

Research Article

Finding Type of ARP Request That Introducing the MAC Address Table Instability Results in Network Sensitivity

Md. Abdullah Yusuf Imam, Prodip Kumar Biswas*

Department of Information and Communication Technology, National University, Gazipur, Bangladesh

Abstract

In network analysis, "looping" or "network loops" refers to situations where a path in a network returns to the same node or nodes multiple times, creating a closed circuit or cycle. In a loop, a single ARP (ARP or Address Resolution Protocol) is a networking protocol that translates Internet Protocol (IP) addresses to Media Access Control (MAC) addresses within a local area network (LAN). This can occur in various network contexts, including project management, computer networks, and electrical circuits. loops occur when a path traverses the same node twice or more. Looping in Computer Programming can be stated as a "loop" is a sequence of instructions that is repeatedly executed until a certain condition is met. This paper is trying to introduce the verities of looping criteria where the ARP is infected first and after that effect of its network smoothness, and also how it can be avoided is tries to show in Computer technology.

Keywords

Arp, Mac, Looping, Ip, Strom, Layer, Router, Switch

1. Network Loops in Computer Networks

In IP networks, the MAC address of an interface can be queried given the IP address using the Address Resolution Protocol (ARP) for internet protocol version 4 (IPV4) or the neighbor discovery protocol (NDP) for IPV6. In this way, ARP or NDP is used to relate IP addresses to Ethernet MAC addresses. A MAC address which is working at OSI Layer 2 like a social security number which remains unchanged for a person's life time (the device), while an IP address which is working at OSI Layer 3 is like a postal code which can be changed [1].

This translation is crucial because devices on a network use IP addresses to identify each other, but communication at the physical level relies on the MAC address. A request is

duplicated and endlessly circulated, creating:

1. Broadcast storms
2. MAC address table instability

Broadcast packets are network packets sent to all hosts on a local subnet. They use a special IP address (255.255.255.255) as the destination, meaning the packet is intended for everyone, not just a specific device. This is different from unicast packets, which are sent to a single, specific IP address.

Broadcast packets are used to send information to all devices on a network, such as when a device needs to discover other devices on the network (e.g., using ARP requests) or when a device is joining a network for the first time. Routers

*Corresponding author: prodipcse01@gmail.com (Prodip Kumar Biswas)

Received: 24 May 2025; **Accepted:** 16 June 2025; **Published:** 7 July 2025



typically do not forward broadcast packets to other subnets, as this can waste bandwidth. However, they can be configured to do so, but this is not the default behavior.

B. Examples of Broadcast Packets:

An ARP requesting where a device asks, "Who has this IP address? And the DHCP device asks for an IP address. Look: A device (Our computers or etc.) wants to send a packet to a known IP address (e.g., 192.168.1.10). It checks its ARP cache to see if it already knows the MAC address. If not, it sends out a broadcast ARP request: "Who has 192.168.1.10? All devices on the local network segment receive this. The device with that IP replies with its MAC address (an ARP reply). The sender stores that IP-MAC mapping in its ARP cache for future use. ARP requests are broadcast to all devices in a Layer 2 network.

2. Broadcast Storms

A broadcast storm is an excessive amount of broadcast traffic on a network that can overwhelm network devices and cause network disruptions. It occurs when a large number of broadcast packets are repeatedly sent and received within a short period, consuming network resources and potentially leading to network instability. Here's a more detailed explanation:

nation:

3. What Causes a Broadcast Storm

Layer 2 Loops:

When a broadcast packet enters a loop (an unintended or redundant connection between switches), it is repeatedly sent and received, creating a loop. In other words, if a device repeatedly sends broadcast messages (like ARP requests, DHCP discovery), and especially if it does so at a high rate, it can cause a broadcast storm. ARP spoofing and MAC table poisoning do the same.

4. Broadcast Address

1st, we need to know about the MAC address. A MAC address is a 12-digit hexadecimal number, typically formatted as six pairs of two hexadecimal digits separated by colons (e.g., 00:1A:2B:3C:4D:5E) or hyphens (e.g., 00-1A-2B-3C-4D-5E). It represents a network interface controller's unique identifier [2].

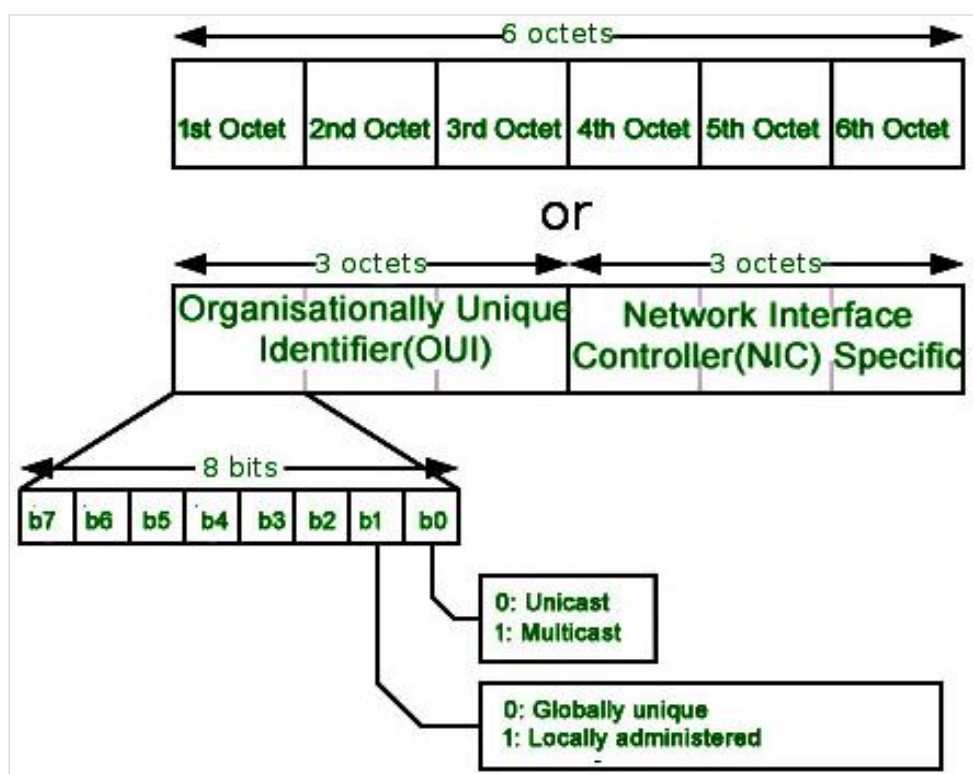


Figure 1. MAC Address Anatomy.

2nd, we need to know about the IP address. An IP address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol. IPv4 addresses

are typically represented as four numbers separated by dots, each number ranging from 0 to 255. For example, 192.168.1.1 is a valid IPv4 address. IPv6 addresses, on the

other hand, are 128-bit addresses written as eight groups of four hexadecimal digits, separated by colons. An example of an IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

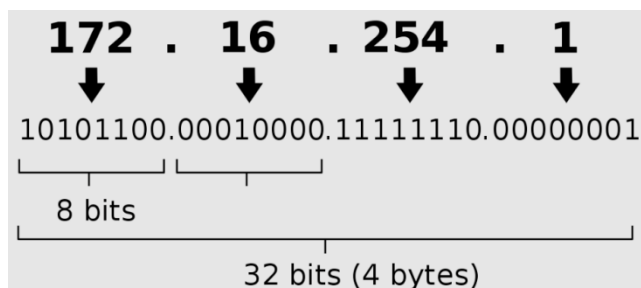


Figure 2. IPv4 Address format.

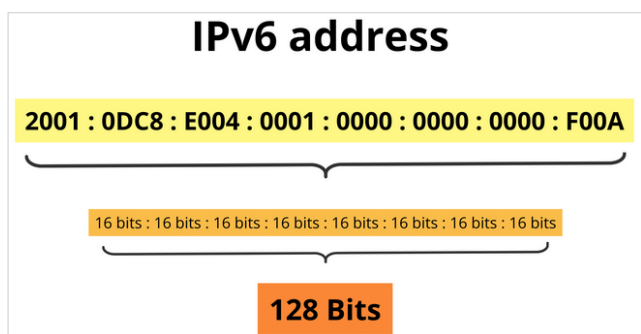


Figure 3. IPv6 Address format.

Now we can say the broadcast IP address is 255.255.255.255. This is a special address that signifies that the packet should be received by all hosts on the local subnet [3].

3rd we have to know OSI reference model. The OSI (Open Systems Interconnection) reference model is a conceptual framework that divides network communication into seven distinct layers. Each layer has specific responsibilities and functions, working together to enable data transmission between networked devices. This model helps standardize network communication and provides a framework for troubleshooting and understanding network issues.

Here's a breakdown of the seven layers:

1. Physical Layer (Layer 1):

Handles the physical transmission of data over the network medium (e.g., cables, wireless).

2. Data Link Layer (Layer 2):

Provides error detection and correction, and manages data transfer between two devices on the same network.

3. Network Layer (Layer 3):

Handles the logical addressing and routing of data packets between networks.

4. Transport Layer (Layer 4):

Ensures reliable data delivery between applications by

adding error control and flow control mechanisms.

5. Session Layer (Layer 5):

Manages the connection and synchronization between applications, including authentication and session control.

6. Presentation Layer (Layer 6):

Formats and transforms data for presentation to the application layer, including encryption/decryption.

7. Application Layer (Layer 7):

Provides the interface for applications to access network services, including protocols like HTTP, SMTP, and FTP.

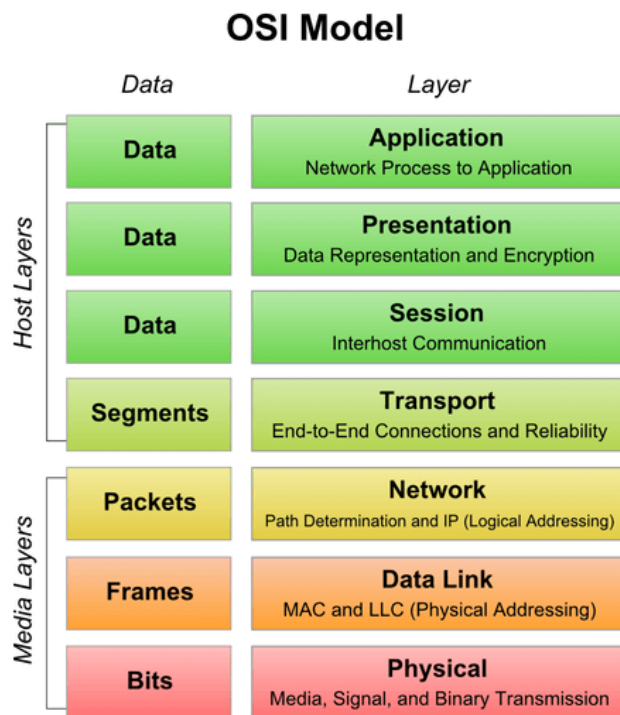


Figure 4. OSI reference model.

The OSI model is a valuable tool for understanding network communication and troubleshooting problems, though the modern internet primarily uses the TCP/IP model. The seven layers of the OSI model are often used as a reference for network professionals to understand the different functions involved in network communication.

Now we can say about looping what is in Layer 2 vs. Layer 3:

At the MAC layer (Layer 2), a broadcast frame uses the MAC address FF:FF:FF:FF:FF:FF. At the network layer (Layer 3), the IP address 255.255.255.255 is used.

5. How Does a Broadcast Storm Impact the Network

1. Network Congestion: Broadcast packets consume network bandwidth, leaving less capacity for normal traffic.

2. Unintended Broadcasts: Misconfigured devices or poor

network management can lead to excessive broadcast traffic.

3. Hub threats: Poor Network Design, using hubs (which flood traffic to all ports) instead of switches can exacerbate broadcast storms.

4. Frames are endlessly circulated: Ethernet frames don't have a TTL (Time To Live) like IP packets, so they can loop forever.

5. Broadcast and multicast storms: One broadcast gets repeated and amplified, flooding the entire network.

6. MAC address table instability: Switches keep updating their MAC address tables rapidly as frames come in from different ports.

7. Packets: Broadcast packets (e.g., ARP requests) enter the loop.

8. Since Layer 2 (Ethernet) has no TTL, these frames circulate indefinitely.

9. Unstable MAC address table: Switch MAC address tables become unstable—MACs keep "moving" between ports.

10. High CPU usage: CPU usage spikes as switches struggle to handle frame forwarding and table updates.

11. Port problem: Ports may start flapping (turning off and

on rapidly).

12. Device Resource Exhaustion: Switches and other network devices struggle to process the high volume of broadcast packets, leading to potential performance issues or crashes.

13. Service Disruption: Network services, like VoIP or video conferencing, that rely on reliable network communication can be affected by the reduced bandwidth and instability caused by a broadcast storm.

6. Create Looping Scenario (Practical Invention) Causes Broadcast Storm and Makes Network Jam

1. A Router is connected to the internet through a console port of the switch, and another distribution port of Router is connected to the same switch at a time. See [Figure 5](#).

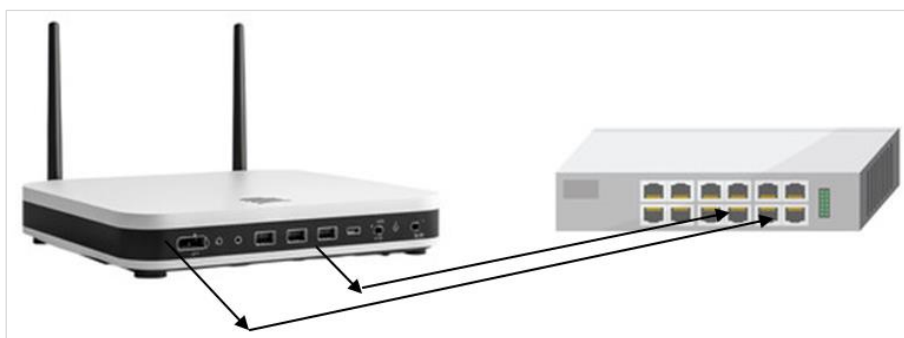


Figure 5. Create Looping 1.

2. Two ports of Router is connected to a same network at a time. See [Figure 6](#).

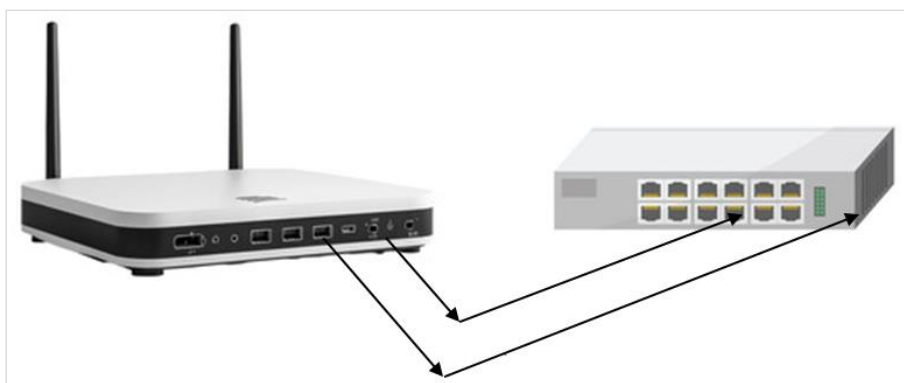


Figure 6. Create Looping 2.

3. One Cable is connected to two ports of the same switch at a time. See [Figure 7](#).

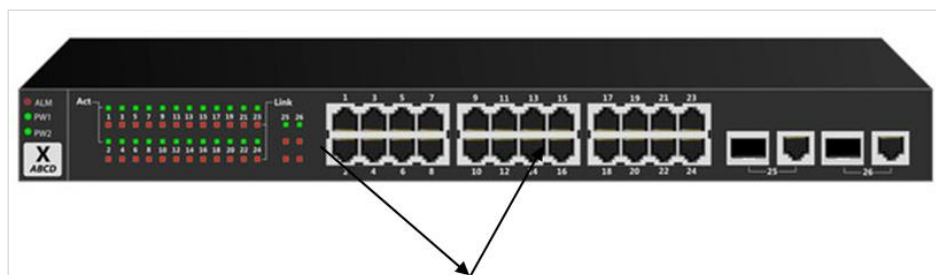


Figure 7. Create Looping 3.

4. Two Switches are connected by two separate cables in the same manner at a time. See [Figure 8](#).

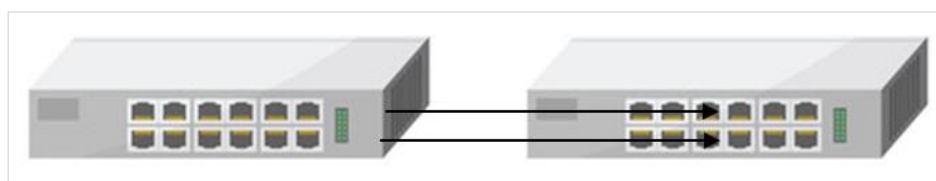


Figure 8. Create Looping 4.

5. To network cards of the same Computer is connected to the same network at a time. See [Figure 9](#).

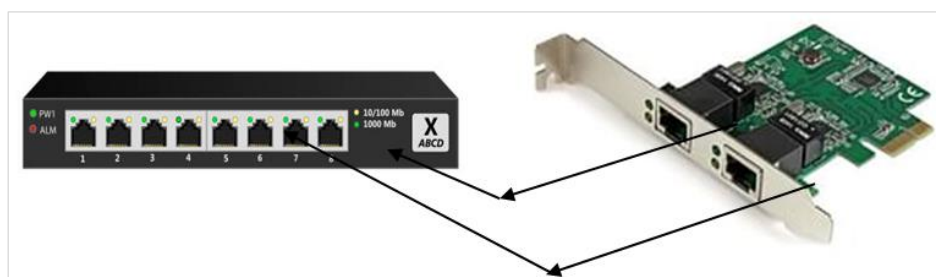


Figure 9. Create Looping 5.

6. Viruses or Malicious programs intended to do broadcast storm.
 7. Error in Cables or Ports of Computers, Routers, Switches etc. [4].

7. Steps for Cancelling Loops in Network

To avoid looping, following steps can be applied.

Spanning Tree Protocol (STP): STP helps prevent Layer 2 loops by identifying and blocking redundant paths, preventing broadcast packets from circulating endlessly.

Network Design: Proper network design with switches and avoiding the use of hubs can help prevent loops.

Monitoring and Alerting: Monitoring tools can help identify excessive broadcast traffic and trigger alerts when a broadcast storm is detected.

Broadcast Filtering: Some devices offer features to limit or

filter broadcast traffic, reducing the impact of a

8. Conclusion

Looping first creates broadcast and then broadcast storm, and then creates network instability. It causes network jam and unavailability. Creative network setup diagram and virus free operating system and apps can prevent it. Also no loop connection, no faulty cables, no faulty jacks can refuse broadcast storm.

Author Contributions

Md. Abdullah Yusuf Imam: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation

Prodip Kumar Biswas: Visualization, Writing – original draft, Writing – review & editing

Conflicts of Interest

As per 1st Author, I declare that is no conflict of interest.

References

- [1] MAC ADDRESS ROUTING POLICY OVER THE IP NETWORK. <https://doi.org/10.33564/IJEAST.2019.v03i11.002> (Accessed from May, 2019)
- [2] MAC ADDRESS CLONING TECHNIQUE RESULTS. <https://doi.org/10.33564/IJEAST.2019.v04i01.001> (Accessed from May, 2019)
- [3] CLONING MAC ADDRESS RESULTS REVIEW https://www.researchgate.net/publication/333031627_CLONING_MAC_ADDRESS_RESULTS_REVIEW (Accessed from May, 2019)
- [4] ALLOCATION OF BANDWIDTH IN DHCP REVIEW https://www.researchgate.net/publication/348737764_ALLOCATION_OF_BANDWIDTH_IN_DHCP_REVIEW (Accessed from December 2020)