**California State Polytechnic University Pomona**

Department of Electrical and Computer Engineering

ECE 4311

Section 01

Network Forensics

Final Term Project

Smart Home IoT Threat Assessment

Prepared by:

Hector Arvizu, Myriam Boutros, Hennessy Olguin, and Chanel Williams

Presented to:

Professor Tamer Omar

29 November 2023

**ABSTRACT**

The rapid integration of Internet of Things (IoT) devices into smart homes has significantly enhanced convenience and automation. However, this proliferation has also exposed vulnerabilities, as these devices become potential targets for malicious activities. This paper explores the threats posed by ARP spoofing, IP spoofing, MAC flooding, and DHCP starvation attacks in the context of smart home IoT environments. By manipulating key networking protocols, adversaries can compromise the integrity and security of smart home systems, leading to unauthorized access, data breaches, and service disruptions. To address these threats, we propose a comprehensive framework for prevention, leveraging security measures and best practices to fortify smart home networks against these sophisticated attacks.

**Table of Contents**

Title Page………………………………………………………………………………… 1

Abstract…………………………………………………………………………………... 2

Table of Contents………………………………………………………………………… 3

Introduction………………………………………………………………………………. 4

ARP Spoofing…………….……………………………………………………………… 5

IP Spoofing………...…………………………………………………………………….. 7

MAC Flooding…………………………………………………………………...………11

DHCP Starvation……………………………………………………………...…………15

Summary of Challenges and Resolutions………………………………………………..17

Conclusions……………………………………………………………………………....19

References………………………………………………………………………………..20

**INTRODUCTION**

The advent of Smart Home Internet of Things (IoT) devices has revolutionized the way we interact with and manage our living spaces. From intelligent thermostats to connected cameras, these devices offer unparalleled convenience and control. However, this increased connectivity also introduces new challenges, particularly in terms of cybersecurity. As smart homes become more interconnected, the vulnerabilities associated with traditional networking protocols such as ARP (Address Resolution Protocol), IP (Internet Protocol), MAC (Media Access Control), and DHCP (Dynamic Host Configuration Protocol) become potential entry points for malicious actors.

This paper focuses on the specific threat landscape posed by ARP spoofing, IP spoofing, MAC flooding, and DHCP starvation attacks within the context of smart home environments. ARP spoofing involves the manipulation of the ARP cache to associate an attacker's MAC address with a legitimate IP address, enabling unauthorized interception of data. IP spoofing allows adversaries to send packets with a false source IP address, leading to identity deception and potential unauthorized access. MAC flooding overwhelms the network switch's MAC address table, causing it to operate inefficiently or even fail, while DHCP starvation exhausts available IP addresses, disrupting network connectivity.

SOFTWARE DESCRIPTION

****

**CISCO Packet Tracer:** Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

**ARP spoofing**

ARP (Address Resolution Protocol) spoofing is a technique used by attackers to intercept and manipulate network traffic. ARP is a protocol used to map an IP address to a physical (MAC) address on a local network. When devices communicate within a network, they use ARP to discover the MAC address associated with a given IP address.

In ARP spoofing, an attacker sends false or “spoofed” ARP messages to associate their own MAC address with the IP address of another device on the network, such as a router or a specific user’s computer. Once this connection is established, the attacker can intercept, modify, and or block the communication between the two parties. ARP Spoofing has many ways on how to attack some including Denial of Service (DoS), Man in the Middle (MitM), and Session Hijacking. Denial of Service attacks by manipulating ARP tables. An attacker can disrupt network communication, causing a denial of service for legitimate users. Man in the Middle attacks by intercepting and forwarding traffic between two parties, an attacker can eavesdrop on sensitive information, such as login credentials. Session Hijacking attacks by using man in the middle, so once the attacker is in the man in the middle position an attacker can hijack established sessions, gaining unauthorized access to sensitive systems or data.

A computer screen shot of a network

Description automatically generated

* PC0
  + 192.168.1.10
  + 00:02:16:49:B0:EE
* Router 1
  + 192.168.1.254
  + 00:D0:FF:8B:99:02
* Web Server
  + 192.168.2.100
* PC1 (Threat)
  + 192.168.1.20
  + 00:06:70:80:20:A8

**Figure A: ARP Spoofing Attack Schematic and Simulations Plus IP and MAC addresses**

In Figure A, we used two personal computers, two switches, one network sniffer, one router, and a web server. One of the PCs is used as a main PC to connect from the router to the web server, while the other PC is used as a threat computer in order to “spoof” the router and main PC. In order for PC0 to communicate with the router to get to the web server, it needs to know the MAC address of the default gateway. Once we successfully get PC0 to understand what the default gateway's IP and MAC address is, we have to make sure the threat PC (PC1) also knows what the default gateway is. ​ ​

A screenshot of a computer

Description automatically generated A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

**Figure B (Top Left), Figure C (Top Right), Figure D (Bottom Middle)**

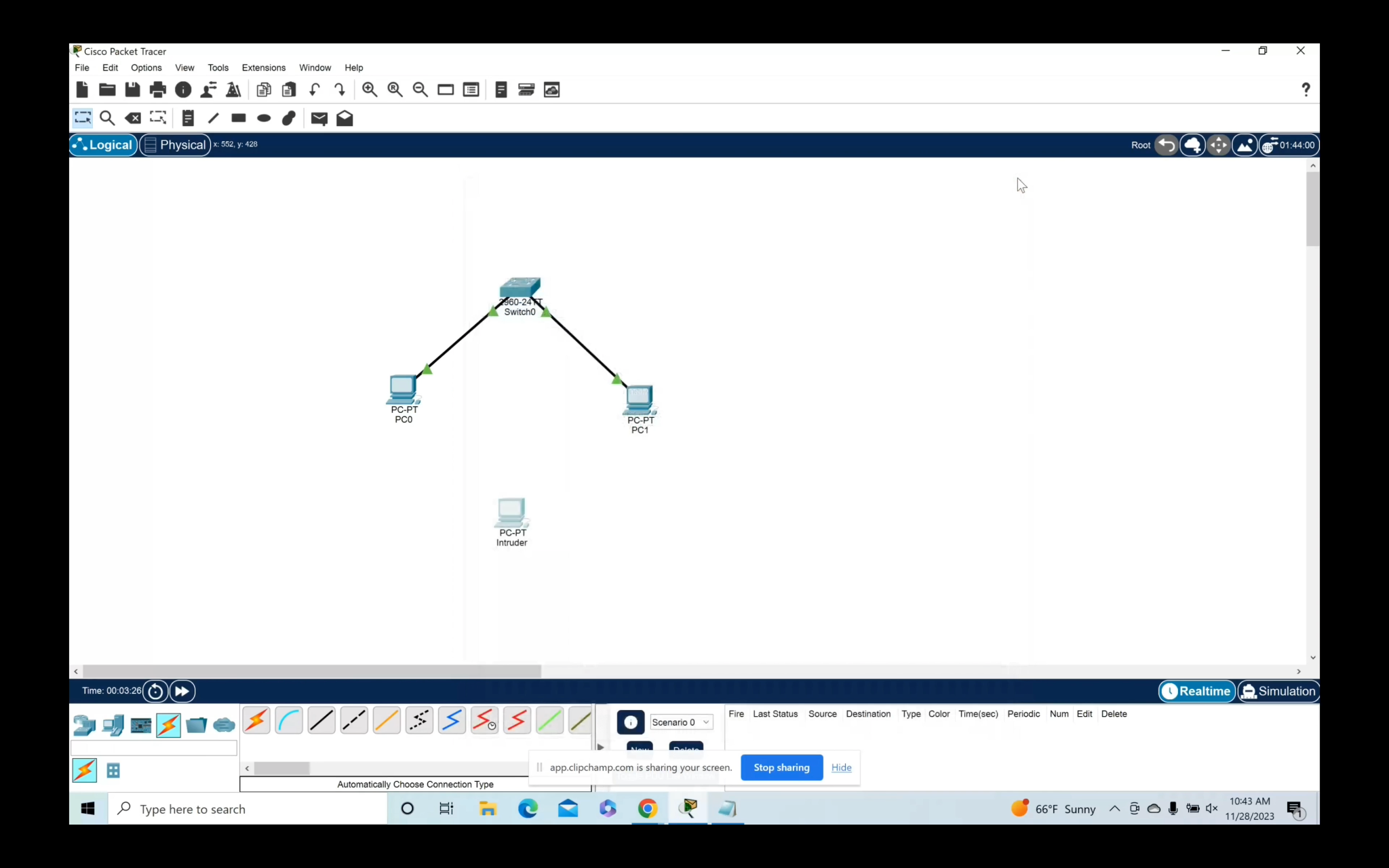
Once that is successful, we manually change the threat PC's MAC address to the MAC address router 1 has, so they are the same and the threat PC (PC1) can be able to spoof router 1 (**Figure D**). Then, we run a constant ping **(Figure B**) to talk to the IP address of PC0 with the source being the spoofed MAC address. The ARP cache for PC0 (**Figure C**) will now show the IP address for the original source, Router 1, and the spoofed source (Threat PC1) , indicating that the Man in the Middle attack was completed.

After exploring and analyzing how ARP spoofing attacks work, possible ways to prevent ARP Spoofing is to use a static ARP, use packet filtering, use a Virtual Private Network (VPN), or run a spoofing attack. A static ARP refers to a configuration where a network administrator manually creates and maintains a mapping between IP addresses and their corresponding MAC addresses. A packet filter is a network security mechanism that operates at the network layer of the OSI model and is used to control the flow of data packets based on a set of defined rules. Packet filtering solutions can identify spoofed ARP packets by seeing that they contain conflicting source information and stop them before they reach devices on the network. A VPN is a technology that establishes a secure and encrypted connection over the internet, allowing users to access a private network from a remote location as if they were physically connected to that network locally. This makes all communication encrypted and worthless for an ARP spoofing attacker. Lastly, running a spoofing attack checks if existing defenses are working. If the attack succeeds, then weak points need to be identified in defensive measures and need to be remediated.

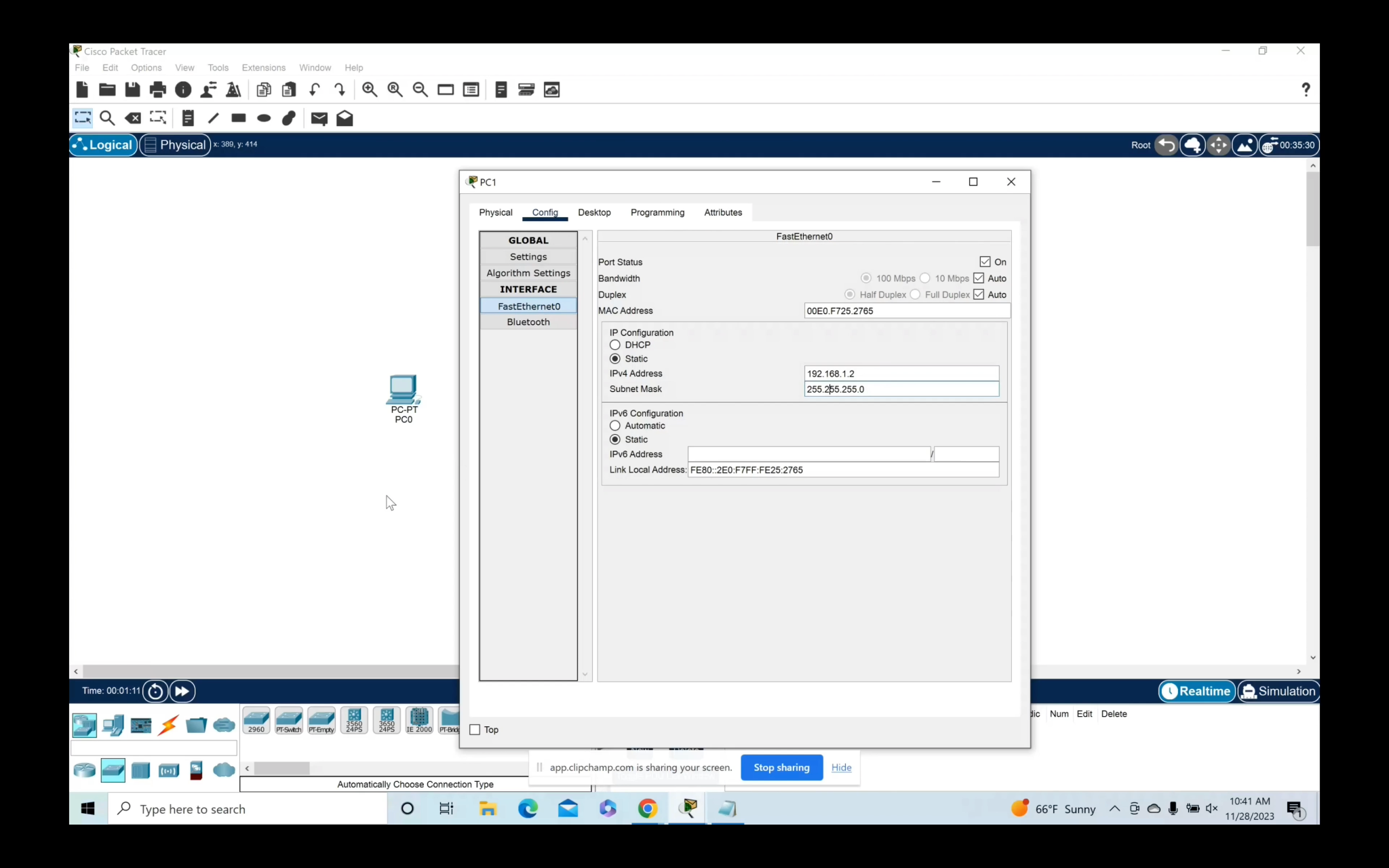
**IP spoofing**

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure. In a smart home environment, devices such as laptops and office computers located inside a smart house are vulnerable to this sort of attack. For this example, we’ll be demonstrating a simple IP Spoof attack on an office computer located in someone’s home.

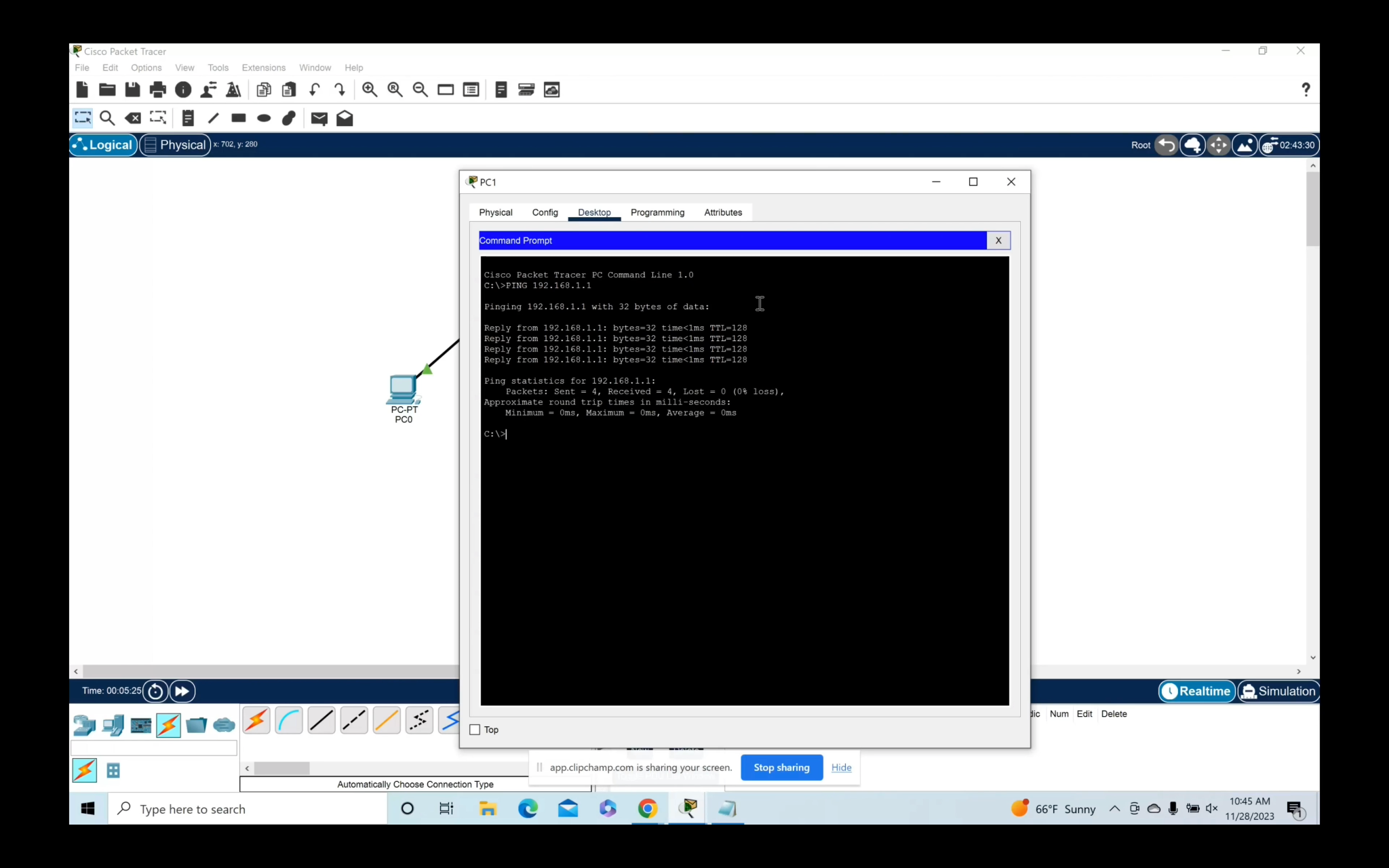
In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering. In this simplified example, a switch is used to connect an intruder computer to a victim computer through the network.



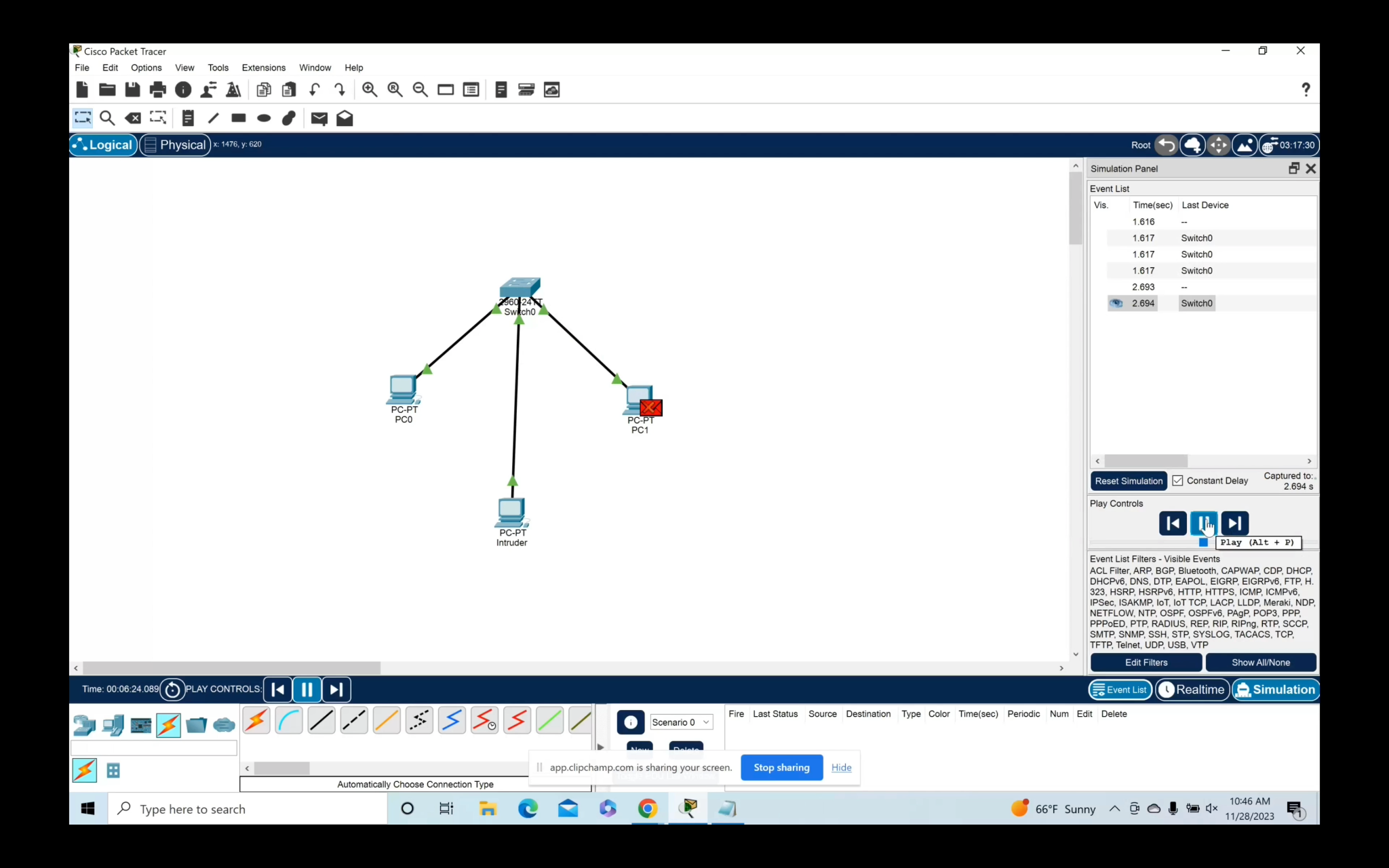
From here we will create the IPs for each computer and make the corresponding network links. Shortly after, we copy the same IP and MAC addresses from the victim computer.

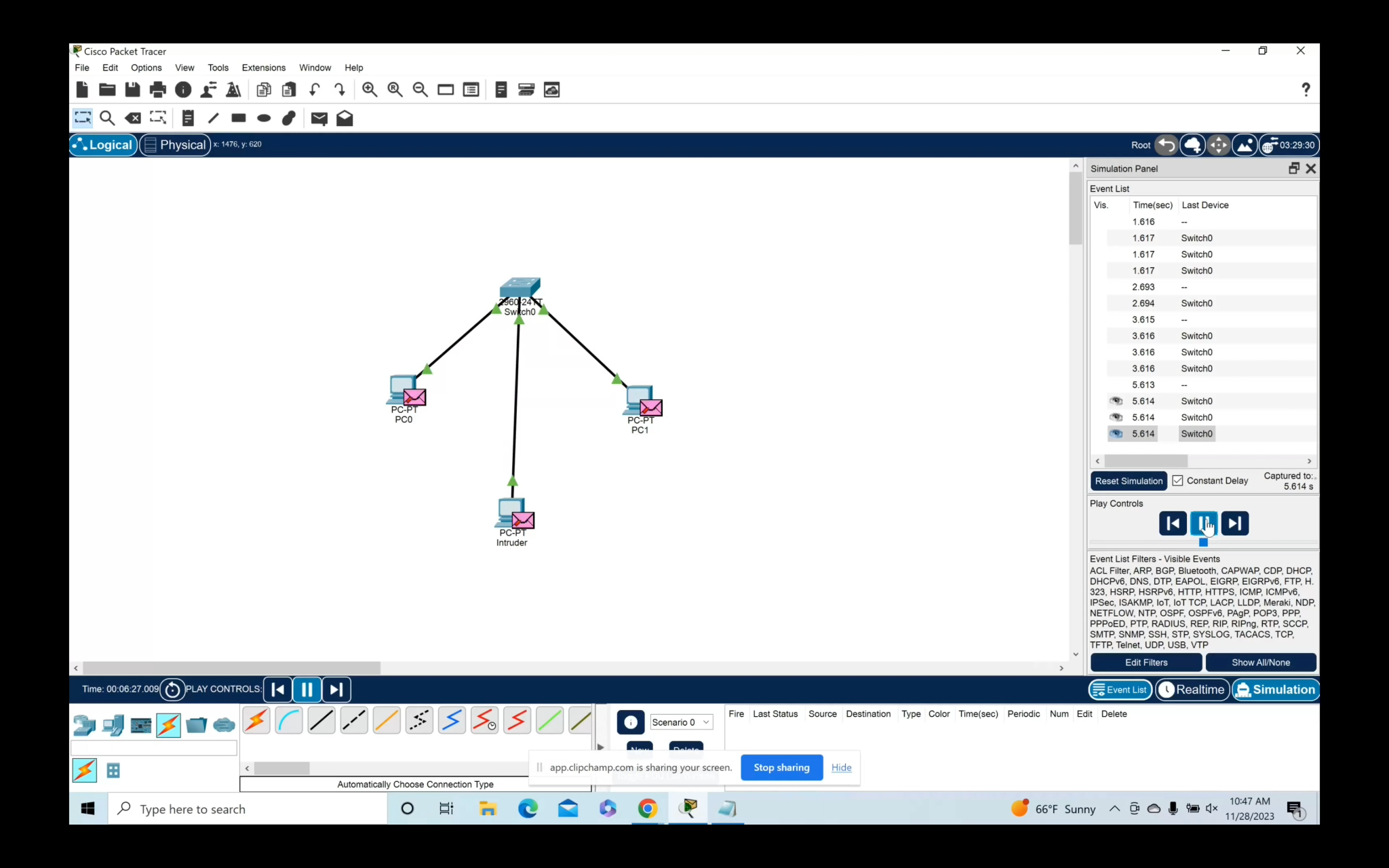


After we make the network connection, we will create a PING in order to create the ARP table. This process is done on our network and victim computer, rather than on the intruding computer.



Finally, we proceed to send the packages to the victim team, before spamming every computer with authorized IP addresses.





After running through this simplified scenario, and after learning about how IP Spoofing attacks generally work, there are ways to prevent these sorts of attacks. Below is a list of several examples on how to prevent IP Spoofing.

* Firewalls: Firewalls can be used to help detect any suspicious IP addresses and any suspicious traffic trying to enter your network.
* New Verification Methods: By using stronger methods, it increases a device's defenses from outside sources that are trying to connect to your network based on IP addresses. Other methods can also help verify websites that are trying to connect to your network.
* HTTPS Websites: Some websites offer secure protocols, but using HTTPS websites is a much safer way to help users detect dangerous websites while browsing through the internet.
* Antivirus Protection: Using reliable and affordable security software can help verify and detect any suspicious activity.

**MAC flooding**

MAC flooding is a type of network attack that targets the layer 2 (Data Link layer) of the OSI model. In a typical Ethernet network, each device on the network has a unique Media Access Control (MAC) address, which is a hardware address assigned to the network interface card (NIC). The MAC address is used to identify devices on a local network. In a MAC flooding attack, the attacker attempts to overload the switch's MAC address table. Switches use MAC address tables to keep track of which devices are connected to each of their ports. When a device sends a frame to the switch, the switch learns the source MAC address of the frame and associates it with the port through which the frame arrived.

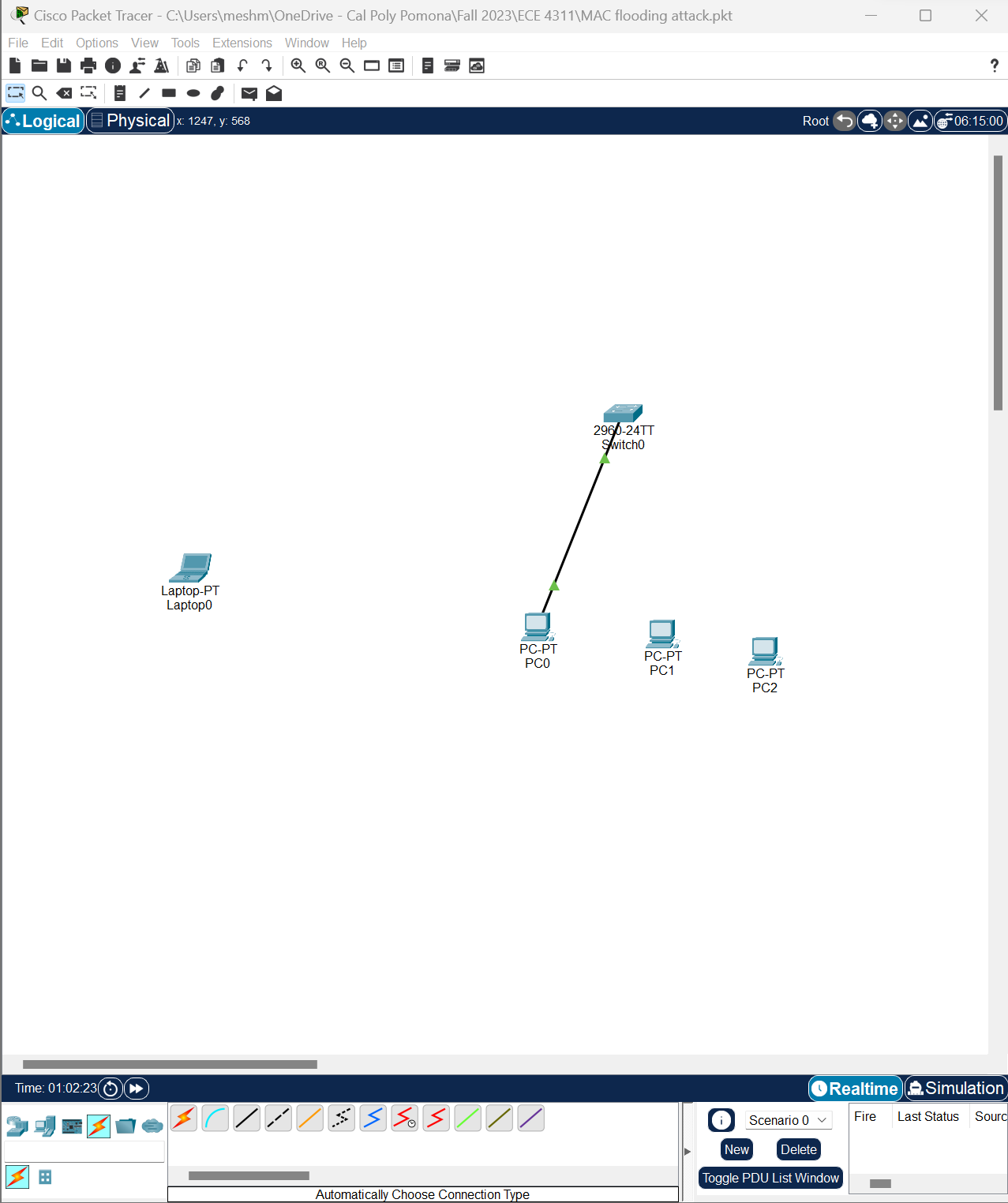
There are three ways to attack using MAC flooding:

Sending a Flood of Frames: The attacker floods the switch with a large number of frames, each containing different source MAC addresses. These MAC addresses may be randomly generated or taken from legitimate devices on the network.

Overloading the MAC Address Table: Since switches have a limited size for their MAC address tables, the flood of frames causes the table to fill up quickly. As the table becomes full, the switch starts behaving like a hub rather than a switch. In a hub-like mode, the switch forwards incoming frames to all of its ports, regardless of the destination MAC address.

Packet Sniffing or Man-in-the-Middle Attacks: With the switch in this hub-like mode, the attacker can sniff or intercept the network traffic, potentially capturing sensitive information or launching further attacks.

In Cisco, I've set up three PCs that are going to be allowed on the network through the switch. I've also set up a laptop that will act as the attacker/hacker. While setting up the switch, I allowed the switch to record and allow the PCs physical addresses. If an attacker connects to the switch, I have enabled the shutdown mode on the switch which will disable the connection.

****

Code to set up the switch:

en

conf t

int f0/1

switchport mode access

switchport port-security

switchport port-security maximum 3

switchport port-security violation ?

switchport port-security violation shutdown

switchport port-security mac-address ?

switchport port-security mac-address sticky

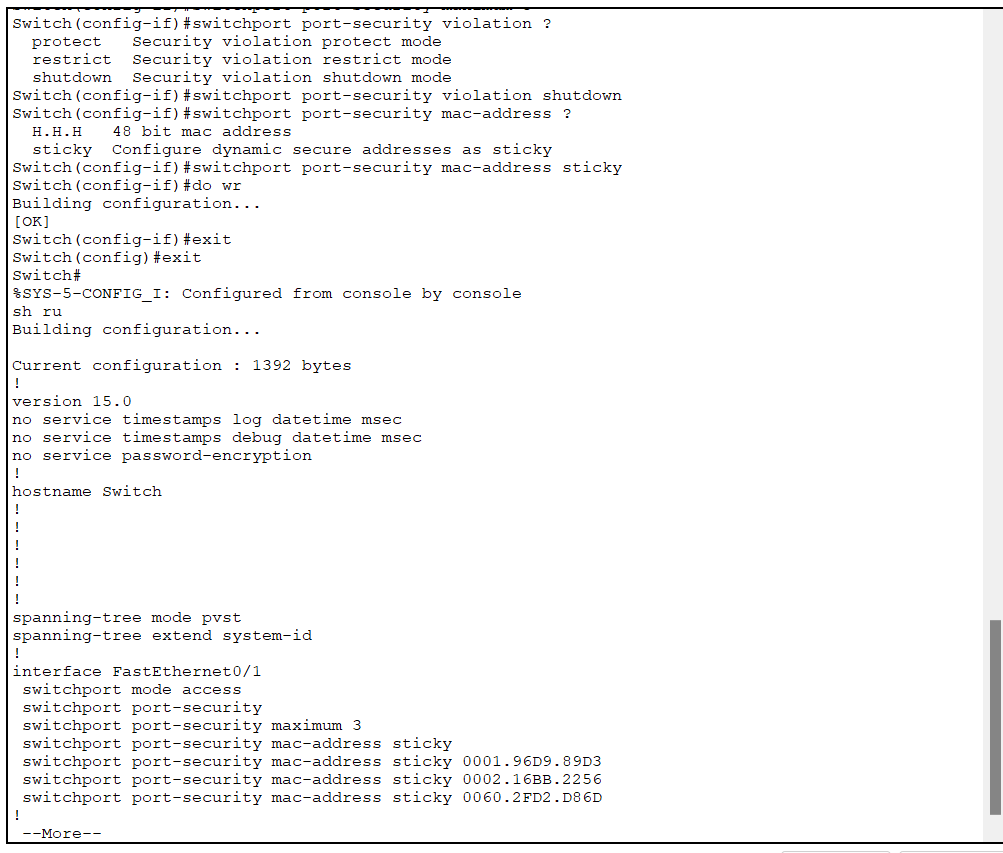
do wr

exit

exit

sh ru

(enter to see the rest of the mac addresses)

****A screenshot of a computer program

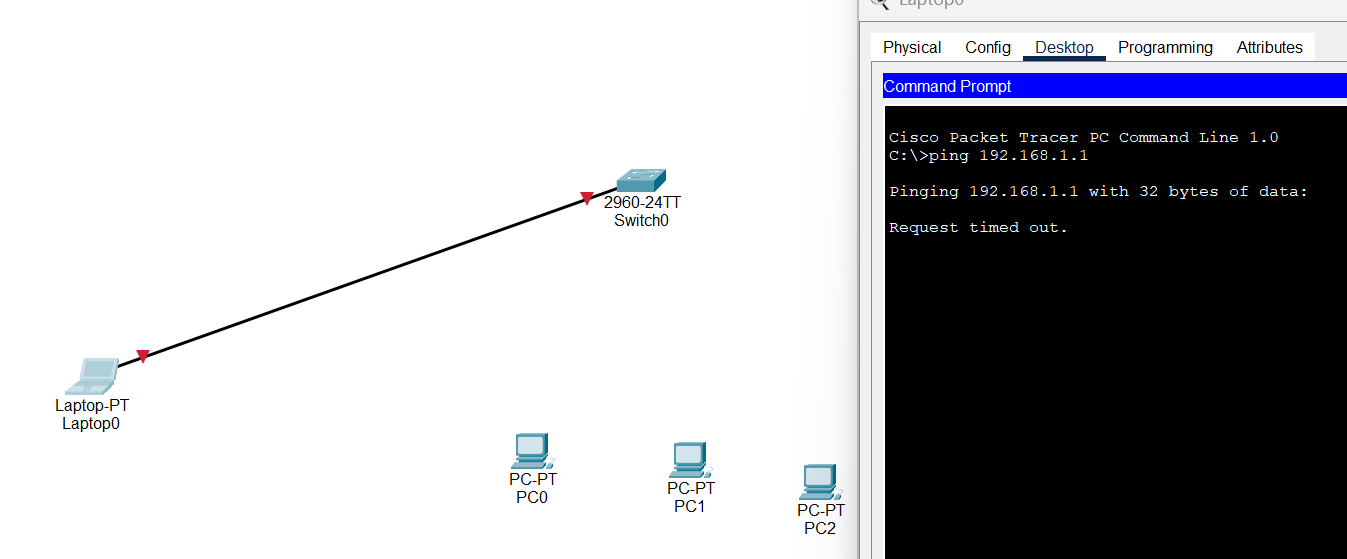
Description automatically generated

Prevention modes:

Protect Mode: In this mode, if a violation occurs (e.g., more MAC addresses are detected than allowed), the switch takes a protective action. The switch can either disable the port (shutdown) or restrict further traffic until the violation is cleared by an administrator.

Restrict Mode: In restrict mode, the switch allows the traffic from the detected MAC addresses but generates a log message or sends an alert to the network administrator. The port remains operational, but the administrator is notified of the security violation.

Shutdown Mode: In shutdown mode (similar to protect mode), the switch disables the port when a violation occurs. The port remains in a shutdown state until manually re-enabled by an administrator. This is a more aggressive response compared to restrict mode.

In a smart home environment, various devices like smart thermostats, cameras, door locks, and other IoT devices are often connected to the local network. These devices communicate with each other and with a central hub or a cloud server. to make sure that the network is secure, the switch has to be set up with the correct maximum of devices and the physical addresses to record who has access. if the wrong device wants to connect, the switch will disable connection to prevent the attack. ****

There are many other ways to prevent a MAC flooding attack. Here are 4 ways:

1. Network Segmentation: Implement network segmentation to isolate IoT devices from critical network infrastructure. This can help contain the impact of a potential attack on IoT devices.
2. Security Best Practices: Follow security best practices for both the network infrastructure and individual IoT devices. This includes using strong passwords, regularly updating firmware/software, and enabling encryption where possible.
3. Intrusion Detection and Prevention Systems: Deploy intrusion detection and prevention systems to monitor network traffic for unusual patterns or activities. This can help in detecting and responding to MAC flooding attacks or other malicious activities.
4. Regular Security Audits: Conduct regular security audits to identify and address vulnerabilities in the smart home network. This includes reviewing the configuration of network devices and ensuring that security features are properly configured.

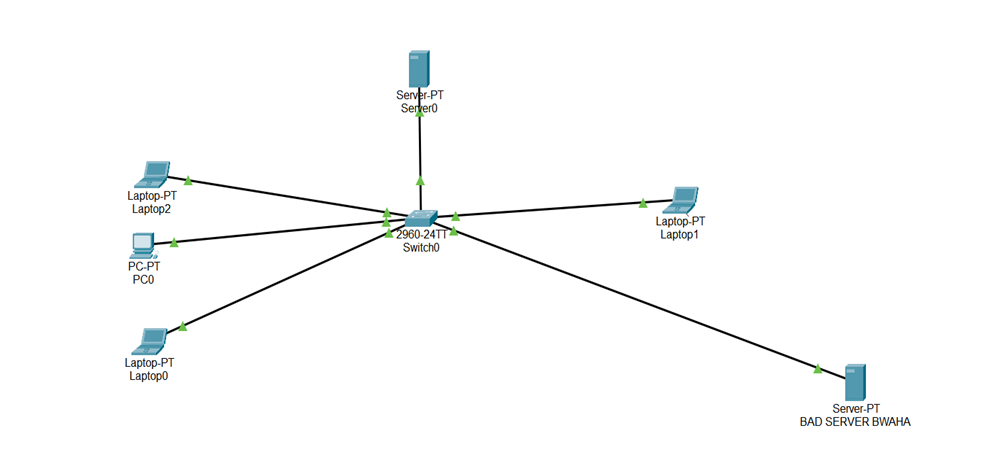
**DHCP Starvation**

A DHCP starvation attack is a type of cyber attack that aims to deplete the available IP addresses in a DHCP server’s address pool. This attack floods the DHCP server with a large number of fake or unauthorized DHCP requests, causing it to run out of available IP addresses to assign to legitimate devices.

An attacker wants to perform a DHCP starvation attack on this network. The attacker uses a tool that can generate many DHCP requests, each with a different MAC address. The tool sends these requests to the DHCP server in the home’s router. As the DHCP server receives these requests, it assigns an IP address to each one, thinking they are legitimate devices. Eventually, the DHCP server runs out of IP addresses to assign because all available addresses have been taken by the attacker’s fake requests.

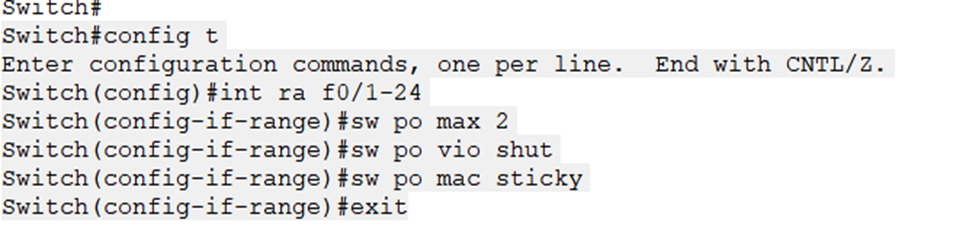
A couple of DHCP starvation attacks that can happen are DoS attacks and MITM attacks. DoS Attack: The attacker sends a flood of bogus DHCP Discover messages with spoofed MAC addresses. As a result, the DHCP server tries to respond to all these bogus messages, and the pool of IP addresses used by the DHCP server is depleted. A legitimate user won’t be able to get an IP address via DHCP. MITM Attack: The attacker can set up a rogue DHCP server to assign IP addresses to legitimate users. This rogue server can also provide the gateway router and DNS server to users. Now, all the network traffic can be routed via the attacker’s machine. This is nothing but the MITM attack. The benefit of that to the attacker is that if a bogus DHCP server is handing out IP addresses, including default DNS and gateway information, clients who use those IP addresses and start to use that default gateway can now be routed through the attacker’s machine

In a smart home scenario, this could prevent legitimate devices like computers and smart home devices from connecting to the network, as they can’t be assigned an IP address. This effectively causes a denial of service, disrupting the functionality of the smart home. To prevent such attacks, security measures like DHCP snooping and port security can be implemented.



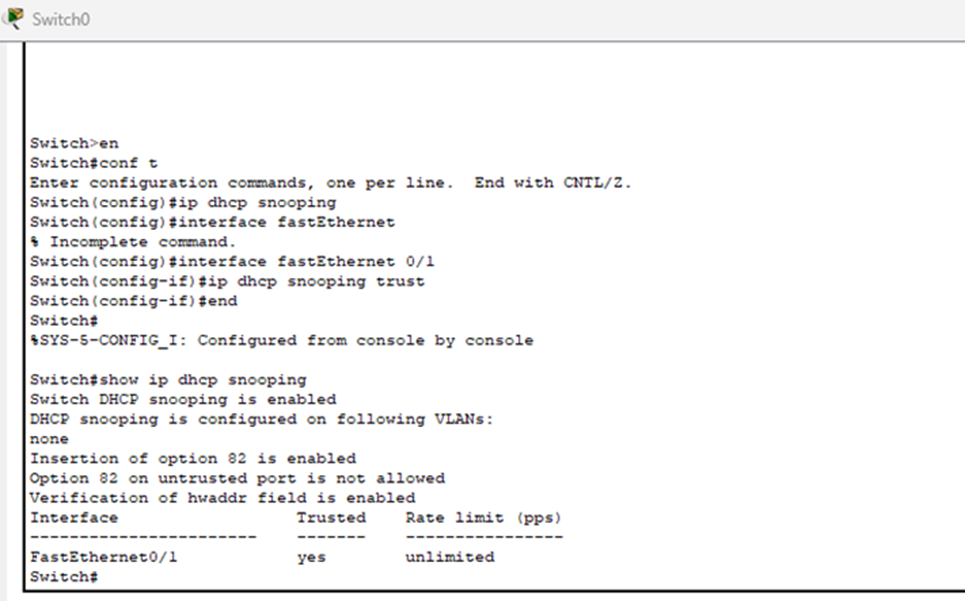
**Figure 1: DHCP Starvation Attack**

From Figure 1 I flood the DHCP server with DHCP DISCOVER packets. These are requests for IP addresses. Then used spoofed MAC addresses for these requests, so they appear to come from unique devices. Each request takes up one IP address from the server’s pool. The server thinks each request is coming from a unique device, it assigns a unique IP address to each one. Exhausting the pool of available IP addresses. Once the pool of IP addresses is exhausted, the DHCP server can’t assign IP addresses to legitimate devices. This prevents new devices from joining the network. I set up a rogue DHCP server on the network. This server responds to DHCP requests from devices, assigning them IP addresses and network configurations. With this server under control, I can manipulate the network configuration to carry out further attacks, such as MITM attacks.



**Figure 2 : Enabling Switch Port Security**

From Figure 2 I enabled port security. Port security on a switch can be enabled to mitigate DHCP starvation attacks. This involves accessing the switch’s command line, entering configuration mode, and selecting the ports to secure. Port security is then activated, and the maximum number of MAC addresses per port is set. The violation mode is set to ‘shutdown’, which disables the port if a violation occurs. Finally, sticky MAC addresses are enabled, allowing the switch to learn the MAC addresses of connected devices. Limiting the number of DHCP requests a single port can send, preventing DHCP starvation attacks.

****

**Figure 3: Enabling DHCP Snooping**

From Figure 3 I enabled DHCP Snooping. DHCP snooping is a security feature that monitors DHCP traffic, allowing packets only from trusted servers. It classifies switch ports into trusted and untrusted, blocking unauthorized traffic from untrusted ports. It also maintains a database of valid host IP and MAC address combinations. If a device connected to an untrusted port sends server messages, the switch discards them, indicating a potential attack. This feature helped protect the network from unauthorized DHCP servers and attacks.

**SUMMARY OF CHALLENGES AND RESOLUTIONS**

Challenge #1: ARP Spoofing

The most challenging part of ARP Spoofing was understanding and deciding which attack to use. From the three attacks mentioned before, Denial of Service and Session Hijacking were the most complicated to understand and gave some difficulty on learning how to execute an attack using them. For Denial of Service, a flooding attack would have been the best option but trying to figure out how to start is where the research and learning about the other attacks began. As for Session Hijacking, there was not enough information to give guidance about the attack. The more research done, the more confusion was built up when trying to process Session Hijacking.

Resolution #1: ARP Spoofing

After many hours of confusion and researching, it was well understood that the Man in the Middle attack can be considered as a Session Hijacking attack and vice versa. Long videos and articles helped grasp a better idea on what the attack was and how to implement it. The demonstrations ranged from simple to difficult which allowed for a better understanding of the attack.

Challenge #2: DHCP starvation

Understanding and executing a DHCP starvation attack required a solid understanding of networking protocols and cybersecurity principles. Since executing this attack is illegal, it was difficult to find information on how to implement the attack

Resolution #2: DHCP starvation

The few tutorials and forums that were found serve as a comprehensive guide, enriching understanding of DHCP starvation attacks and cybersecurity as a whole. These resources offer a deep dive into the technical aspects of these attacks, demonstrating how they’re executed and how they can be mitigated.

Challenge #3: MAC Flooding

In MAC flooding, if the MAC address table is not filled with the maximum number of devices, an attacker could hack into your network because the switch for example will not know that their Mac address is not allowed because there is still space for a device. for example, if the maximum is set to 3 and only two MAC addresses are on the table of the switch, the hacker is able to hack into the network since the switch will record their physical address as of the devices allowed in the network.

Resolution #3: MAC Flooding

One way to prevent this from happening is to make sure to set up the switch with the correct number of devices allowed and their physical addresses recorded on the switch. This will help the switch attack or shutdown any hacker from getting into your network.

**CONCLUSION**

The rise of Smart Home Internet of Things (IoT) devices has transformed our living spaces, offering unprecedented convenience and control. However, this increased connectivity also presents new cybersecurity challenges. As smart homes become more interconnected, traditional networking protocols such as ARP, IP, MAC, and DHCP can become potential entry points for malicious actors. This paper has explored the specific threats posed by ARP spoofing, IP spoofing, MAC flooding, and DHCP starvation attacks in smart home environments. Each of these attacks exploits vulnerabilities in networking protocols to disrupt network connectivity or gain unauthorized access. Using Cisco Packet Tracer as the environment, we’ve demonstrated how these attacks can be carried out and their potential impact on a network. This understanding is crucial for developing effective countermeasures and securing our increasingly connected homes against potential cyber threats.

**REFERENCES**

[1] Zuel, “DHCP Starvation attack demonstration,” YouTube. Jan. 26, 2019. [Online]. Available: https://www.youtube.com/watch?v=bmjcURg8Tg8

[2] Farshad Zare, “DHCP snooping attack and mitigation,” YouTube. Apr. 20, 2022. [Online]. Available: https://www.youtube.com/watch?v=FmEkVMWk5OM

[3] Tons OF Network Fun, “►DHCP Spoofing Attack Explained Packet Tracer I IP dhcp snooping I Tons OF Network Fun,” YouTube. Jul. 03, 2023. [Online]. Available: https://www.youtube.com/watch?v=djJPo9U8Gsg

[4] Moustapha Fall, “Comment l’attaque DHCP starvation fonctionne,” YouTube. Feb. 21, 2022. [Online]. Available: https://www.youtube.com/watch?v=-47KH2V2gpc

[5] Crowdstrike, “What is ARP Spoofing? How to Prevent an ARP Attack – CrowdStrike,” *crowdstrike.com*, May 19, 2022. https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/arp-spoofing/

[6] “ARP Poisoning or ARP Spoofing Attack - Explanation & Demonstration,” *www.youtube.com*. https://youtu.be/iEqq-6YDOlc (accessed Nov. 27, 2023).

[7] Imperva, “What is ARP Spoofing | ARP Cache Poisoning Attack Explained | Imperva,” *Imperva*, 2022. https://www.imperva.com/learn/application-security/arp-spoofing/

[8] B. Lutkevich and L. Rosencrance, “What is IP spoofing? how to prevent it,” Security, https://www.techtarget.com/searchsecurity/definition/IP-spoofing (accessed Nov. 28, 2023).

[9] S. Vanvliet, “What it is IP spoofing, how to protect against it,” Keyfactor, https://www.keyfactor.com/blog/what-it-is-ip-spoofing-how-to-protect-against-it/ (accessed Nov. 28, 2023).

[10] D. Ghimiray, “How to Spot and Prevent IP Spoofing ,” How to spot and prevent IP spoofing, https://www.avast.com/c-how-to-prevent-ip-spoofing# (accessed Dec. 4, 2023).

[11]“►Mac Flooding Attack Example Packet Tracer I CISCO CCNA I f/01 switchport port security maximum 3 I,” www.youtube.com. https://www.youtube.com/watch?v=pNyWBThtqTc (accessed Dec. 04, 2023).

[12]“MAC flooding attack,” library.mosse-institute.com. https://mcsi-library.readthedocs.io/articles/2022/06/mac-flooding-attack/mac-flooding-attack.html#:~:text=A%20MAC%20flooding%20attack%20is%20a%20type%20of (accessed Dec. 04, 2023).

‌[13]M. Higgins, “MAC flooding: What it is and how to prevent it | NordVPN,” nordvpn.com, Apr. 11, 2023. https://nordvpn.com/blog/mac-flooding/

‌