بررسی دو سناریو در رابطه با اختلال در شبکه های کامپیوتری
(DHCP SPOOFING & CAM TABLE OVERFLOW)

TABLE OF CONTENTS

The Goal of This Seminar

CAM Table Overflow Attack

- Introduction of CAM Table Overflow Attack
- Explain CAM Table Overflow Attack
- How to Defend!

DHCP Spoofing Attack

- Introduction of DHCP Spoofing Attack
- Explain DHCP Spoofing Attack
- How to Defend!

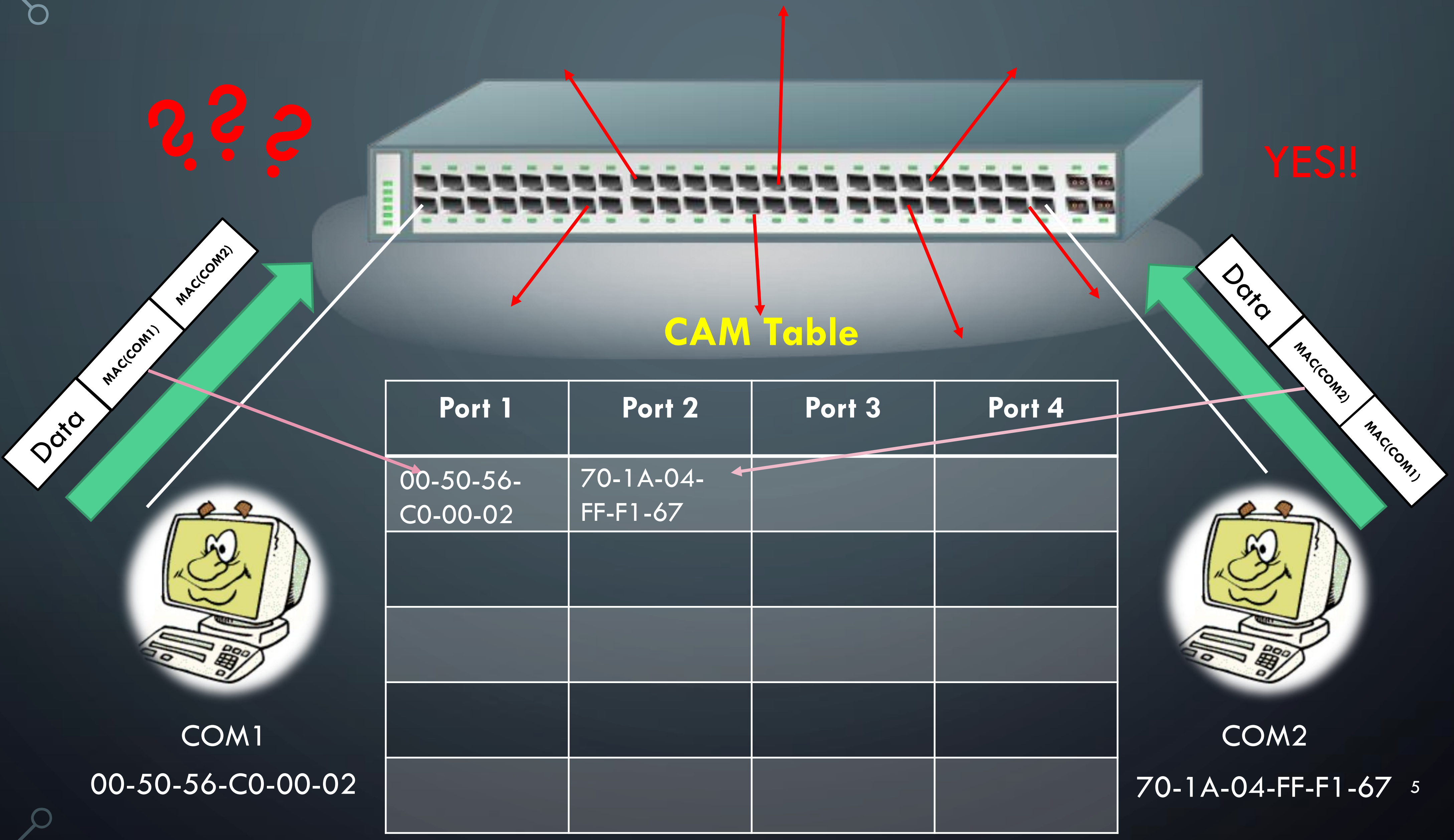
THE GOAL OF THIS SEMINAR

- According to a study by the FBI, an estimated 70 percent of these network breaches originate from within.

- Disorder in computer networks is not a big work . It is just abuse of some simple Rules.

CAM Table overflow Attack

- Introduction of CAM Table Overflow Attack



CAM Table

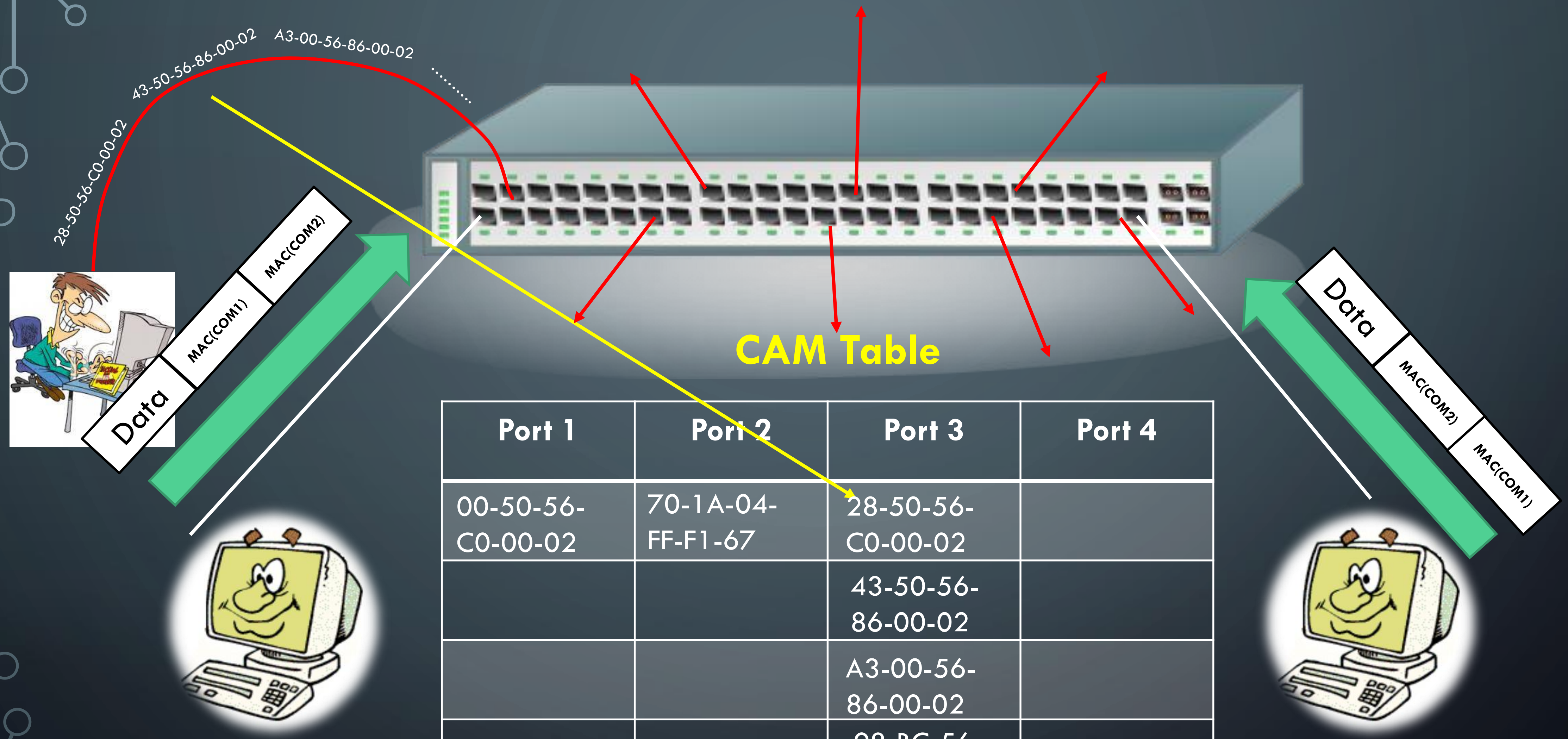
Port 1	Port 2	Port 3	Port 4
00-50-56-C0-00-02	70-1A-04-FF-F1-67		

COM1
00-50-56-C0-00-02

COM2
70-1A-04-FF-F1-67

CAM Table overflow Attack

- Introduction of CAM Table Overflow Attack
- Explain CAM Table Overflow Attack



CAM Table

Port 1	Port 2	Port 3	Port 4
00-50-56-C0-00-02	70-1A-04-FF-F1-67	28-50-56-C0-00-02	
		43-50-56-86-00-02	
		A3-00-56-86-00-02	
		98-BC-56-86-00-02	
		F3-64-56-86-00-02	

COM1

00-50-56-C0-00-02

COM2

70-1A-04-FF-F1-67

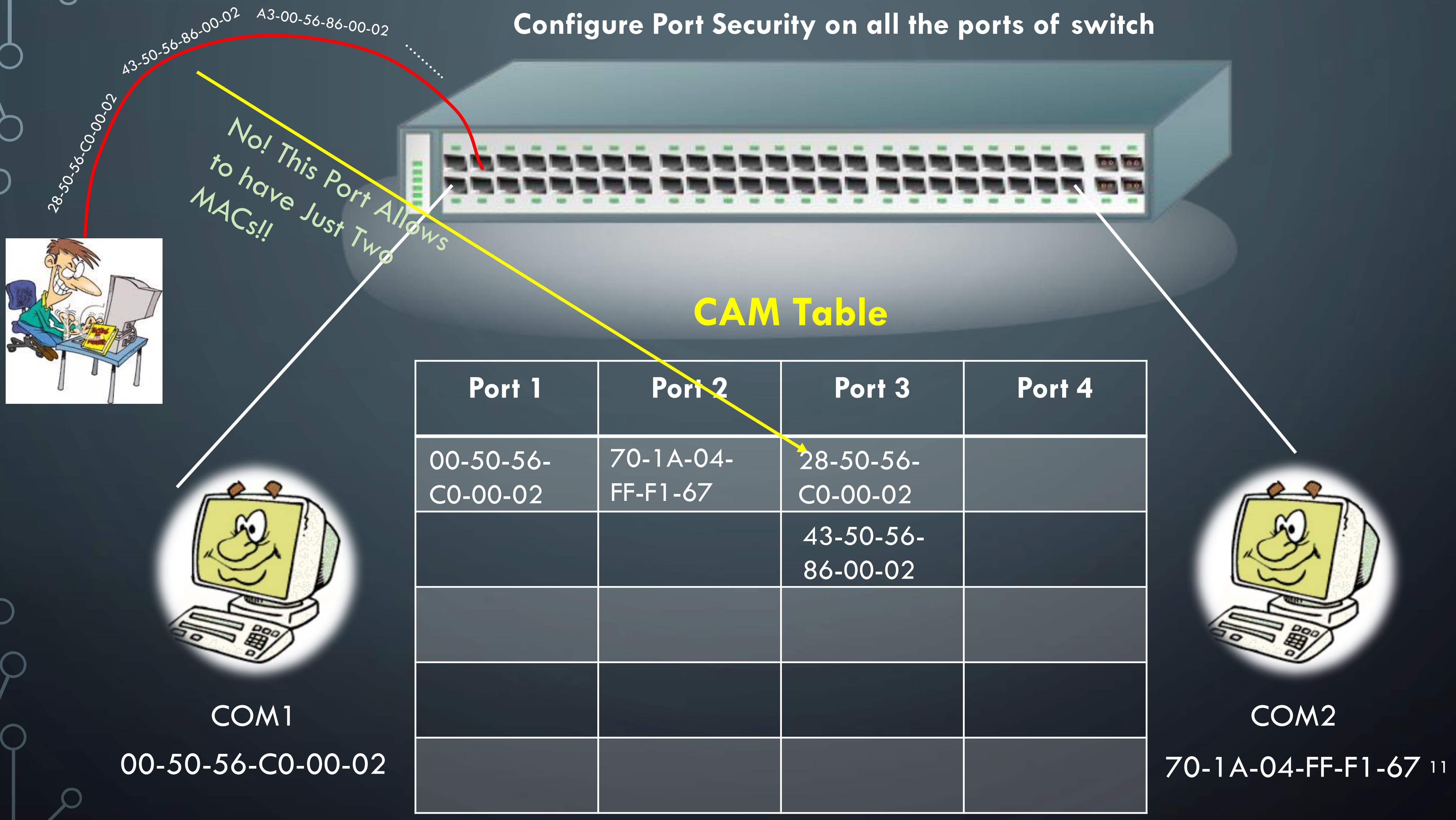
CAM Table overflow Attack

- Introduction of CAM Table Overflow Attack
- Explain CAM Table Overflow Attack
- How to Defend!

THE SOLUTION IS:

Port Security

Configure Port Security on all the ports of switch

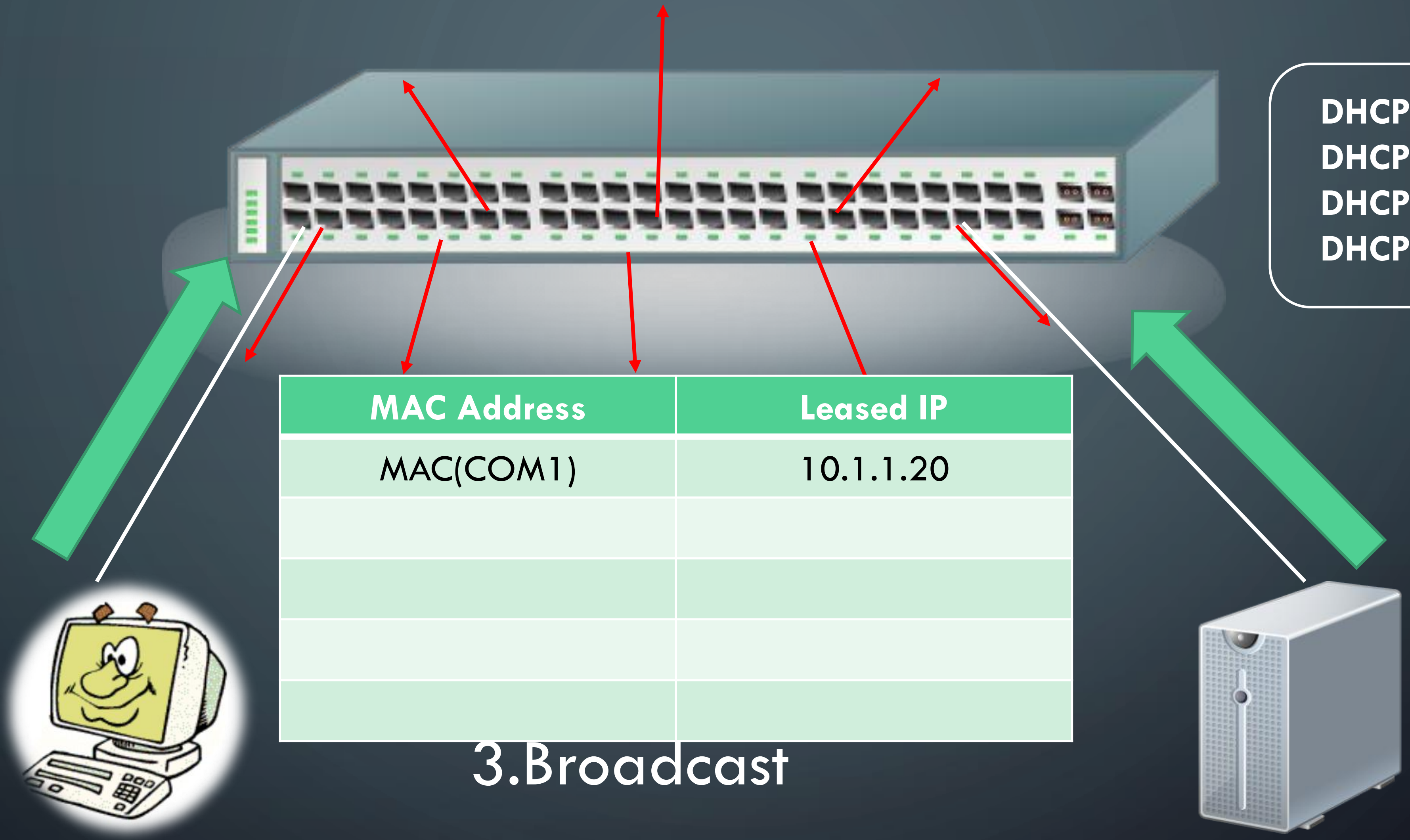


Port 1	Port 2	Port 3	Port 4
00-50-56-C0-00-02	70-1A-04-FF-F1-67	28-50-56-C0-00-02	
		43-50-56-86-00-02	

DHCP Spoofing Attack

- Introduction of DHCP Spoofing Attack

DHCP Discover
DHCP Offer
DHCP Request
DHCPAcknowledgment



MAC Address	Leased IP
MAC(COM1)	10.1.1.20

3.Broadcast

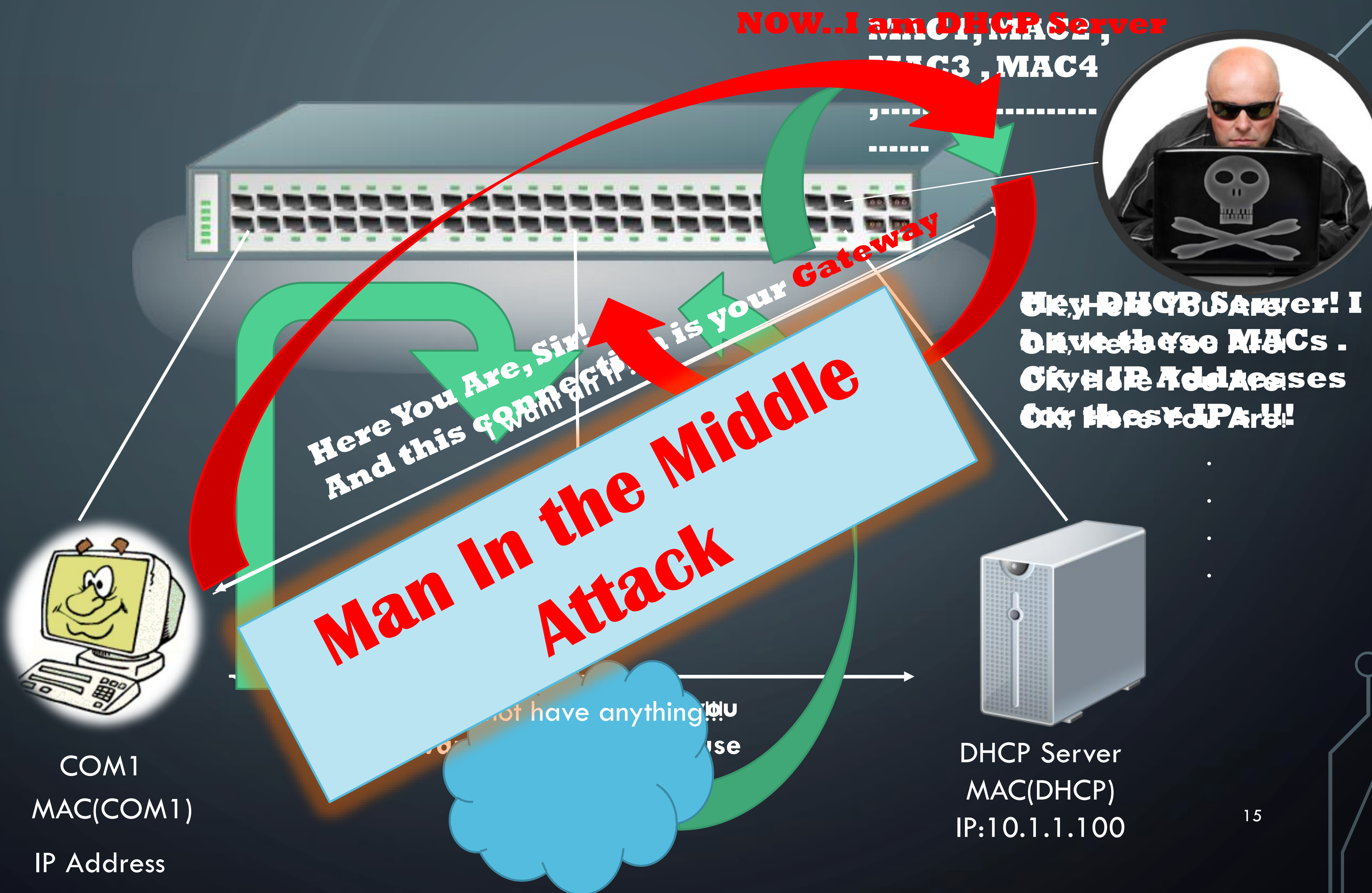
COM1
MAC(COM1)
IP Address

???

DHCP Server
MAC(DHCP)
IP:10.1.1.100

DHCP Spoofing Attack

- Introduction of DHCP Spoofing Attack
- Explain DHCP Spoofing Attack



NOW..I am DHCP Server

MAC1, MAC2 , MAC3 , MAC4 ,................ ......

Hey DHCP Server! I have these MACs . Give IP Addresses for these IPs !!!

Ok, Here You Are!

Ok, Here You Are!

Ok, Here You Are!

Ok, Here You Are!

. . . .

Here You Are, Sir! And this connection is your Gateway

I want an IP

Man In the Middle Attack

not have anything!!!

ou

va

use

COM1

MAC(COM1)

IP Address

DHCP Server

MAC(DHCP)

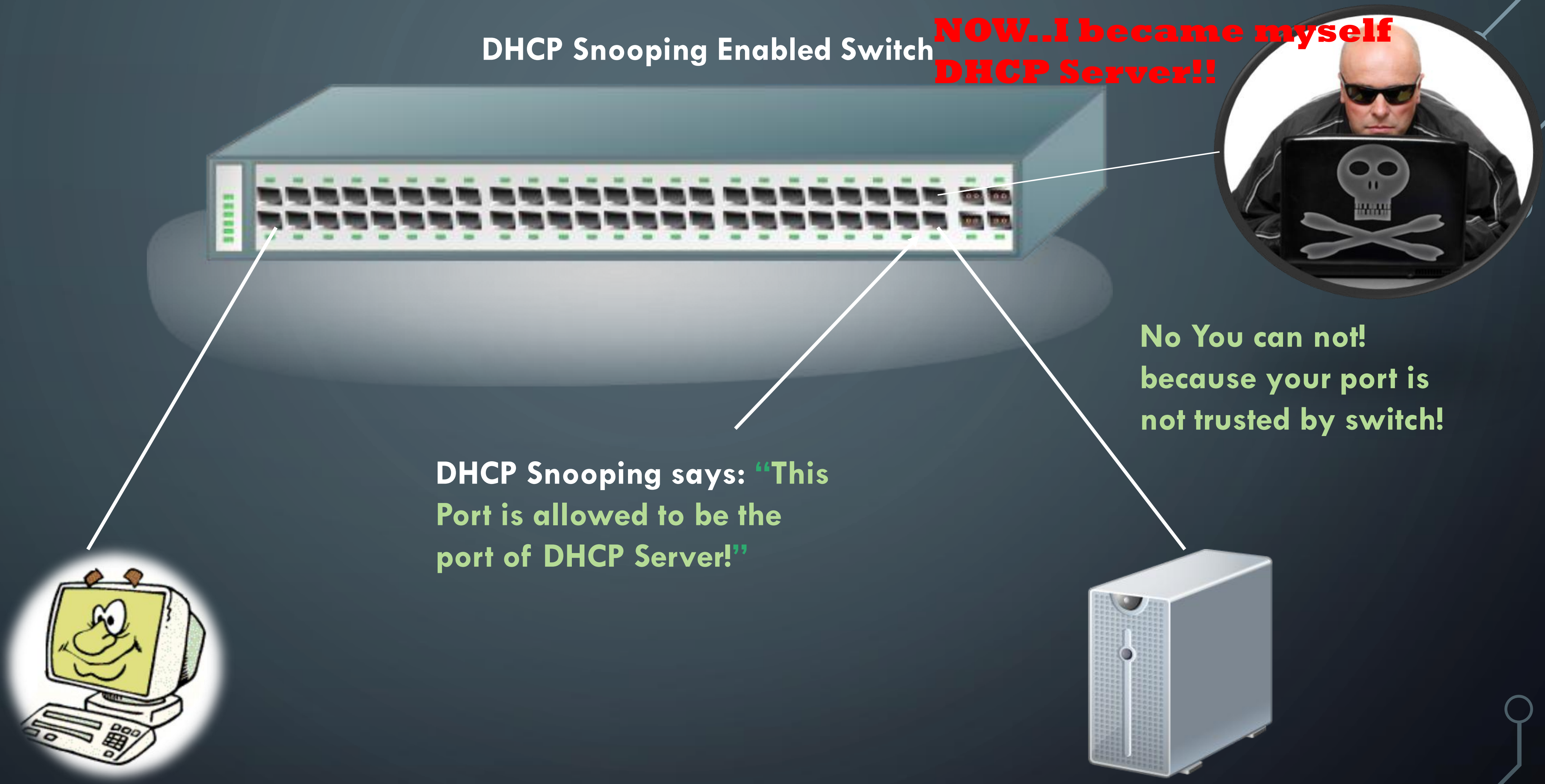
IP:10.1.1.100

DHCP Spoofing Attack

- Introduction of DHCP Spoofing Attack
- Explain DHCP Spoofing Attack
- How to Defend!

THE SOLUTION IS:

DHCP Snooping



DHCP Snooping Enabled Switch

NOW..I became myself DHCP Server!!

No You can not! because your port is not trusted by switch!

DHCP Snooping says: “This Port is allowed to be the port of DHCP Server!”

COM1
MAC(COM1)
IP Address

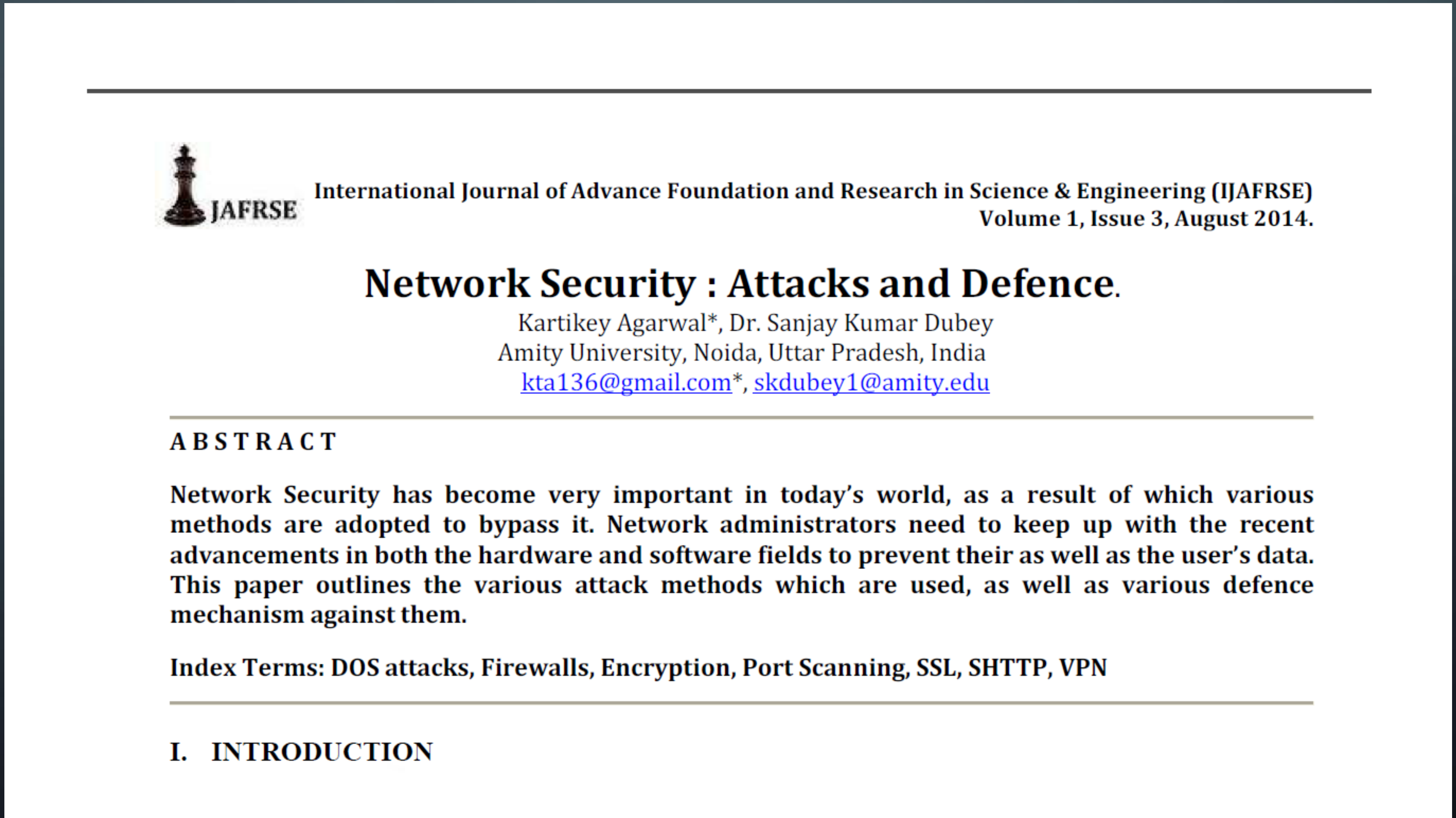
DHCP Server
MAC(DHCP)
IP:10.1.1.100

CONCLUSION

Disorder in computer networks is not a big work .

It is just abuse of some simple Rules.

PAPERS & REPORT



IJAFRSE International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE)
Volume 1, Issue 3, August 2014.

Network Security : Attacks and Defence.

Kartikey Agarwal*, Dr. Sanjay Kumar Dubey
Amity University, Noida, Uttar Pradesh, India
kta136@gmail.com*, skdubey1@amity.edu

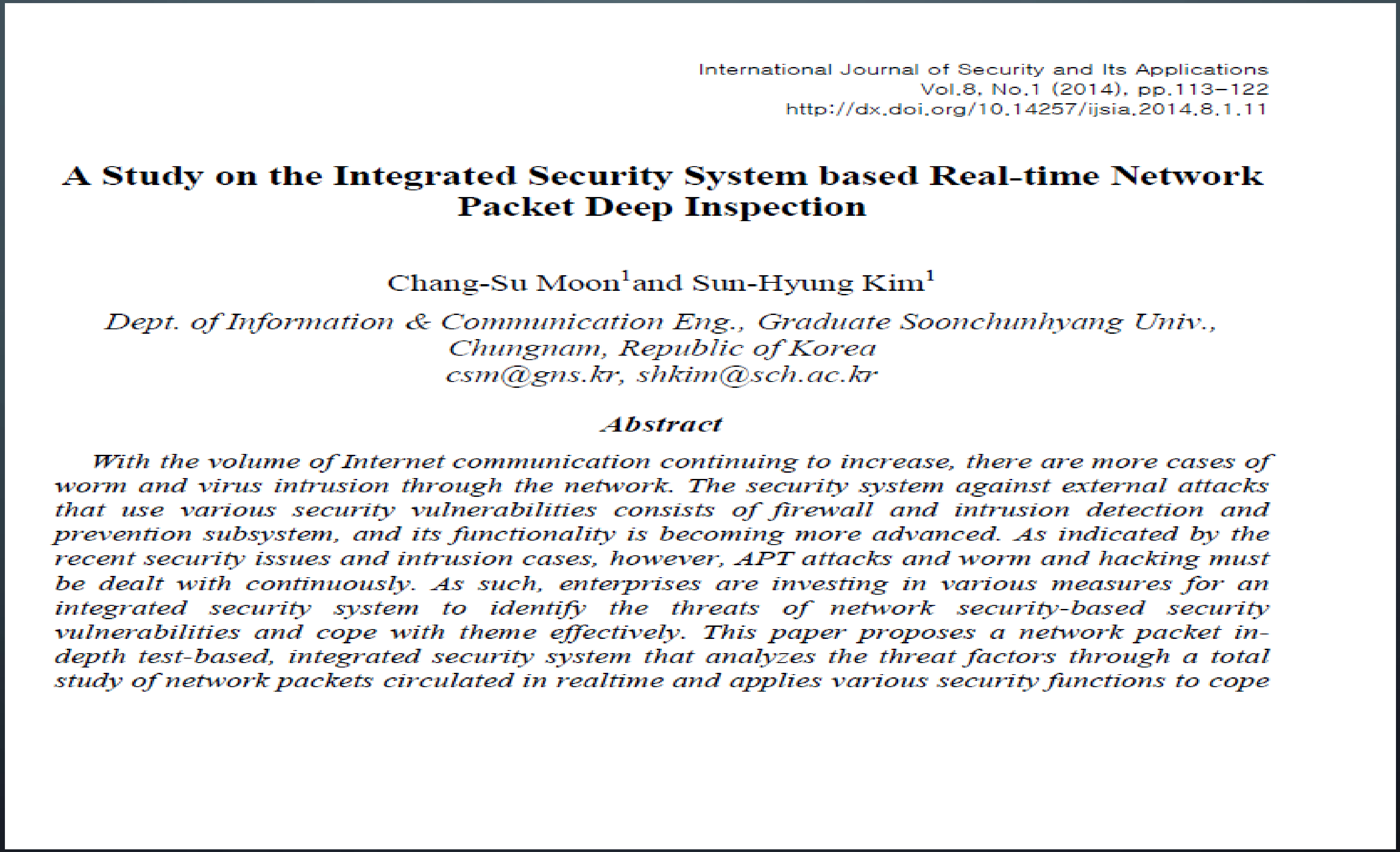
ABSTRACT

Network Security has become very important in today's world, as a result of which various methods are adopted to bypass it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. This paper outlines the various attack methods which are used, as well as various defence mechanism against them.

Index Terms: DOS attacks, Firewalls, Encryption, Port Scanning, SSL, SHTTP, VPN

I. INTRODUCTION

PAPERS & REPORT



International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.113-122
http://dx.doi.org/10.14257/ijsia.2014.8.1.11

A Study on the Integrated Security System based Real-time Network Packet Deep Inspection

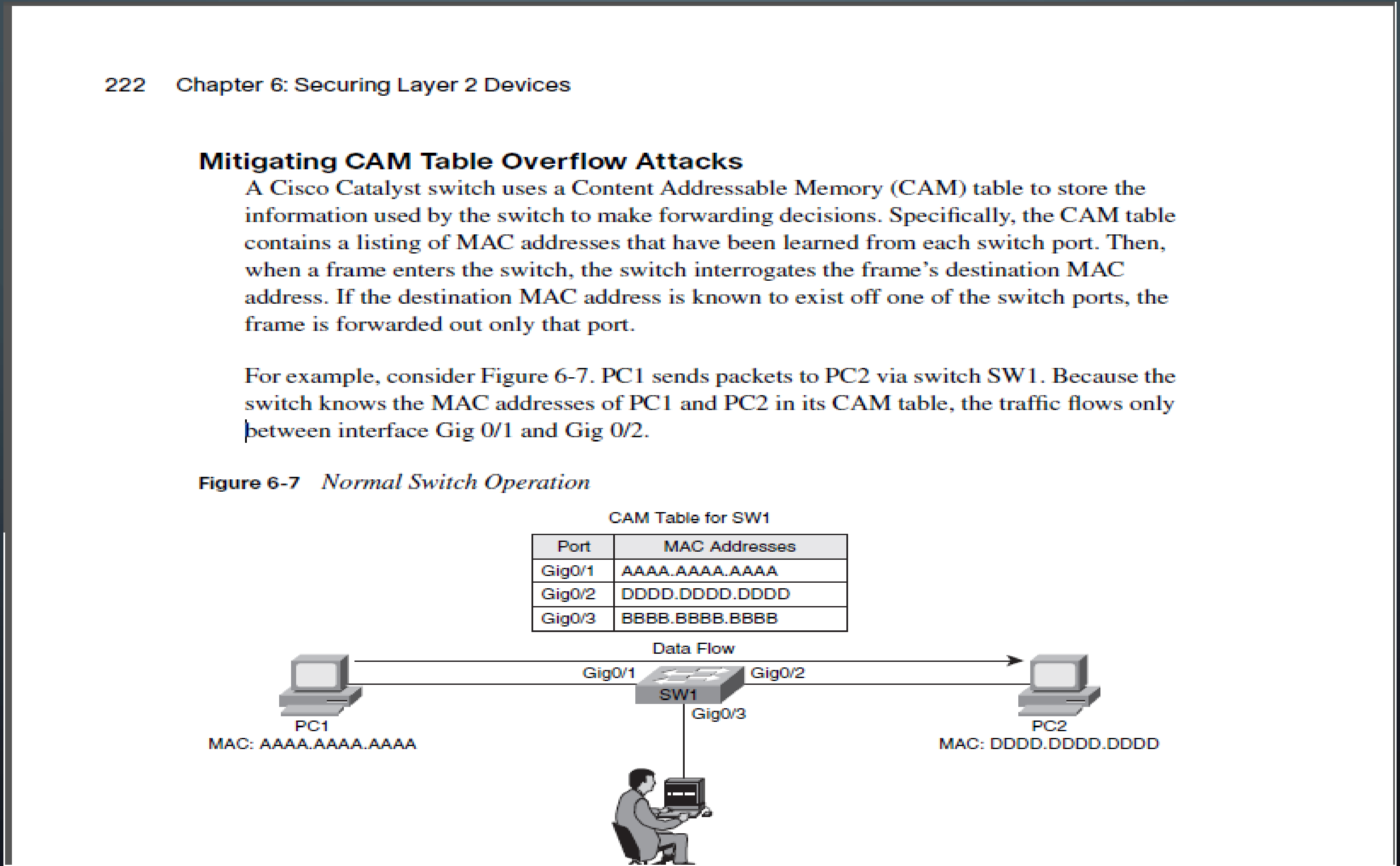
Chang-Su Moon[1]and Sun-Hyung Kim[1]

*Dept. of Information & Communication Eng., Graduate Soonchunhyang Univ.,
Chungnam, Republic of Korea
csm@gns.kr, shkim@sch.ac.kr*

Abstract

With the volume of Internet communication continuing to increase, there are more cases of worm and virus intrusion through the network. The security system against external attacks that use various security vulnerabilities consists of firewall and intrusion detection and prevention subsystem, and its functionality is becoming more advanced. As indicated by the recent security issues and intrusion cases, however, APT attacks and worm and hacking must be dealt with continuously. As such, enterprises are investing in various measures for an integrated security system to identify the threats of network security-based security vulnerabilities and cope with theme effectively. This paper proposes a network packet in-depth test-based, integrated security system that analyzes the threat factors through a total study of network packets circulated in realtime and applies various security functions to cope

PAPERS & REPORT



Mitigating CAM Table Overflow Attacks

A Cisco Catalyst switch uses a Content Addressable Memory (CAM) table to store the information used by the switch to make forwarding decisions. Specifically, the CAM table contains a listing of MAC addresses that have been learned from each switch port. Then, when a frame enters the switch, the switch interrogates the frame's destination MAC address. If the destination MAC address is known to exist off one of the switch ports, the frame is forwarded out only that port.

For example, consider Figure 6-7. PC1 sends packets to PC2 via switch SW1. Because the switch knows the MAC addresses of PC1 and PC2 in its CAM table, the traffic flows only between interface Gig 0/1 and Gig 0/2.

Figure 6-7 *Normal Switch Operation*

CAM Table for SW1

Port	MAC Addresses
Gig0/1	AAAA.AAAA.AAAA
Gig0/2	DDDD.DDDD.DDDD
Gig0/3	BBBB.BBBB.BBBB

REFERENCES

CCNA Security

Official Exam Certification Guide

(Chapter 6 : Securing Layer 2 Devices)

با تشکر از همراهی شما دوستان عزیز