

CSE 406 Project

ARP DoS via Gratuitous ARP storm

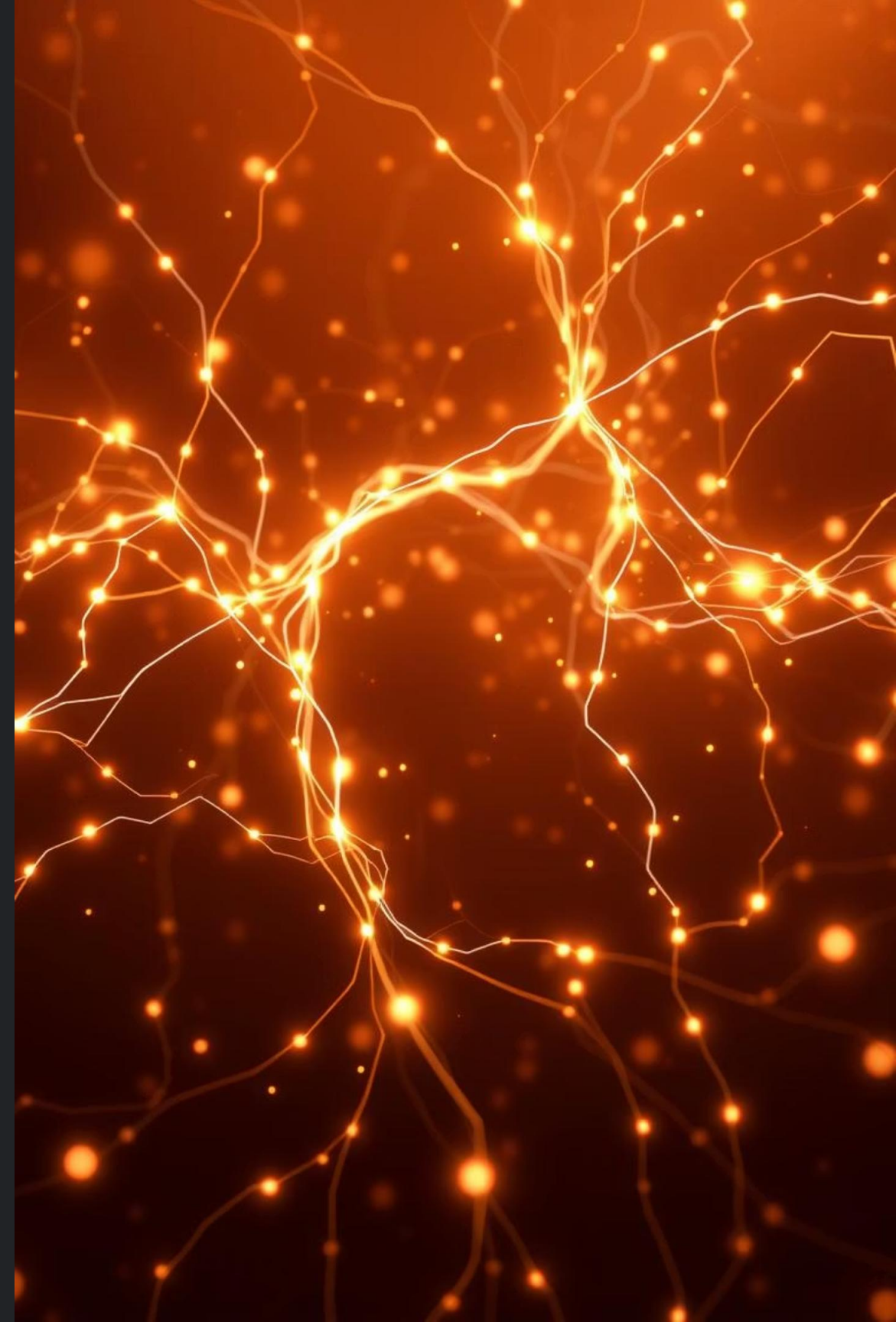
Members:

2005074 – Dipanta Kumar Roy Nobo

2005090 – Tawkir Aziz Rahman

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.

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

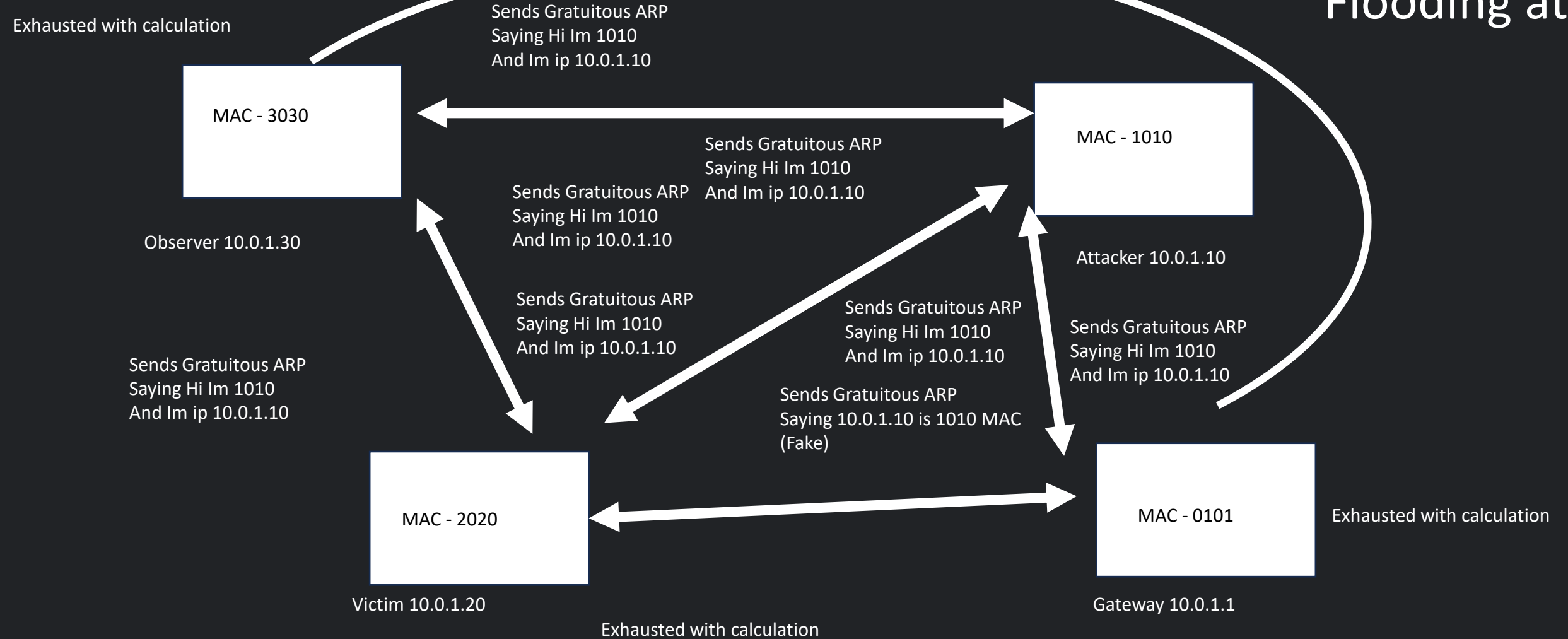
Consequently, traffic intended for legitimate devices (e.g., the default gateway) is redirected to the attacker's machine, enabling Man-in-the-Middle (MITM) attacks.

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.

Flooding attack

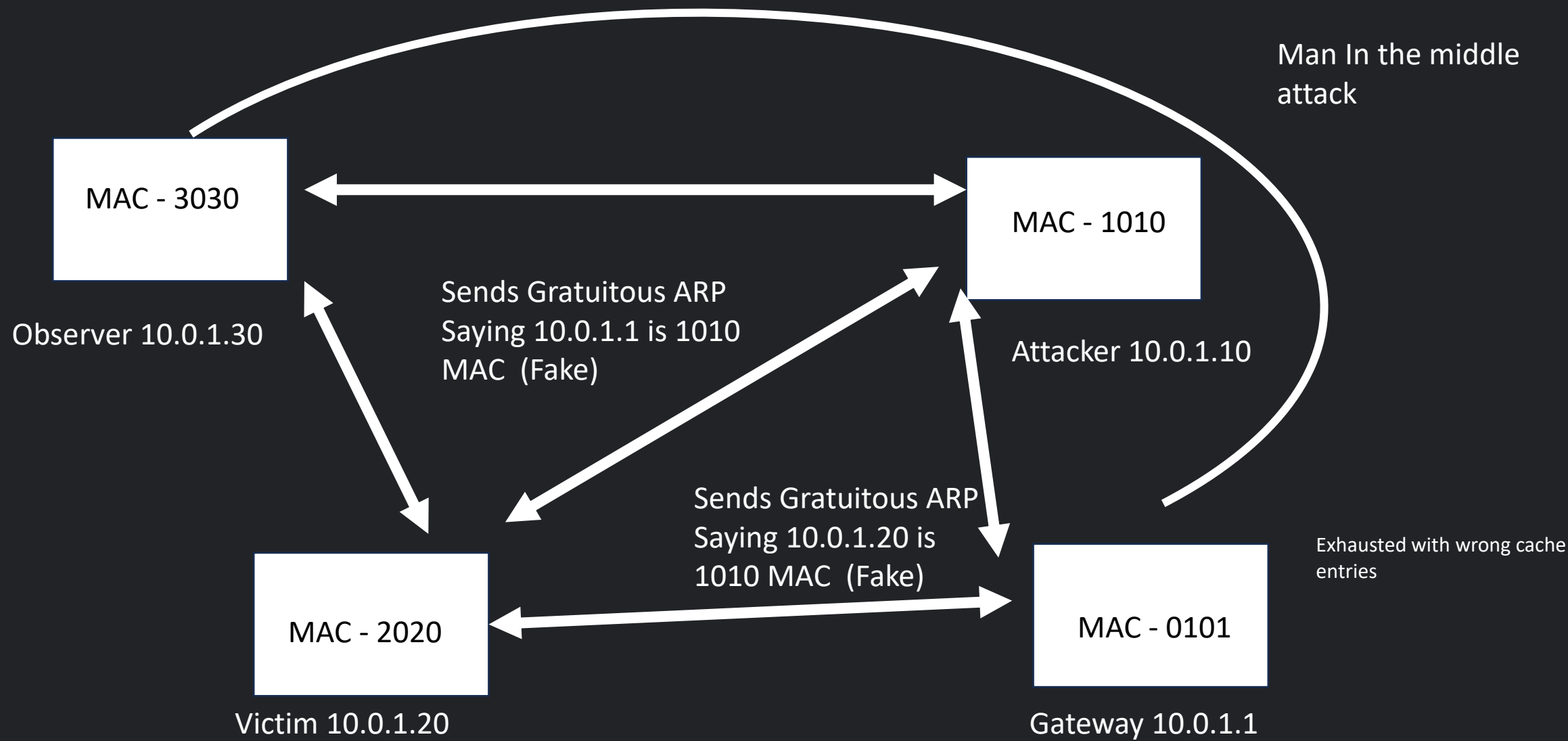


Victim ARP table

IP	MAC
10.0.1.1	0101
10.0.1.10	

Gateway ARP table

IP	MAC
10.1.0.20	2020



Victim ARP table

IP	MAC
10.0.1.1	0101

Gateway ARP table

IP	MAC
10.0.1.20	2020

arp_capture_20250728_002452.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
76	713.689335	42:b3:4e:50:b4:58		ARP	48	Who has 10.0.1.20? Tell 10.0.1.30
77	713.689401	da:66:fd:4f:dd:6f		ARP	48	Who has 10.0.1.30? Tell 10.0.1.20
78	713.689406	42:b3:4e:50:b4:58		ARP	48	10.0.1.30 is at 42:b3:4e:50:b4:58
79	713.689409	da:66:fd:4f:dd:6f		ARP	48	10.0.1.20 is at da:66:fd:4f:dd:6f
80	750.522647	da:66:fd:4f:dd:6f		ARP	48	Who has 10.0.1.30? Tell 10.0.1.20
81	750.522679	42:b3:4e:50:b4:58		ARP	48	10.0.1.30 is at 42:b3:4e:50:b4:58
82	760.682610	42:b3:4e:50:b4:58		ARP	48	Who has 10.0.1.20? Tell 10.0.1.30
83	760.682674	da:66:fd:4f:dd:6f		ARP	48	10.0.1.20 is at da:66:fd:4f:dd:6f
84	787.491793	da:66:fd:4f:dd:6f		ARP	48	Who has 10.0.1.30? Tell 10.0.1.20
85	787.491812	42:b3:4e:50:b4:58		ARP	48	10.0.1.30 is at 42:b3:4e:50:b4:58
86	809.049168	42:b3:4e:50:b4:58		ARP	48	Who has 10.0.1.20? Tell 10.0.1.30
87	809.049222	da:66:fd:4f:dd:6f		ARP	48	10.0.1.20 is at da:66:fd:4f:dd:6f
88	824.239203	da:66:fd:4f:dd:6f		ARP	48	Who has 10.0.1.30? Tell 10.0.1.20
89	824.239239	42:b3:4e:50:b4:58		ARP	48	10.0.1.30 is at 42:b3:4e:50:b4:58
90	838.205103	fc:c7:be:7b:0a:89		ARP	48	Gratuitous ARP for 10.0.1.64 (Reply)
91	838.205224	c8:b0:4d:98:17:35		ARP	48	Gratuitous ARP for 10.0.1.200 (Reply)
92	838.215323	92:51:1d:55:41:2b		ARP	48	Gratuitous ARP for 10.0.1.249 (Reply)
93	838.215381	b2:a2:12:96:20:8b		ARP	48	Gratuitous ARP for 10.0.1.147 (Reply)
94	838.225607	dc:d3:de:69:d8:32		ARP	48	Gratuitous ARP for 10.0.1.181 (Reply)
95	838.225668	48:a3:e0:f2:b7:84		ARP	48	Gratuitous ARP for 10.0.1.150 (Reply)
96	838.225790	72:a0:8e:05:64:e4		ARP	48	Gratuitous ARP for 10.0.1.228 (Reply)
97	838.235805	6e:7b:14:52:93:e4		ARP	48	Gratuitous ARP for 10.0.1.116 (Reply)
98	838.235831	fa:e9:94:9d:29:e7		ARP	48	Gratuitous ARP for 10.0.1.236 (Reply)
99	838.245636	ac:21:bc:79:f7:a8		ARP	48	Gratuitous ARP for 10.0.1.106 (Reply)
100	838.246144	f2:e1:23:68:df:98		ARP	48	Gratuitous ARP for 10.0.1.167 (Reply)
101	838.266383	0c:d7:2b:d0:cb:00		ARP	48	Gratuitous ARP for 10.0.1.154 (Reply)
102	838.276078	5c:cb:a4:3d:5c:17		ARP	48	Gratuitous ARP for 10.0.1.120 (Reply)
103	838.276580	70:be:9a:4f:60:c1		ARP	48	Gratuitous ARP for 10.0.1.74 (Reply)
104	838.286471	36:c7:ad:a5:9c:ca		ARP	48	Gratuitous ARP for 10.0.1.129 (Reply)
105	838.296383	ca:cd:60:99:57:ab		ARP	48	Gratuitous ARP for 10.0.1.92 (Reply)
106	838.296977	22:be:3b:8e:49:ef		ARP	48	Gratuitous ARP for 10.0.1.84 (Reply)
107	838.297073	a6:25:a6:01:92:a8		ARP	48	Gratuitous ARP for 10.0.1.4 (Reply)

▶ Frame 90: 48 bytes on wire (384 bits), 48 bytes captured (384 bits)
 ▶ Linux cooked capture v2
 ▶ Address Resolution Protocol (reply/gratuitous ARP)

```

0000  08 06 00 00 00 00 02 00 01 01 06 fc c7 be 7b  .......{
0010  0a 89 00 00 00 01 08 00 06 04 00 02 fc c7 be 7b  .....{
0020  0a 89 0a 00 01 40 00 00 00 00 00 0a 00 01 40  .....@
  
```


arp_capture_20250728_002452.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14657	6220.176362	c6:7b:ad:86:85:85		ARP	48	Gratuitous ARP for 10.0.1.49 (Reply) (duplicate use of 10.0.1.49 detected!)
14658	6220.186290	66:31:ab:31:90:5c		ARP	48	Gratuitous ARP for 10.0.1.176 (Reply) (duplicate use of 10.0.1.176 detected!)
14659	6220.186562	56:8f:41:d2:a5:b7		ARP	48	Gratuitous ARP for 10.0.1.129 (Reply) (duplicate use of 10.0.1.129 detected!)
14660	6220.196500	14:0c:0f:04:ea:ee		ARP	48	Gratuitous ARP for 10.0.1.118 (Reply) (duplicate use of 10.0.1.118 detected!)
14661	6220.196731	6a:96:de:55:a5:2d		ARP	48	Gratuitous ARP for 10.0.1.146 (Reply) (duplicate use of 10.0.1.146 detected!)
14662	6220.206730	3a:f3:39:9a:61:bf		ARP	48	Gratuitous ARP for 10.0.1.13 (Reply) (duplicate use of 10.0.1.13 detected!)
14663	6220.206816	96:8f:bf:61:82:c9		ARP	48	Gratuitous ARP for 10.0.1.88 (Reply) (duplicate use of 10.0.1.88 detected!)
14664	6220.206885	9a:3e:2f:32:1b:13		ARP	48	Gratuitous ARP for 10.0.1.130 (Reply) (duplicate use of 10.0.1.130 detected!)
14665	6220.206965	be:5f:1f:77:82:84		ARP	48	Gratuitous ARP for 10.0.1.13 (Reply) (duplicate use of 10.0.1.13 detected!)
14666	6220.217262	ea:c4:31:14:2f:19		ARP	48	Gratuitous ARP for 10.0.1.240 (Reply) (duplicate use of 10.0.1.240 detected!)
14667	6220.227367	68:24:4e:5d:a9:5e		ARP	48	Gratuitous ARP for 10.0.1.89 (Reply) (duplicate use of 10.0.1.89 detected!)
14668	6220.227495	3c:b5:be:ab:81:b4		ARP	48	Gratuitous ARP for 10.0.1.66 (Reply) (duplicate use of 10.0.1.66 detected!)
14669	6220.227550	74:10:5f:87:7f:54		ARP	48	Gratuitous ARP for 10.0.1.107 (Reply) (duplicate use of 10.0.1.107 detected!)
14670	6220.237490	7e:25:29:fa:df:cc		ARP	48	Gratuitous ARP for 10.0.1.161 (Reply) (duplicate use of 10.0.1.161 detected!)
14671	6220.237705	f6:53:75:99:d7:e8		ARP	48	Gratuitous ARP for 10.0.1.76 (Reply) (duplicate use of 10.0.1.76 detected!)
14672	6220.237872	f2:cb:b7:d8:fe:7c		ARP	48	Gratuitous ARP for 10.0.1.88 (Reply) (duplicate use of 10.0.1.88 detected!)
14673	6220.247624	28:4f:83:eb:4d:d4		ARP	48	Gratuitous ARP for 10.0.1.169 (Reply) (duplicate use of 10.0.1.169 detected!)
14674	6220.248078	c0:f9:b1:f4:21:be		ARP	48	Gratuitous ARP for 10.0.1.148 (Reply) (duplicate use of 10.0.1.148 detected!)
14675	6220.257754	c2:bc:50:1a:f7:03		ARP	48	Gratuitous ARP for 10.0.1.154 (Reply) (duplicate use of 10.0.1.154 detected!)
14676	6220.257999	86:fa:39:96:52:f3		ARP	48	Gratuitous ARP for 10.0.1.66 (Reply) (duplicate use of 10.0.1.66 detected!)
14677	6220.258137	30:ad:3a:7b:0a:e8		ARP	48	Gratuitous ARP for 10.0.1.156 (Reply) (duplicate use of 10.0.1.156 detected!)
14678	6220.258207	6e:bf:ea:e5:84:56		ARP	48	Gratuitous ARP for 10.0.1.232 (Reply) (duplicate use of 10.0.1.232 detected!)
14679	6220.268087	72:4f:f0:94:33:6b		ARP	48	Gratuitous ARP for 10.0.1.157 (Reply) (duplicate use of 10.0.1.157 detected!)
14680	6220.268318	2e:e3:7a:0a:4c:61		ARP	48	Gratuitous ARP for 10.0.1.135 (Reply) (duplicate use of 10.0.1.135 detected!)
14681	6220.277952	3c:e4:a4:8a:1c:03		ARP	48	Gratuitous ARP for 10.0.1.171 (Reply) (duplicate use of 10.0.1.171 detected!)
14682	6220.278461	96:27:ac:6a:92:44		ARP	48	Gratuitous ARP for 10.0.1.189 (Reply) (duplicate use of 10.0.1.189 detected!)
14683	6220.288053	ec:17:37:19:11:3e		ARP	48	Gratuitous ARP for 10.0.1.124 (Reply) (duplicate use of 10.0.1.124 detected!)
14684	6220.288263	5e:e1:c5:a0:03:64		ARP	48	Gratuitous ARP for 10.0.1.63 (Reply) (duplicate use of 10.0.1.63 detected!)
14685	6220.288692	4c:32:0c:b1:5d:7a		ARP	48	Gratuitous ARP for 10.0.1.99 (Reply) (duplicate use of 10.0.1.99 detected!)
14686	6220.298168	e4:a8:fe:44:6a:24		ARP	48	Gratuitous ARP for 10.0.1.126 (Reply) (duplicate use of 10.0.1.126 detected!)
14687	6220.298417	de:cc:d9:1b:63:1d		ARP	48	Gratuitous ARP for 10.0.1.74 (Reply) (duplicate use of 10.0.1.74 detected!)
14688	6220.298751	e0:b7:0c:be:dd:d4		ARP	48	Gratuitous ARP for 10.0.1.214 (Reply) (duplicate use of 10.0.1.214 detected!)

Frame 14675: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 0

Linux cooked capture v2

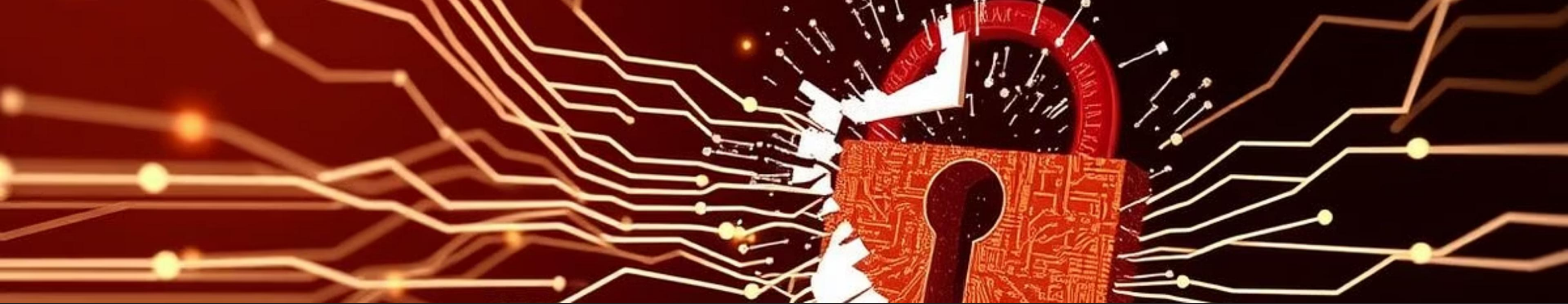
Address Resolution Protocol (reply/gratuitous ARP)

[Duplicate IP address detected for 10.0.1.154 (c2:bc:50:1a:f7:03) - also in us

arp_capture_20250728_002452.pcap

Packets: 25535

Profile: Default



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.

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.

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.

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.

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.

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.

Port Configuration

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

Outcome

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

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.

Thank you