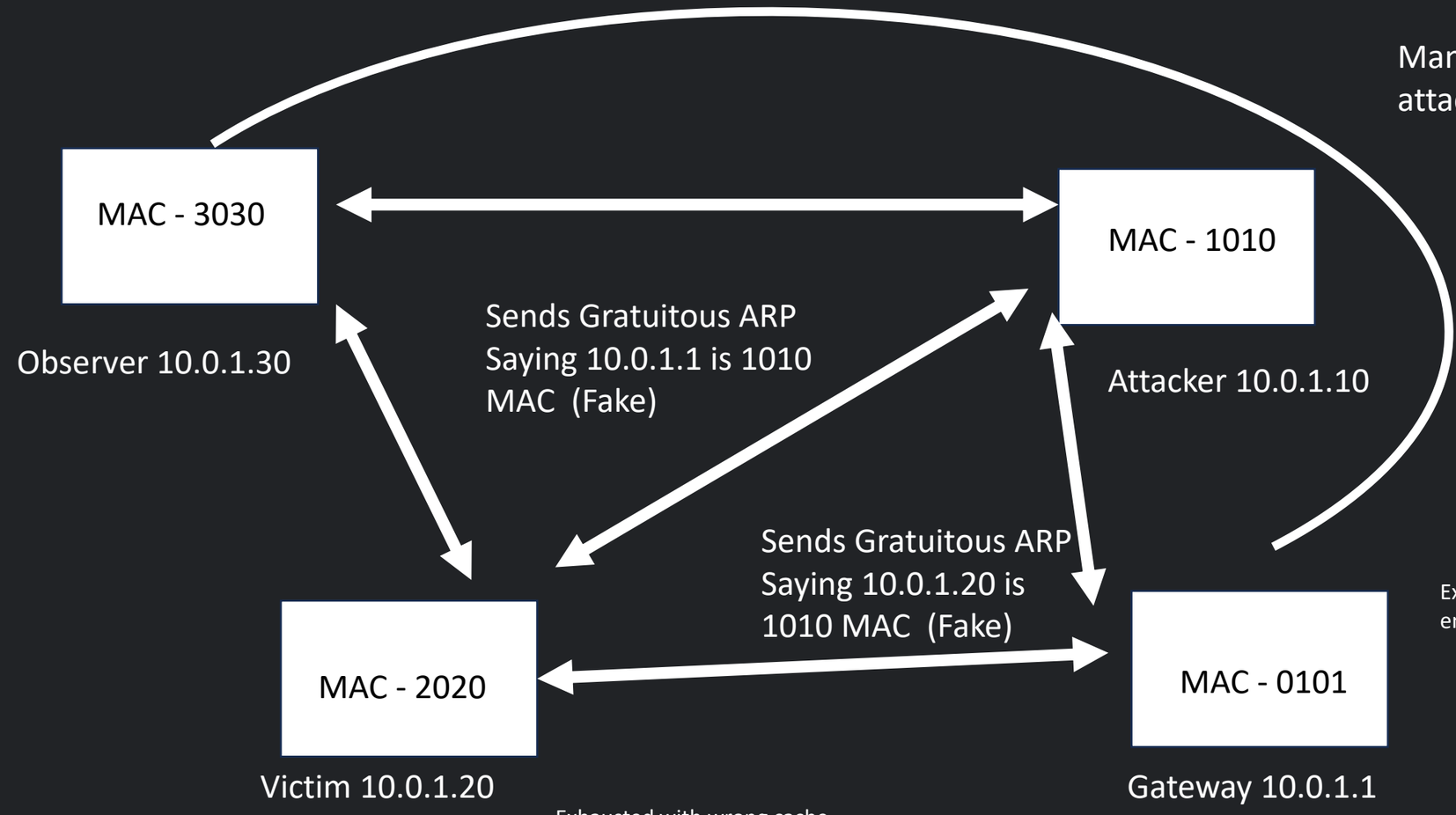
Victim ARP table

IP	MAC
10.0.1.1	0101
10.0.1.10	

IP	MAC
10.1.0.20	2020

Gateway ARP table

Made with GAMMA



Exhausted with wrong cache entries
Cant find the right MAC

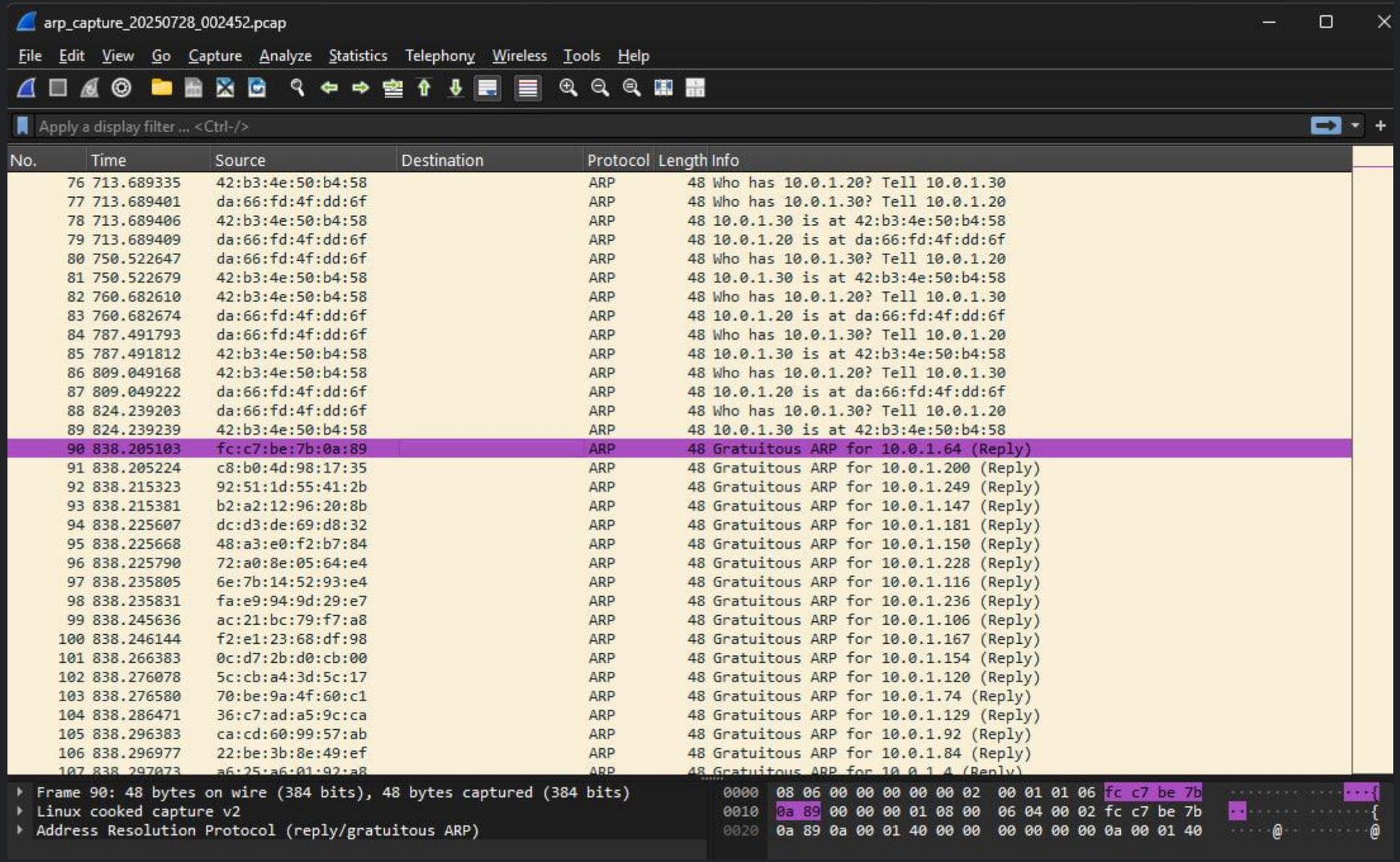
Victim ARP table

IP	MAC
10.0.1.1	0101

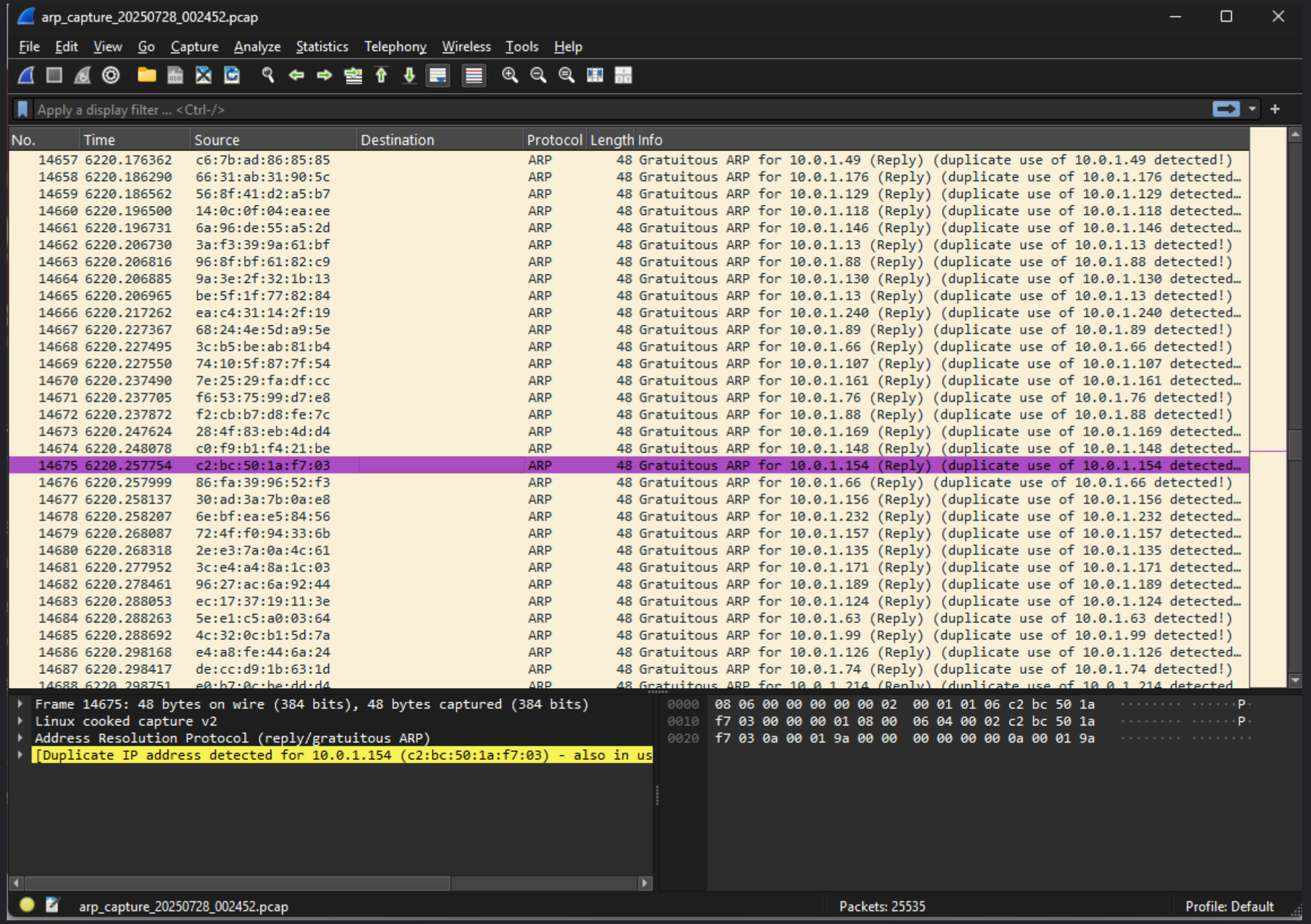
IP	MAC
10.0.1.20	2020

Gateway ARP table

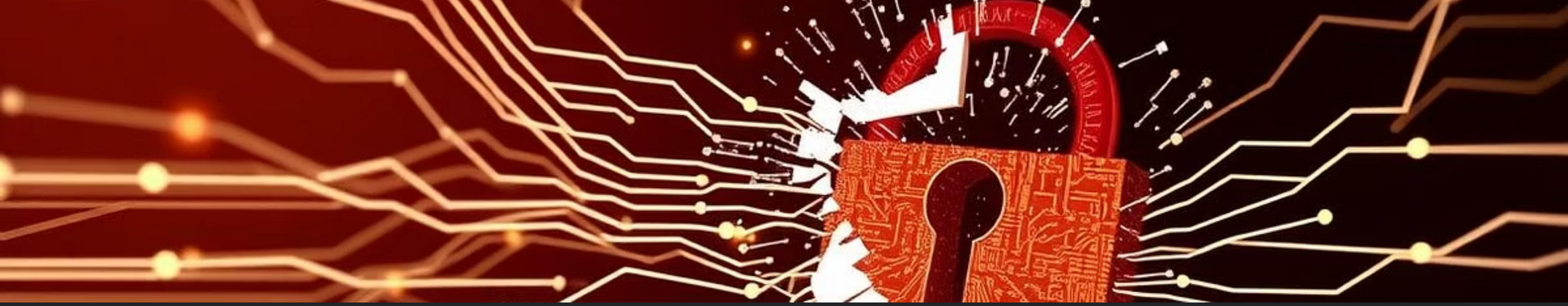
Made with GAMMA



Made with GAMMA



Made with GAMMA



Impact and Risks of ARP Gratuitous Storms

- Man-in-the-Middle (MITM) Interception: Attackers can intercept and read sensitive data, including login credentials and confidential communications.
- Session Hijacking: Gaining unauthorised control over active user sessions, leading to data breaches or system compromise.
- Network Disruption and Performance Degradation: The high volume of fake ARP traffic can congest the network, causing severe performance issues or complete outages.
- Facilitation of Further Attacks: ARP storms can be a precursor to more sophisticated attacks, such as Distributed Denial of Service (DDoS) or malware injection.

Made with GAMMA

Detecting ARP Gratuitous Storm Attacks

Detecting an ARP gratuitous storm requires vigilant monitoring and the use of specific tools.

Monitor ARP Tables

Regularly inspect ARP tables for unusual entries, such as multiple IP addresses mapped to the same MAC address, indicating suspicious activity.

Command Line Checks

Use the `arp -a` command on Windows or Linux to view current ARP cache entries and spot any suspicious or rapidly changing mappings.

Network Traffic Analysis

Utilise packet sniffers like Wireshark to capture and analyse network traffic. Look for an unusually high volume of ARP replies without corresponding requests.

ARP Monitoring Software

Deploy dedicated ARP monitoring tools such as cARP or ARPwatch, which are designed to detect and alert on ARP table inconsistencies and anomalies in real-time.

Made with GAMMA

Defence Mechanisms: DHCP Snooping & Dynamic ARP Inspection

DHCP Snooping

DHCP Snooping validates DHCP messages and maintains a database of trusted IP-MAC address bindings. This table is then used to verify the legitimacy of ARP packets.

- Builds trusted bindings from legitimate DHCP exchanges.
- Prevents rogue DHCP servers from assigning fake IPs.

Dynamic ARP Inspection (DAI)

DAI leverages the trusted bindings from DHCP Snooping to block invalid ARP packets on untrusted switch ports. It ensures that only valid ARP replies are processed.

- Drops ARP packets with invalid IP-MAC mappings.
- Requires trusted ports for DHCP servers and network devices.

Both DHCP Snooping and DAI are crucial features configured on managed switches to provide robust protection against ARP spoofing and storms.

Made with GAMMA

Software Tools and Network Configurations

Beyond switch-level defences, various software tools and network configurations can enhance protection against ARP attacks.

ARP Spoofing Detection Tools	Arpspoof, Ettercap, Cain & Abel
ARP Monitoring & Alerting	cARP, ARPwatch, Net Sensor
Traffic Encryption	Use VPNs (Virtual Private Networks) to encrypt all network traffic, preventing Man-in-the-Middle (MITM) data interception.
Secure Protocols	Prioritise cryptographic protocols like TLS, SSH, and HTTPS for all sensitive communications.

Made with GAMMA

Best Practices for Prevention

- Limit Trust: Avoid relying solely on IP addresses for trust relationships within the network. Implement additional authentication.
- Regular Updates: Ensure all network devices, operating systems, and software are regularly updated and patched to address known vulnerabilities.
- Network Segmentation: Implement VLANs (Virtual Local Area Networks) to segment the network, isolating different departments or device types. This limits the blast radius of ARP attacks.
- User Education: Train users and administrators to recognise the signs of ARP-based attacks, fostering a security-aware culture.

Case Study: Implementing ARP Defence on Enterprise Switches

A medium-sized enterprise deployed Juniper EX Series switches across its network, aiming to mitigate ARP spoofing and flooding incidents.

Configuration Setup

DHCP Snooping and Dynamic ARP Inspection (DAI) were enabled globally on all access layer switches.

Port Configuration

Ports connected to legitimate DHCP servers and core network infrastructure were configured as "trusted." All client-facing ports were designated as "untrusted."

Verification

Network administrators used commands like `show ethernet-switching-options analyser` and `show ip-source-binding` to confirm the active status of DHCP Snooping and DAI, verifying the integrity of IP-MAC bindings.

Outcome

Post-implementation, the organisation observed a significant reduction in reported ARP spoofing incidents and enhanced network stability, demonstrating the effectiveness of integrated defence.

Made with GAMMA

Summary and Key Takeaways

ARP gratuitous storm attacks exploit fundamental weaknesses in the ARP protocol, leading to serious security breaches like MITM and DoS. Effective defence requires a multi-layered approach.

- Attack Vulnerability: ARP's stateless nature allows attackers to poison network caches with fake gratuitous ARP replies.
- Vigilant Detection: Crucial for early response, involving ARP table monitoring, traffic analysis with tools like Wireshark, and alerts from dedicated ARP monitoring software.
- Layered Defence: Combine managed switch features (DAI, DHCP Snooping), host-based tools (static ARP, firewall rules), and traffic encryption (VPNs, HTTPS/TLS).
- Proactive Security: Network segmentation (VLANs), regular updates, and continuous user education are vital for a robust defence posture against evolving ARP-based threats.

Made with GAMMA

Thank you

Made with GAMMA