A COURSE PROJECT REPORT BY

MAC- FLOODING ATTACK DEMONSTRATION

AJITH SOWMYAN R.J.(RA2111003011410)
SURAJ SINGH S (RA2111003011415)
SHRUTHI A (RA2111003011397)
NEHA GUPTA (RA211100311416)
AVINASH SINGH(RA2111003011414)

Under the guidance of

Dr. Pradeep Mohan Kumar K

(Associate Professor)

In partial fulfillment for the Course

of

18CSS202J - COMPUTER COMMUNICATIONS

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

MAY 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY (Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that 18CSS202J minor project report titled “MAC-FLOODING ATTACK DEMONSTRATION ” is the bonafide work of “ __________________________ “ who carried out the minor project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE
Dr. Pradeep Mohan
Kumar K
Associate Professor
Course Faculty
COMPUTER COMMUNICATIONS
Department of Computing
technologies

SIGNATURE
HOD NAME -
HEAD OF THE DEPARTMENT
Professor
Dept. of Computing
Technologies

Signature of the Panel Head
Panel Head Name
Panel Head Affiliation

TABLE OF CONTENTS

ABSTRACT

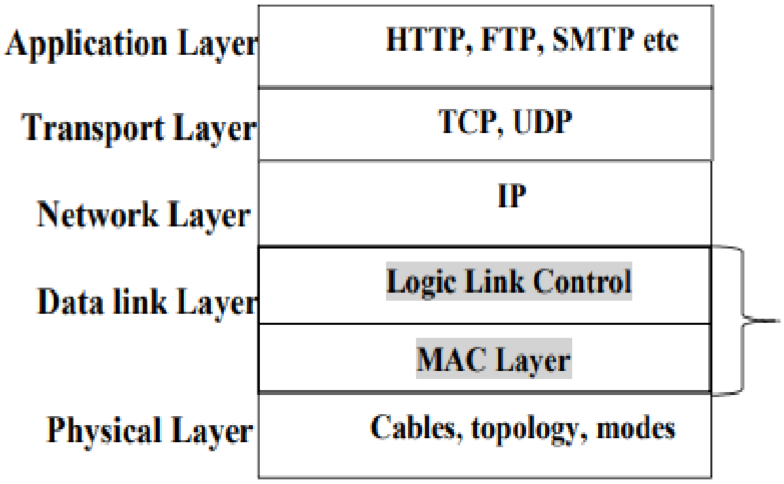
Media Access Control (MAC)attack is a type of attack in computer networks to challenge the security of network switches. The network is flooded with fake MAC addresses to steal sensitive information from the network. In this paper we propose three techniques with our traditional methods to prevent MAC Flooding Attack. They are priority scheduling with time stamp, authorization, authentication technique with digital signature and a security measure by using machine learning. Also examine how to limit the number of entries in a MAC table. Keywords: MAC, Spoofing, Authentication Filtering

The wide scale deployment of IEEE 802.11 based wireless networks have led to a number of security challenges. The MAC and Physical layers of IEEE 802.11 wireless networks possess various vulnerabilities to Denial of Service (DoS) attacks. In this work we discuss DoS attacks which exploit the MAC layer vulnerabilities of IEEE 802.11 networks. In recent years, DoS attacks in wireless networks have been getting the attention of researchers and it has been demonstrated that MAC layer related DoS attacks can easily be launched by using off the shelf equipment. In most cases the attacker forges the MAC addresses of wireless devices in order to halt the operation of the wireless network. MAC address spoofing is possible because the IEEE 802.11 standard does not provide per frame source authentication for control and management frames. Even the new WLAN security standard IEEE 802.11i does not solve these problems. Many tools are easily available for attackers to launch such types of attack. In this paper we classify MAC layer DoS attacks into three categories, and we compare the existing countermeasures to such attacks. We also identify the issues with existing countermeasure and provide future research directions.

INTRODUCTION

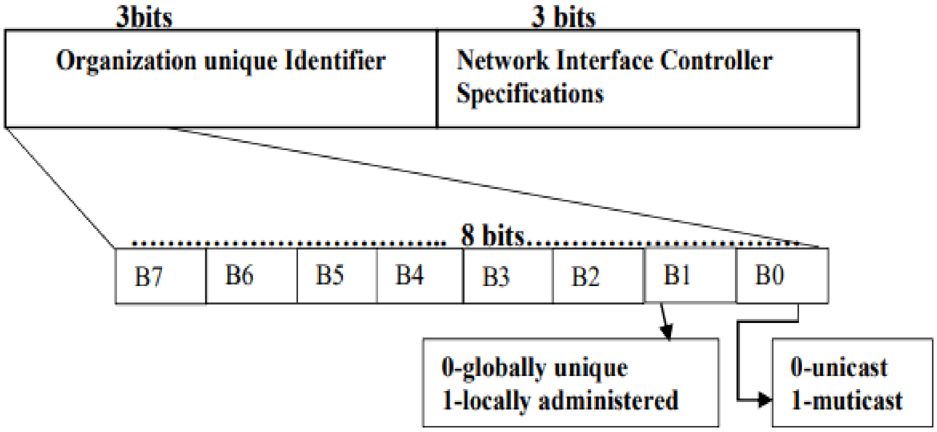
Media Access Control (MAC)

Media Access Control is a sublayer of the data link layer of OSI reference model. MAC has an important function that is transmitting data packets to and from the network interface Card (NIC)and other channels. It is responsible for flow control and multiplexing for transmission medium. MAC Layer controls the transmission of data packets via remotely shared channels. It is responsible for encapsulating frames so that they are suitable for transmission through the physical medium. Also, MAC resolves the addressing of source station as well as the destination station and performs multiple access resolutions when more than one data frame is to be transmitted. Then determines the channel access method for transmission.



MAC Addresses.

MAC address is a unique identifier allotted to a network Interface Controller (NIC) of a device. It is used as a network address for data transmission with in a network segment like Ethernet, Wi-Fi and Bluetooth. This address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard coded in the Network interface Card(NIC).A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons or no separators:

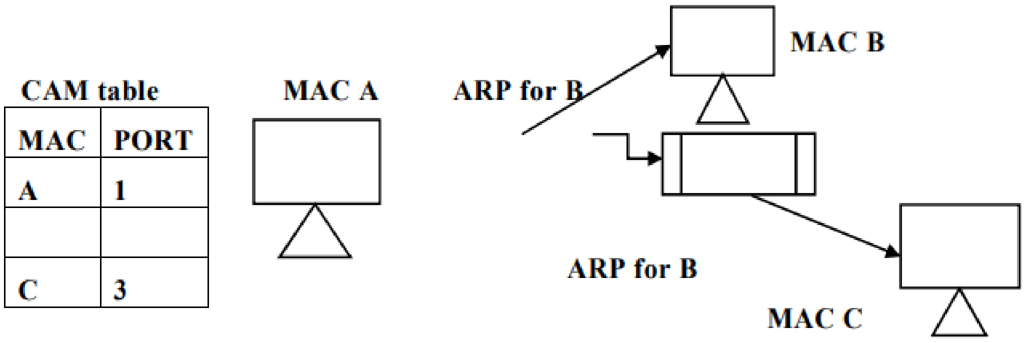

3bits
3 bits
Organization unique Identifier
Network Interface Controller Specifications
8 bits
B7
B6
B5
B4
B3
B2
B1
B0
0-globally unique
1-locally administered
0-unicast
1-muticast

Managing the MAC Address Table

Switches use MAC address tables to determine how to forward traffic between ports. These MAC tables include dynamic and static addresses. Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for MAC addresses. The default time is 300 seconds. Setting too short an aging time can cause addresses to be prematurely removed from the table. Then, when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same LAN (or VLAN) as the receiving port. This unnecessary flooding badly affect the performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being entered. This can also cause flooding. The switch provides dynamic addressing by learning the source MAC address of each frame that it receives on each port, and then adding the source MAC address and its associated port number to the MAC address table. As computers are added or removed from the network, the switch updates the MAC address table, adding new entries and aging out those that are currently not in use. A network administrator can specifically assign static MAC addresses to certain ports. Static addresses are not aged out, and the switch always knows which port to send out traffic destined for that specific MAC address. As a result, there is no need to relearn or refresh which port the MAC address is connected to. One reason to implement static MAC addresses is to provide the network administrator complete control over access to the network. Only those devices that are known to the network administrator can connect to the network.

MAC Flooding Attack

The MAC Flooding is an attacking method intended to not compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting. As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker will be able to steal sensitive data from the communication of the victim and other computers. Usually a packet analyzer is used to capture these sensitive data.



CAM table

MAC	PORT
A	1
C	3

MAC- FLOODING

REQUIREMENT ANALYSIS

Hardware and Software:

- Two PC (Ubuntu and Windows)
- Scapy and Python (Free download)
- Cisco Switch (1nos) – 2950 is used in the project.
- Network cables.

OPERATING SYSTEM	:WINDOWS 7 AND ABOVE
LOCAL PLATFORM	:CISCO PACKET TRACER

ARCHITECTURE AND DESIGN

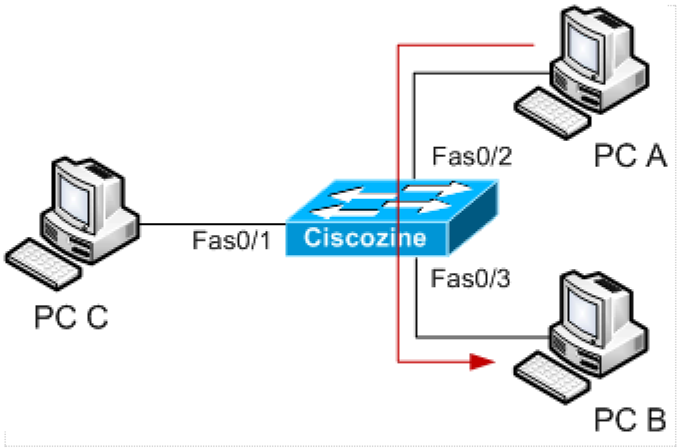
In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.

The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. A malicious user could then use a packet sniffer running in promiscuous mode to capture sensitive data from other computers, which would not be accessible were the switch operating normally.

Cisco gives you an opportunity to set up protection against this attack with limiting and/or hardwiring some MAC addresses to a dedicated port.

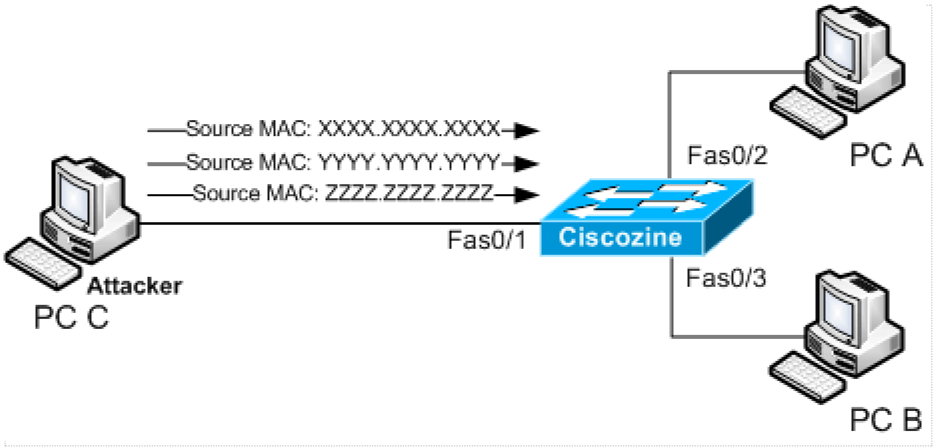
Understand the MAC flooding attack

Suppose to have a switch with 3 PC: PC A, PC B and PC C; in normal situation, when PC A sends a packet to PC B, PC C does not view packet sent between PC A and PC B.

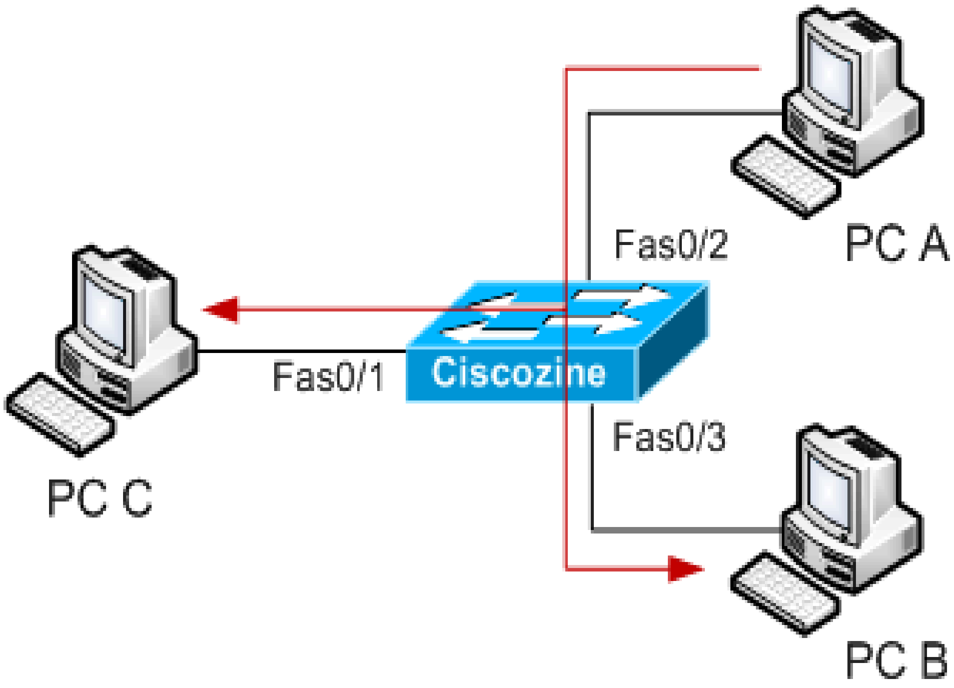


This because the 3 PC are connected to a switch and NOT to a hub.

Under MAC flooding attack, the switch behaviour is different. During the MAC flooding attack, the attacker (in this instance PC C) floods the switch with packets, each with different source MAC address.


Source MAC: XXXX.XXXX.XXXX
Source MAC: YYYY.YYYY.YYYY
Source MAC: ZZZZ.ZZZZ.ZZZZ
Fas0/2
PC A
Fas0/1
Ciscozine
Fas0/3
Attacker
PC C
PC B

If the Content Addressable Memory (the memory where the MAC addresses are stored) is full, the switch works like an hub; so, if the PC A sends a packet to PC B, the packet will be received to PC C too.



How Does MAC Flooding work

MAC flooding happens when the attacker tries to send numerable invalid MAC addresses to the MAC table. It floods the source table with the invalid MAC addresses. Once the MAC table reaches the assigned limit of the MAC table, it starts to remove the valid MAC addresses. This is one of the characteristics of the MAC table, it removes the previous address as and when the new addresses get added to it.

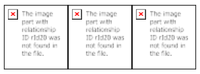
Now, all the valid MAC addresses have been removed. The switch will now behave as the network hub. If the users connected to the same network trying to access the web, they receive a broadcast or a flood throughout the network.

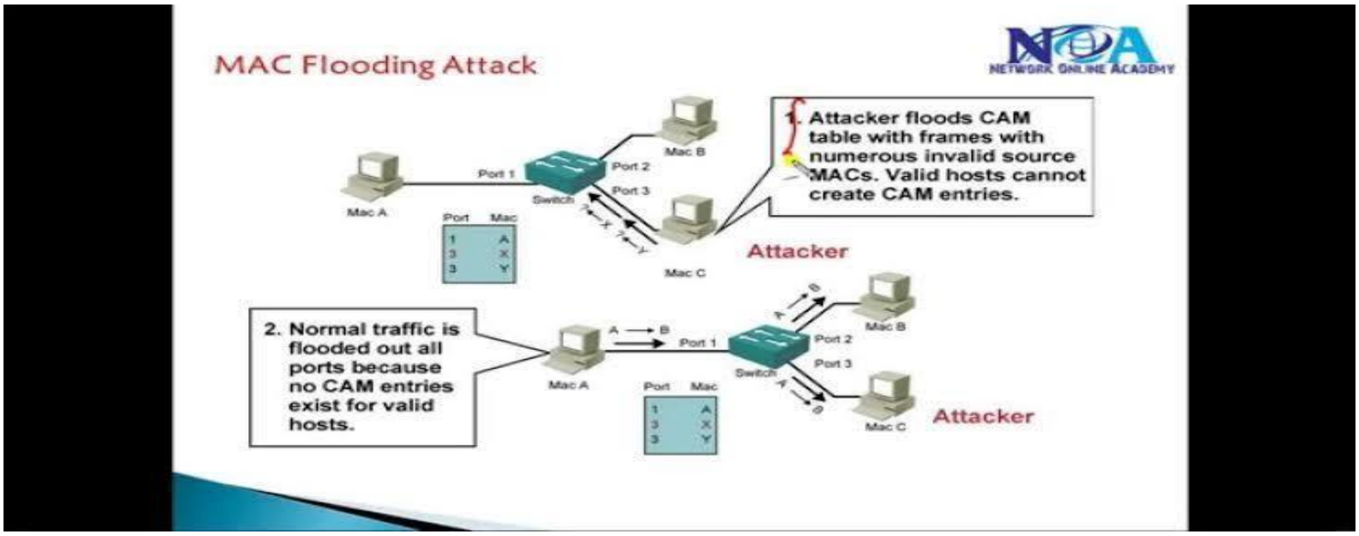
When two valid users trying to connect, their data will be forwarded to all the ports like broadcasting. This is also known as the MAC table flooding attack. Once this is done, all the valid users are not going to make an entry. They are going to work based on the broadcast.

In such scenarios, attackers are part of a network. It will send malicious data packs to the user machine. This will enable the attacker to be able to steal sensitive data from the user machine. It will also allow the attacker to get all the to and fro communication data. This makes a MAC flooding attack successful.

- **Denial of service attacks, once the traffic is flooded in the MAC table, it overloads and ends up in error.**
- **Session hijacking allows the attacker to hijack the session and steal sensitive information.**
- **Man in the middle attack allows the attacker to intercept and modify the traffic between users.**

ARCHITECTURE DIAGRAM


The image part with relationship ID rId20 was not found in the file.
The image part with relationship ID rId20 was not found in the file.
The image part with relationship ID rId20 was not found in the file.



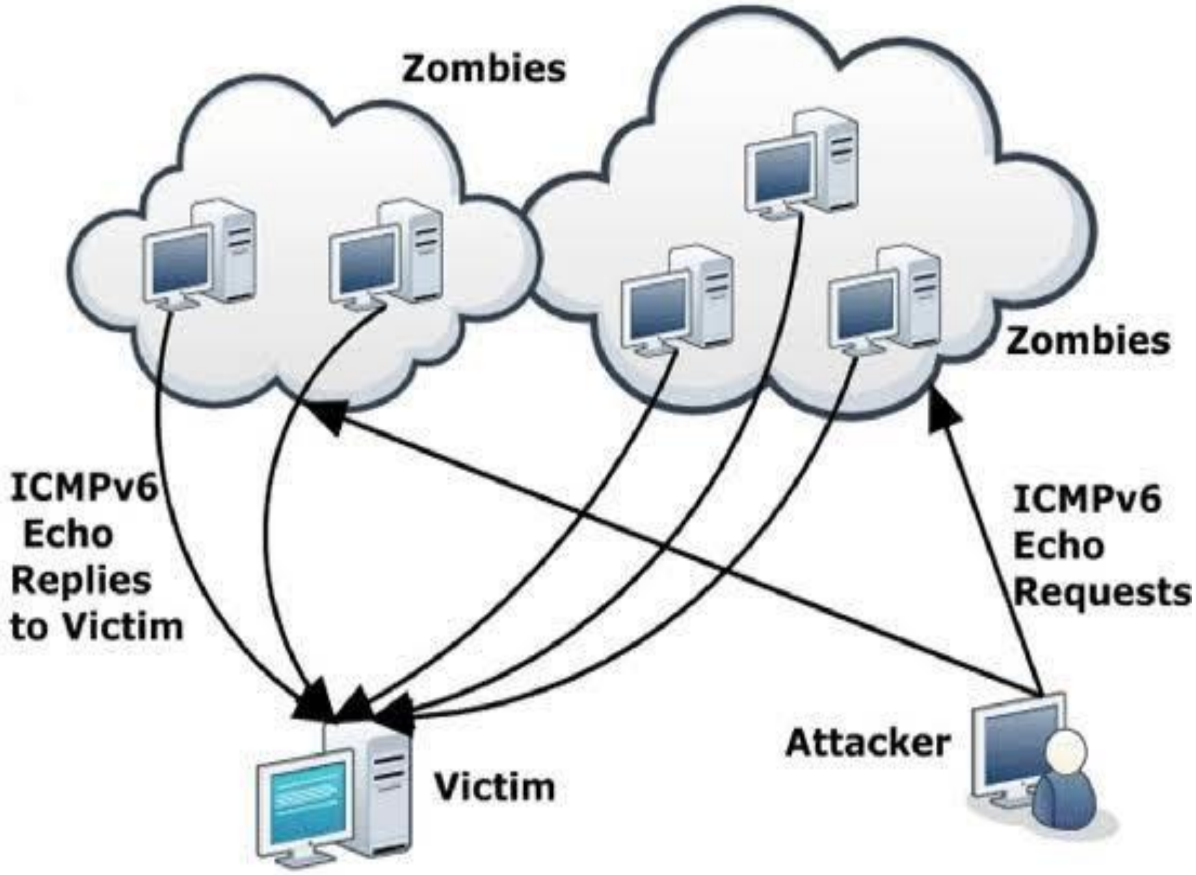
MAC Flooding Attack

1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

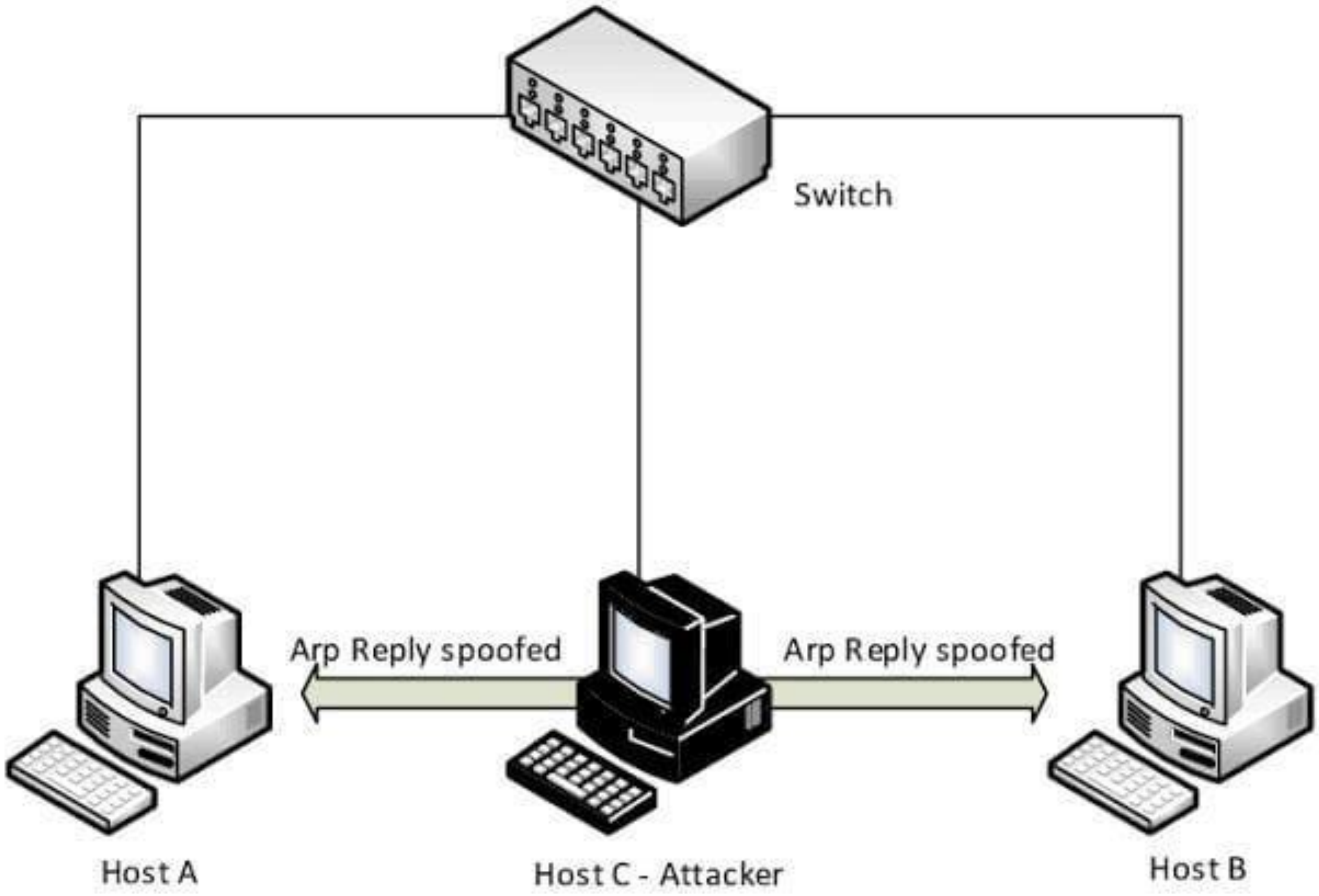
2. Normal traffic is flooded out all ports because no CAM entries exist for valid hosts.

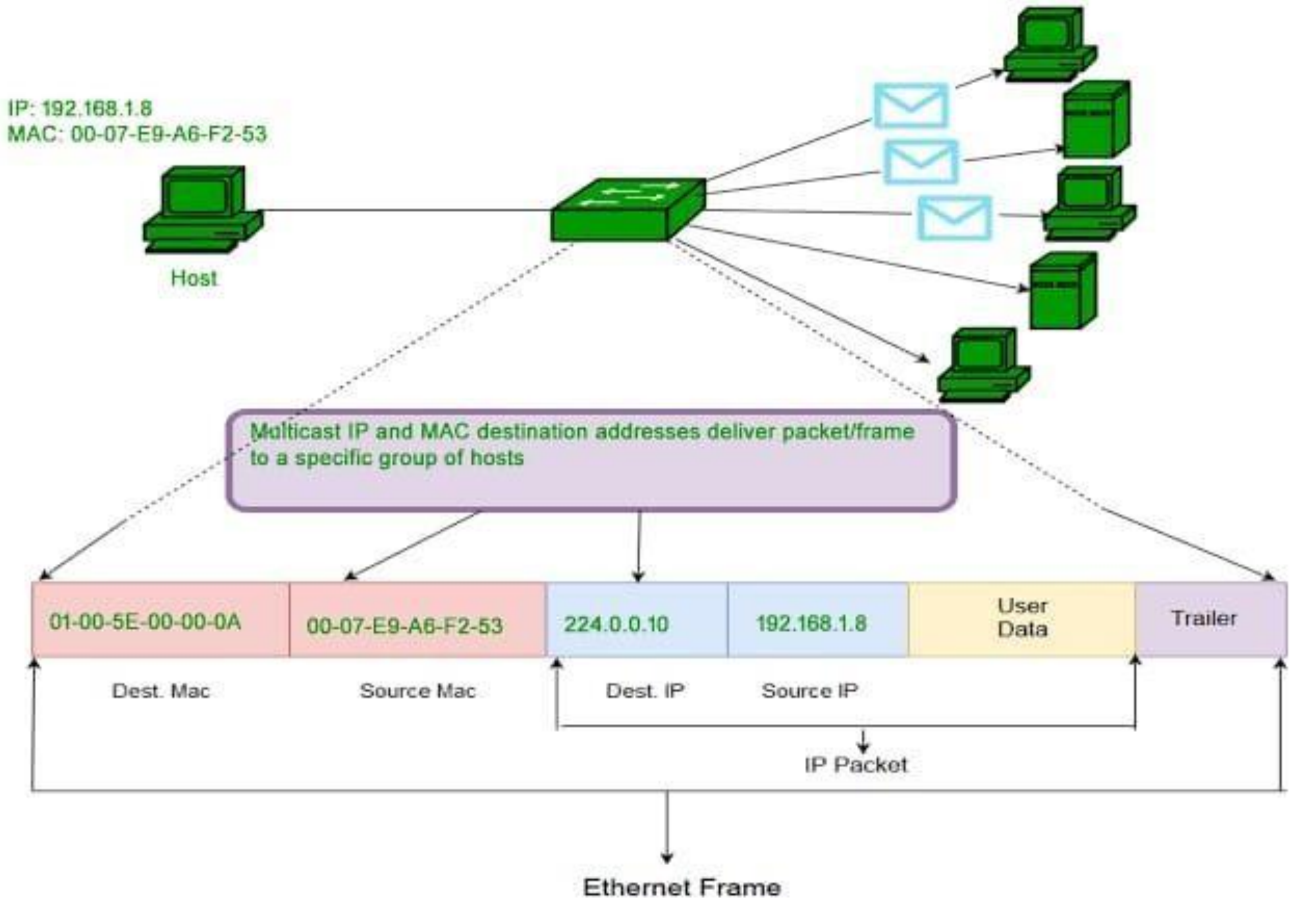
Port	Mac
1	A
3	X
3	Y

The image part with relationship ID rId20 was not found in the file.



address of host B and the MAC address of host C.





MAC flooding happens when the attacker tries to send numerable invalid MAC addresses to the MAC table. It floods the source table with the invalid MAC addresses. Once the MAC table reaches the assigned limit of the MAC table, it starts to remove the valid MAC addresses.

IMPLEMENTATION

Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address. These are the methods often used to prevent the MAC Flooding attack.

The idea behind a MAC flooding attack is to send a huge amount of ARP replies to a switch, thereby overloading the cam table of the switch. Once the switch overloads, it goes into hub mode, meaning that it will forward the traffic to every single computer on the network. All the attacker needs to do now is run a sniffer to capture all the traffic.

This attack does not work on every switch; lots of newer switches have built-in protection against an attack.

1. **ROUTER (1941)**
2. **WIRELESS ROUTER**
3. **SWITCH**
4. **LAPTOP**
5. **PRINTER**
6. **PC**

Switches maintain a MAC table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as an Ethernet hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for.

In a typical MAC flooding attack, a switch is fed many Ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table.

The effect of this attack may vary across implementations, however the desired effect (by the attacker) is to force legitimate MAC addresses out of the MAC address table, causing significant quantities of incoming frames to be flooded out on all ports. It is from this flooding behavior that the MAC flooding attack gets its name.

After launching a successful MAC flooding attack, a malicious user can use a packet analyzer to capture sensitive data being transmitted between other computers, which would not be accessible were the switch operating normally. The attacker may also follow up with an ARP spoofing attack which will allow them to retain access to privileged data after switches recover from the initial MAC flooding attack.

MAC flooding can also be used as a rudimentary VLAN hopping attack

To prevent MAC flooding attacks, network operators usually rely on the presence of one or more features in their network equipment:

With a feature often called "port security" by vendors, many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations. A smaller table of *secure* MAC addresses is maintained in addition to (and as a subset to) the traditional MAC address table.

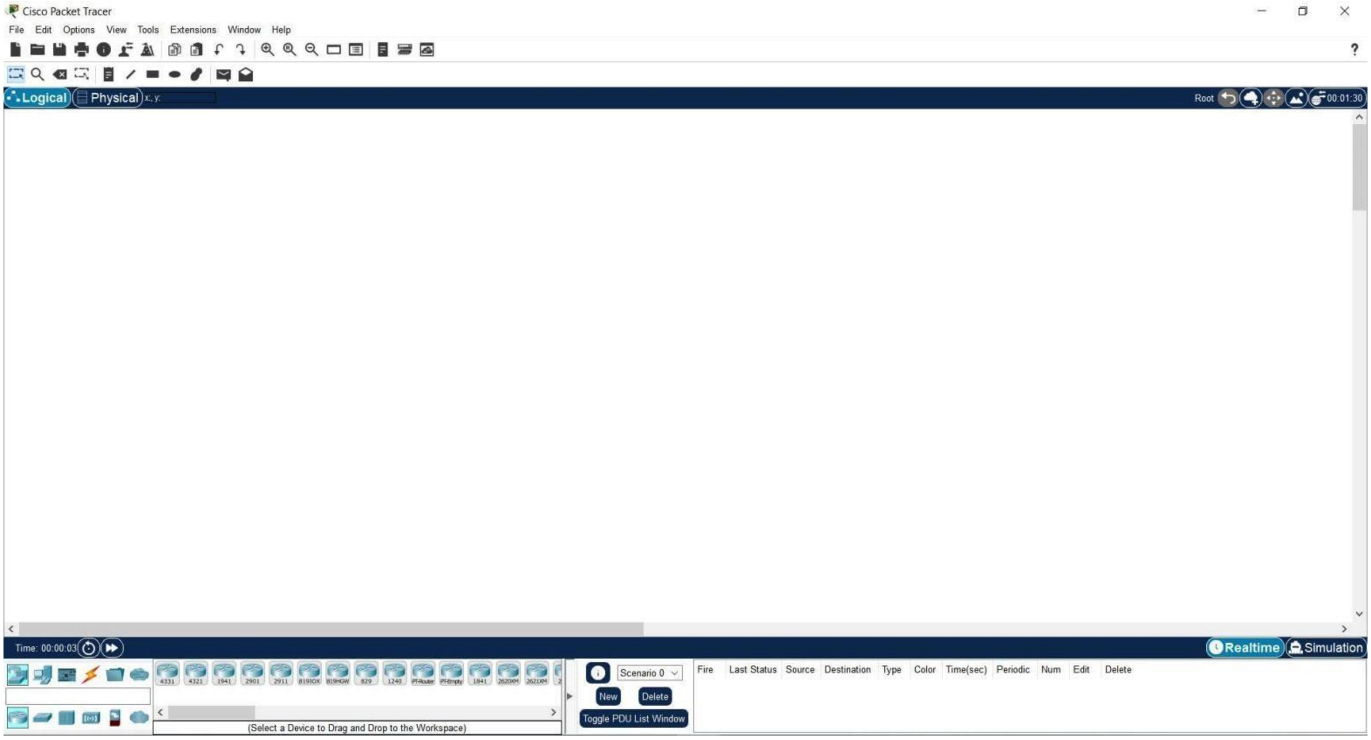
Many vendors allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered.

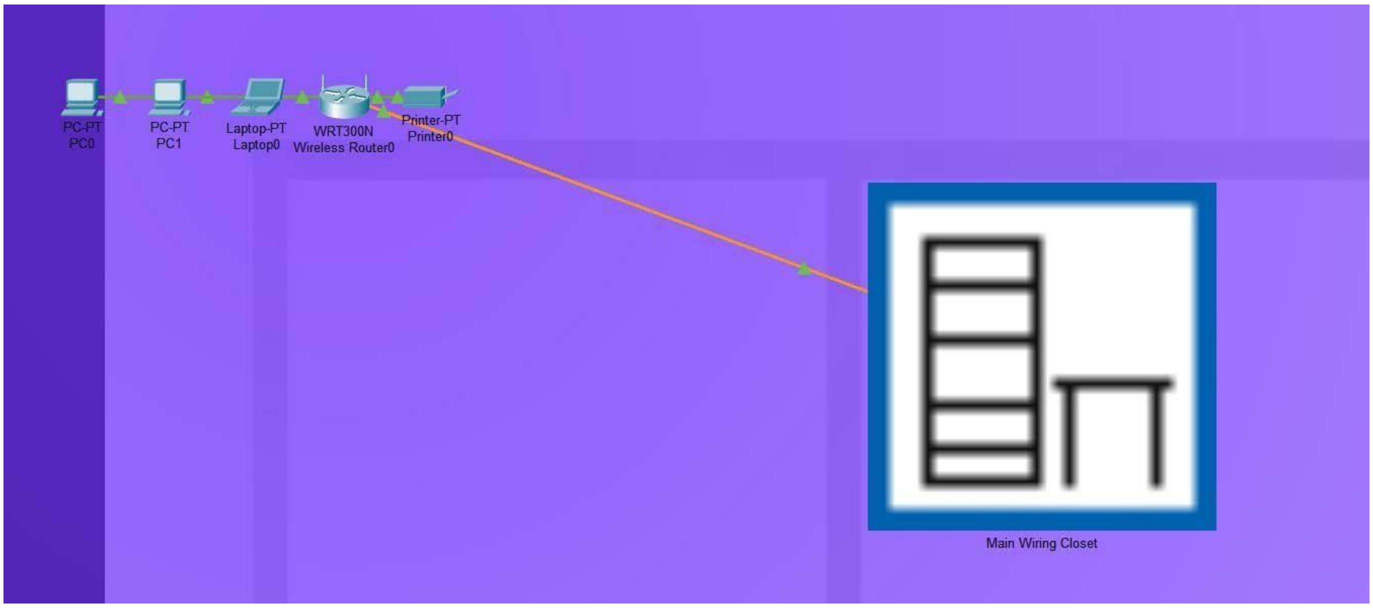
Implementations of IEEE 802.1X suites often allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

Security features to prevent ARP spoofing or IP address spoofing in some cases may also perform additional MAC address filtering on unicast packets, however this is an implementation-dependent side-effect.

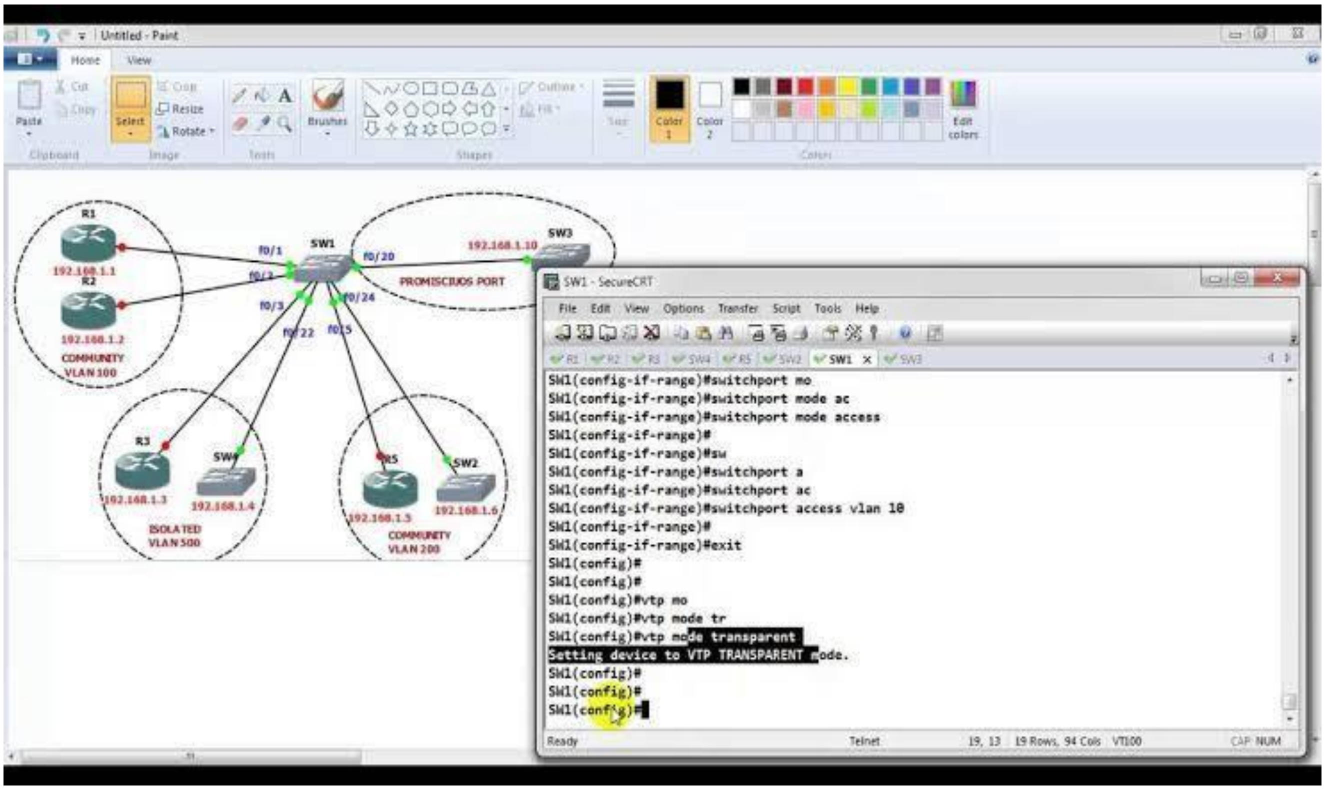
Additional security measures are sometimes applied along with the above to prevent normal unicast flooding for unknown MAC addresses. This feature usually relies on the "port security" feature to retain all *secure* MAC addresses for at least as long as they remain in the ARP table of layer 3 devices. Hence, the aging time of learned *secure* MAC addresses is separately adjustable. This feature prevents packets from flooding under normal operational circumstances, as well as mitigating the effects of a MAC flood attack.

PACKET TRACER

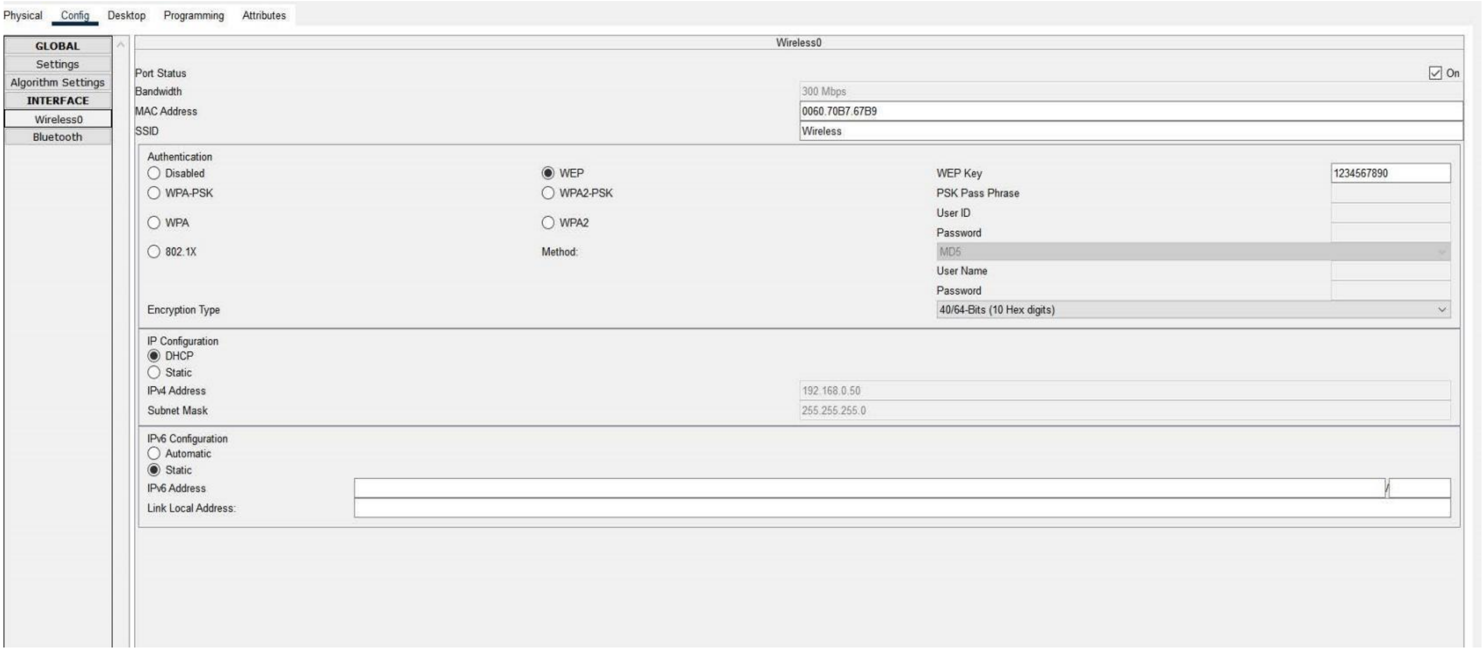

Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
00:01:30
Time: 00:00:03
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)



ASSIGNING IP ADDRESS



```
SW1(config-if-range)#switchport mo
SW1(config-if-range)#switchport mode ac
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#
SW1(config-if-range)#sw
SW1(config-if-range)#switchport a
SW1(config-if-range)#switchport ac
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#
SW1(config-if-range)#exit
SW1(config)#
SW1(config)#
SW1(config)#vtp mo
SW1(config)#vtp mode tr
SW1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SW1(config)#
SW1(config)#
SW1(config)#
```



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0060.70B7.67B9

SSID Wireless

Authentication

○ Disabled ● WEP WEP Key 1234567890

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.0.50

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

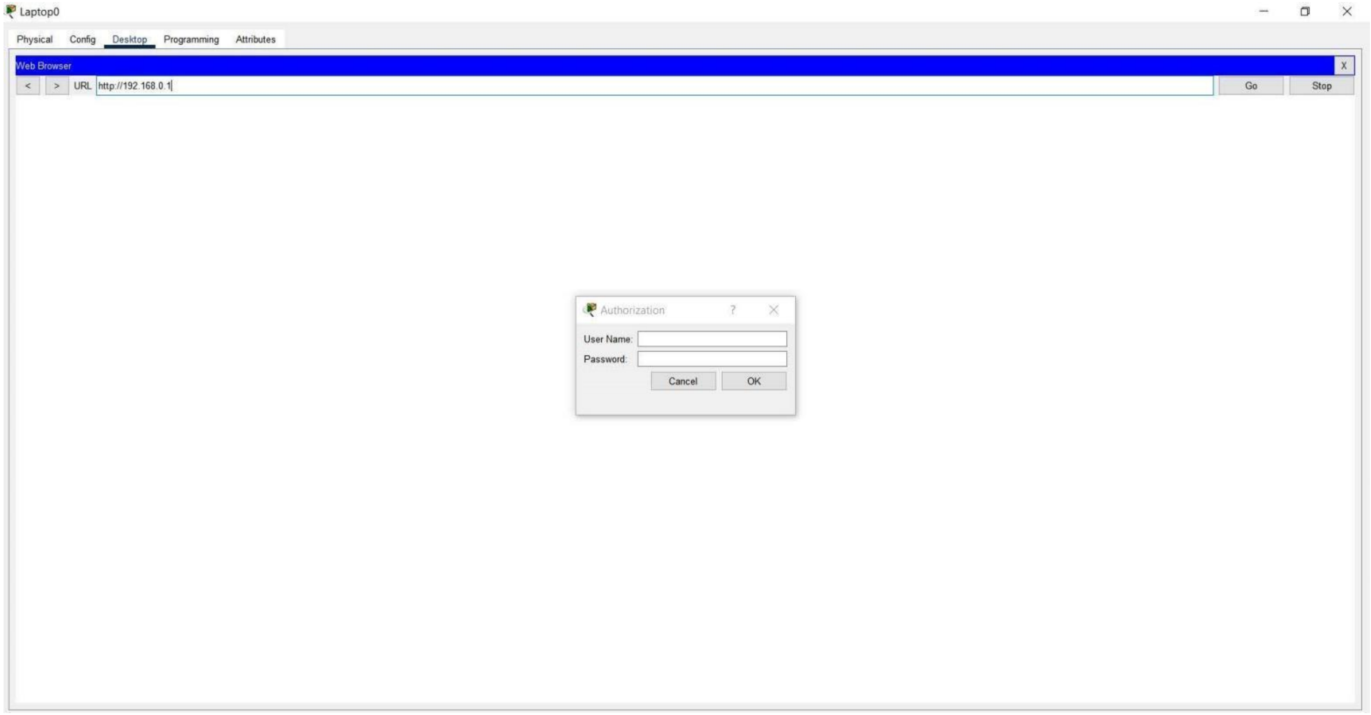
● Static

IPv6 Address /

Link Local Address:

Admin Login:

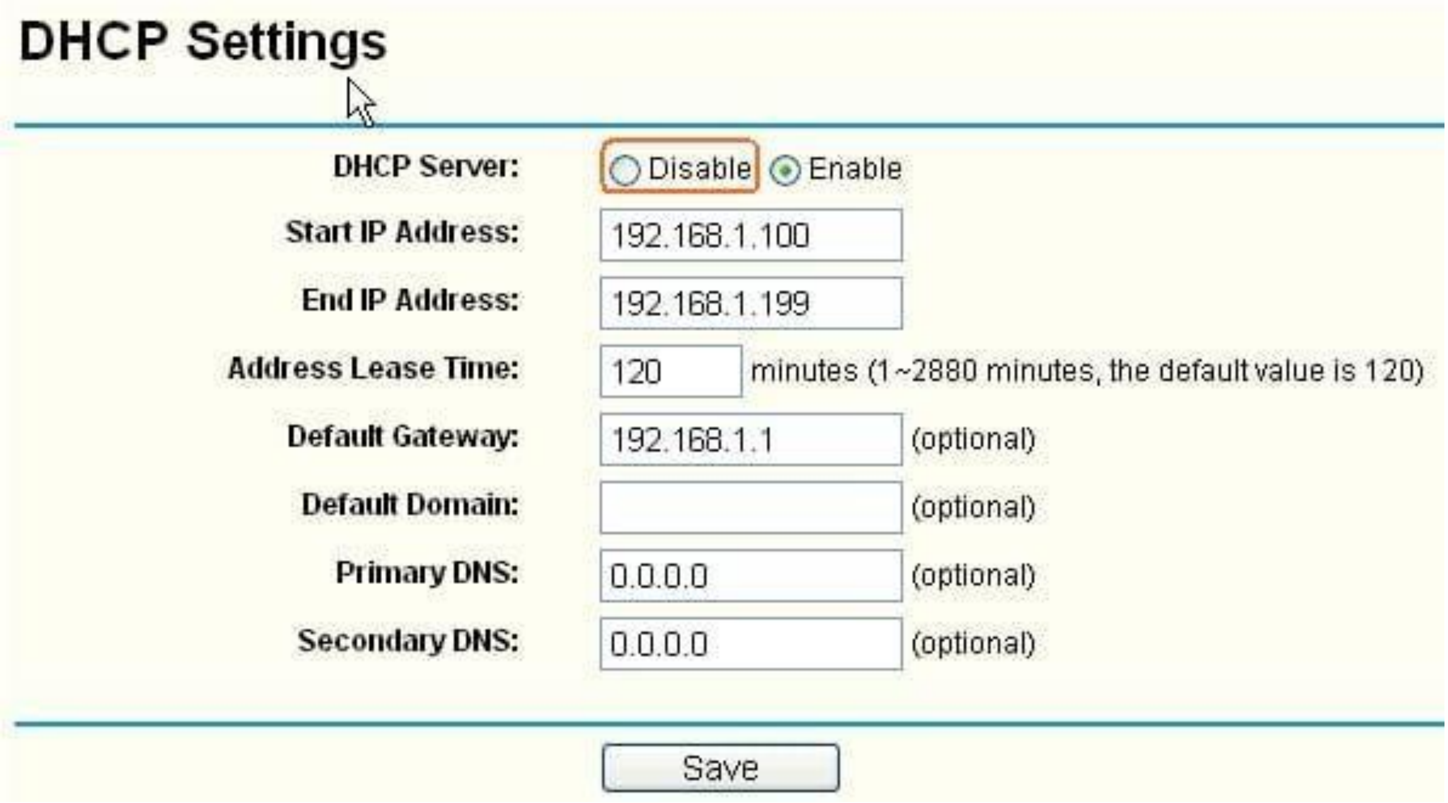
The Admin login inputs Admin’s ID and password and verifies the login credentials.



URL http://192.168.0.1

User Name:

Password:



DHCP Settings

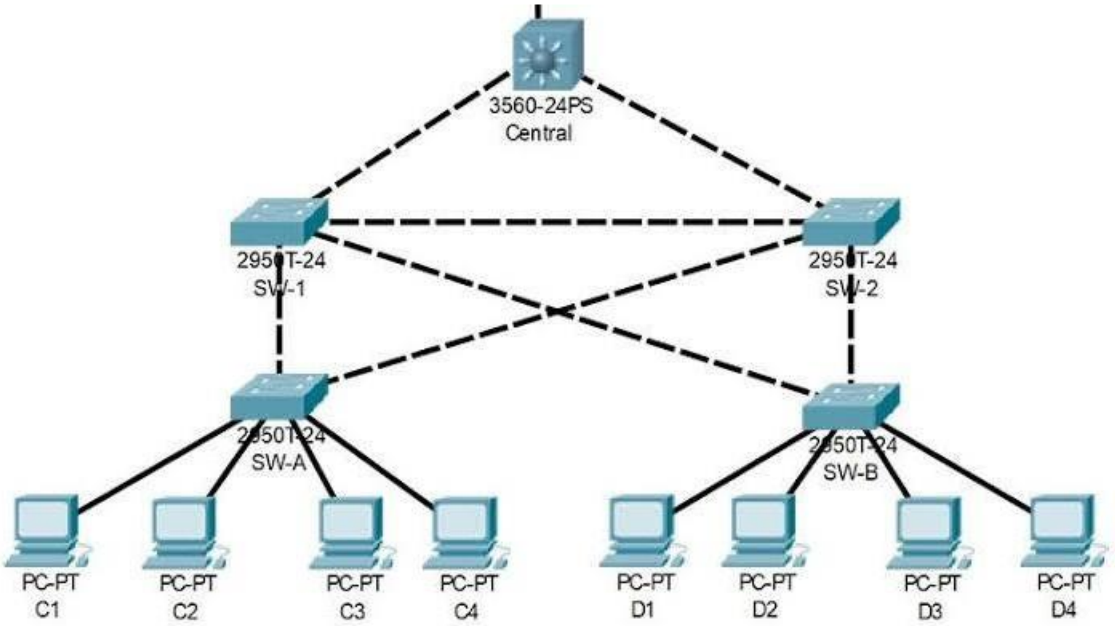
DHCP Server:	○ Disable ● Enable
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.199
Address Lease Time:	120 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.1.1 (optional)
Default Domain:	(optional)
Primary DNS:	0.0.0.0 (optional)
Secondary DNS:	0.0.0.0 (optional)

EXPERIMENT RESULTS AND ANALYSIS

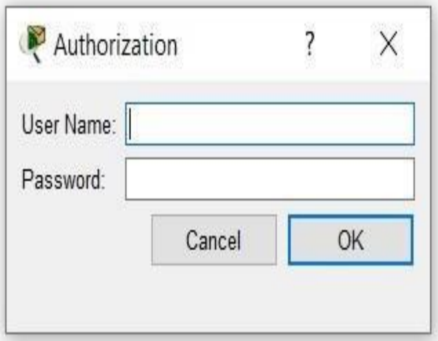
RESULTS

MAC flooding attack is very intensive attack today in the lowest network level. We examined the scope of the attack in detail and suggest some new methods to prevent the effect of MAC flooding attack. Exact differentiation of processing is available. So clear cut output should be obtained.

WORKING MODEL DIAGRAM:



Autentication details for an user:



CONCLUSION AND SCOPE

The effects of a MAC flooding attack can differ considering how it is implemented. It can result in the leak of personal and sensitive information of the user that could be used for malicious purposes, so its prevention is necessary. A MAC flooding attack can be prevented by many methods including the authentication of discovered MAC addresses against “AAA” Server, etc.

A data link layer acts as a medium for communication between two directly connected hosts. At the sending front, it transforms the data stream into signals bit by bit and transfers it to the hardware. On the contrary, as a receiver, it receives data in the shape of electrical signals and transforms them into an identifiable frame.

MAC can be classified as a sublayer of the data link layer that is accountable for physical addressing. MAC address is a unique address for a network adapter allocated by the manufactures for transmitting data to the destination host. If a device has several network adapters i.e., Ethernet, Wi-Fi, Bluetooth, etc., there would be different MAC addresses for each standard.

In this article, you'll learn how this sublayer gets manipulated to execute the MAC flooding attack and how we can prevent the attack from happening.

MAC (Media Access Control) Flooding is a cyber-attack in which an attacker floods network switches with fake MAC addresses to compromise their security. A switch does not broadcast network packets to the whole network and maintains network integrity by segregating data and making use of VLANs (Virtual Local Area Network).

The motive behind MAC Flooding attack is to steal data from a victim's system that is being transferred into a network. It can be achieved by forcing the switch's rightful MAC table contents out, and the switch's unicast behavior. This results in the transfer of sensitive data to other parts of the network and eventually turning the switch into a hub and causing significant quantities of incoming frames to be flooded out on all ports. Therefore, it is also called the MAC address table overflowing attack.

All the legitimate users will now be able to make an entry until this is completed. In these situations, malicious entities make them a part of a network and send malicious data packets to the user's computer.

As a result, the attacker will be able to capture all the ingoing and outgoing traffic passing through the user's system and can sniff the confidential data it contains. The following snapshot of the sniffing tool, Wireshark, displays how the MAC address table is flooded with bogus MAC addresses.

Project Scope

Mac-flooding is an attack by which the attacker attempts to fill the mac-address table of the switch, by simulating random mac-addresses. The project aims to demonstrate the concept of mac-flooding by using packet crafting tools like scapy in a test lab.

REFERENCES

L. Senecal, “Understanding and preventing attacks at layer 2 of the OSI reference Model”, 4th annual communication Networks and Services conference (2006) William Stallings, “Cryptography and network Security”, Fourth edition, Pearson Education. Sumit Dhar, “Switch Sniff, Linux Journal” (2002)

Tapan P Gondaliya, Maninder Singh, “Intrusion Detection System on MAC layer for attack prevention in MANET”, Fourth International conference on computing, Communications and Networking technologies”,2013 [5] Larsen, R. Trip and C. R. Johnson, “Methods for procedures related to the electrophysiology of the heart”, U.S. Patent 5,529,067, (1995) June 25. [6] Mallesham Dasani, Stony Brook, “Real Time Detection of MAC Layer DOS attack in IEEE 802.11 wireless networks”,14th IEEE Annual Consumer Communications And Networking conference (2017)