International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 11, November 2016)

Additional Layer of Security in Local Area Network (LAN): Port Security

Dr. Anil Kumar Singh[1], Dr. Bharat Mishra[2]

[1]Jagran Institute of Management, Kanpur

[2]MGCGV Chitrakoot, Satna MP

Abstract-- **In this paper a design and implementation of a port security has presented using CISCO 2960 series manageable switch. We will exemplify how a switch locks down the ports based on MAC address to prevent unauthorized access [1][2]. In this paper we will configure and verify the port security on a switch. As we know that port security allows to network administrator to confine port ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port [3][4]. For demonstration purpose we will use packet tracer network simulator software.**

Keywords-- **Manageable Switch, MAC Address, Rogue, Hacker, Sticky, Security Violation, Shutdown, Restrict, Protect.**

I. INTRODUCTION

Network security is a very difficult task. Historically it is only tackled by well trained and experienced expert. However as more as people become “wired” an increasing number of people need to understands the basics of security in networked world [5]. Security has one purpose: “to protect assets” [6] [7] in terms of computer networks the assets can be Information, files and data etc. For most of time periods in the past, security meant building big strong walls to stop the unauthorized users, and establishing small, well-guarded doors to provide secure access for the authorized users [8]. With the outstanding growth in the Internet, network security has become an integral part of computer and information security [9] [10].

Network security includes the events accepted to protect the resources and integrity of a computer network. Vulnerability is a weakness which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves [11].

II. REQUIREMENTS

3 Personal Computers, CISCO 2960 Series Manageable Switch, Packet Tracer 5.0 etc.

III. METHOD

A. Design of Experiment

Device	MAC Address	IP Address	Subnet Mask
PC-1	0002.175E.6A97	80.0.0.1	255.0.0.0
PC-2	000C.CF8C.2E6D	80.0.0.2	255.0.0.0
Rogue-PC	000C.8SEB.1DA6	80.0.0.3	255.0.0.0

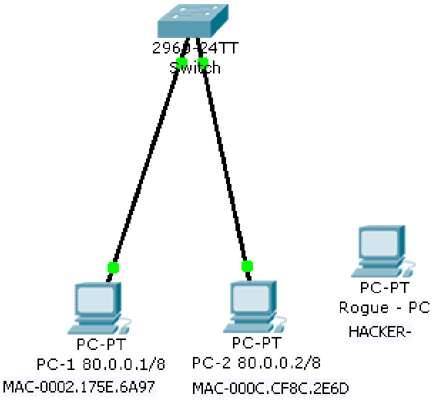


Fig. 1.0 Shows the Design of Experiment

IV. PORT SECURITY VIOLATION MODES

A security violation occurs if an illegal MAC address attempts to forward traffic through a port [12]. There are three violation actions a switch can perform:

A. Shutdown: If a violation occurs it puts the interface into the error-disabled condition immediately and sends an SNMP trap notification. The interface will stop forwarding all traffic, including non-violating traffic, until it is removed from an errdisable state. This is the default action for Port Security.

B. *Restrict:* If a violation occurs, the interface will remain online. Legitimate traffic will be forwarded, and unauthorized traffic will be dropped. An SNMP trap is generated, the log is appended. And the violation counter is incremented. It drops packets with unidentified source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the Security Violation counter to increment.

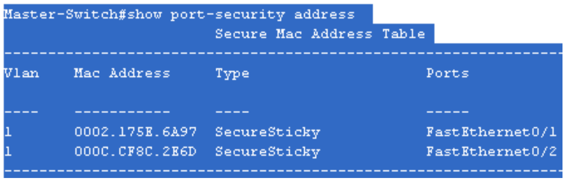
C. *Protect:* If a violation occurs, the interface will remain online. Legitimate traffic will be forwarded and unauthorized traffic will be dropped, but No notification is given of this occurrence. It drops packets with unidentified source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.[13]

V. Configure The Switch

Now we access the switch via command line and enable the port security on Fast Ethernet Port 0/1 and 0/2. Set the maximum on above port numbers so that only one device can access the Fast Ethernet ports 0/1 & 0/2. Set the MAC address sticky, which will be dynamically add the MAC addresses in running configuration of switch.

```
Master-Switch>enable
Master-Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Master-Switch(config)#interface fastEthernet 0/1
Master-Switch(config-if)#switchport mode access
Master-Switch(config-if)#switchport port-security
Master-Switch(config-if)#switchport port-security maximum 1
Master-Switch(config-if)#switchport port-security mac-address sticky
Master-Switch(config-if)#switchport port-security violation shutdown
Master-Switch(config-if)#exit
Master-Switch(config)#interface fastEthernet 0/2
Master-Switch(config-if)#switchport mode access
Master-Switch(config-if)#switchport port-security
Master-Switch(config-if)#switchport port-security maximum 1
Master-Switch(config-if)#switchport port-security mac-address sticky
Master-Switch(config-if)#switchport port-security violation shutdown
Master-Switch(config-if)#exit
Master-Switch(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Master-Switch#
```

A. MAC Address Table

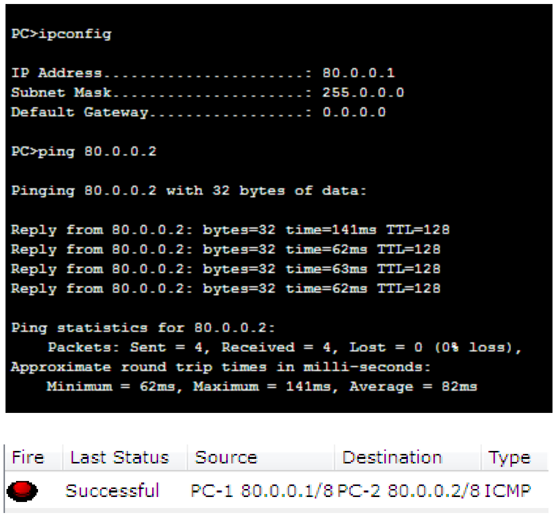


```
Master-Switch#show port-security address
                              Secure Mac Address Table
-------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports
----    -----------       ----                          -----
1       0002.175E.6A97    SecureSticky                  FastEthernet0/1
1       000C.CF8C.2E6D    SecureSticky                  FastEthernet0/2
-------------------------------------------------------------------------------
```

Fig.2.0 Shows the Secure MAC address Table

Hosts configured with the above two MAC addresses i.e. 0002.175E.6A97 and 000C.CF8C.2E6D will be allowed to send traffic through this port.

VI. Communication Between Pc-1 And PC-2



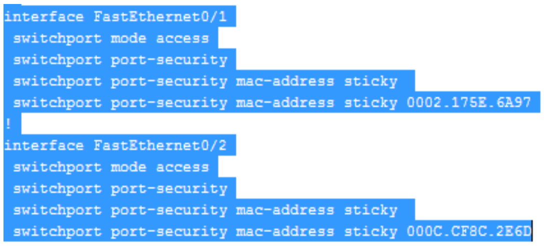
```
PC>ipconfig

IP Address......................: 80.0.0.1
Subnet Mask.....................: 255.0.0.0
Default Gateway.................: 0.0.0.0

PC>ping 80.0.0.2

Pinging 80.0.0.2 with 32 bytes of data:

Reply from 80.0.0.2: bytes=32 time=141ms TTL=128
Reply from 80.0.0.2: bytes=32 time=62ms TTL=128
Reply from 80.0.0.2: bytes=32 time=63ms TTL=128
Reply from 80.0.0.2: bytes=32 time=62ms TTL=128

Ping statistics for 80.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 141ms, Average = 82ms
```

Fire	Last Status	Source	Destination	Type
●	Successful	PC-1 80.0.0.1/8	PC-2 80.0.0.2/8	ICMP

Fig. 3.0 Shows the communication Successful

VII. Verify The Sticky Mac Address Command

Master-Switch#show running-config



```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0002.175E.6A97
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.CF8C.2E6D
```

Fig. 4.0 Shows MAC addresses are dynamically added on running configuration of switch

VIII. Security Violation By Hacker

Now Hacker connects their Rogue PC with the switch's Fast Ethernet's port number 0/1

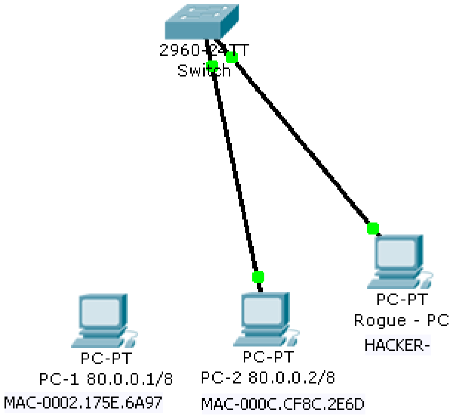
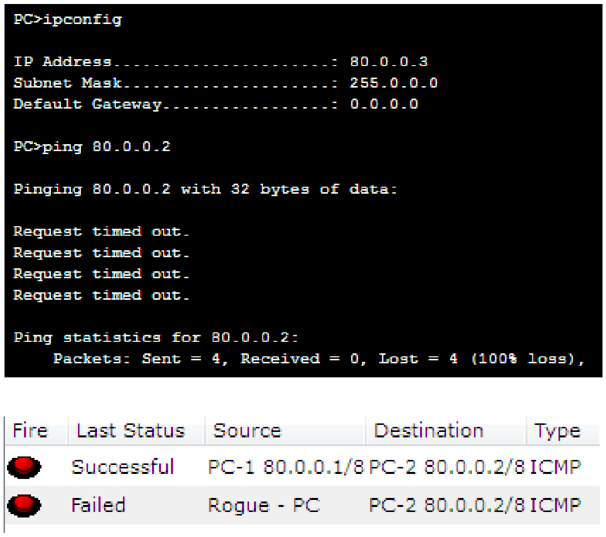


Fig. 5.0 Shows physical connection of Hacker's Rogue PC with Fast Ethernet 0/1

IX. Communication Between Rogue Pc And Host

After successful physical connection with Fast Ethernet 0/1 port, hacker tried to communicate with other nodes on that network. As a result he failed in communication. The result shown in the below diagram.



```
PC>ipconfig

IP Address......................: 80.0.0.3
Subnet Mask.....................: 255.0.0.0
Default Gateway.................: 0.0.0.0

PC>ping 80.0.0.2

Pinging 80.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 80.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fire	Last Status	Source	Destination	Type
●	Successful	PC-1 80.0.0.1/8	PC-2 80.0.0.2/8	ICMP
●	Failed	Rogue - PC	PC-2 80.0.0.2/8	ICMP

Fig. 6.0 shows the communication status of the Hacker

X. Result

It was found that hacker's rogue PC unable to communicate with other host on the network. Due to enable of port security in switch. When rogue PC try to communicate with other nodes then security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol manager.

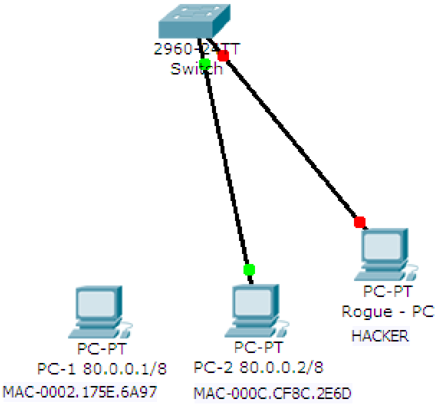


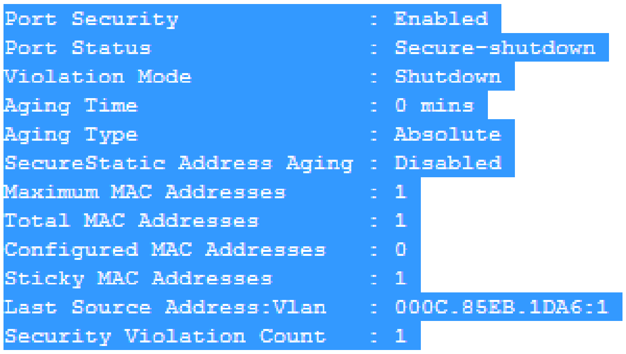
Fig. 7.0 Sows switch port physically shutdown

XI. Verification Of Port Security Violation

Now go to switch's configuration mode and try to know the status of port number 0/1 because the hacker physically connects with port number 0/1. Therefore, try the command show port-security interface Fast Ethernet 0/1. It displays output from the show port-security command for a specified interface i.e. 0/1:

Master-Switch#show port-security interface fastEthernet 0/1

The screen shot shows the security violation count=1. It means hacker only 1 time has tryied to communicate. Last source address shows the MAC address of hacker's PC.



```
Port Security                : Enabled
Port Status                  : Secure-shutdown
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : 000C.85EB.1DA6:1
Security Violation Count     : 1
```

XII. CONCLUSION

The root behind network security is to ensure access to the network and its data for authorized hosts and deny access to unauthorized hosts. In above paper it was found that hacker's rogue PC unable to communicate with other PC on the network due to enable of port security with maximum value of MAC. When rogue PC try to communicate with other nodes then security violation occurs, as a result of the link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol manager. In this way we can secure our LAN from the Rogue/unauthorised PC.

REFERENCES

[1] Configuring and Monitoring Port Security - http://whp-aus2.cold.extweb.hp.com/pub /networking /software/Security-Oct2005-59906024-Chap09-Port_Security.pdf

[2] Cisco IOS Software Configuration Guide, Release 12.2SX, chapter 62 Configuring port security

[3] Routing and Switching Essentials Companion Guide, Chapters 1-3 http://ptgmedia. pearsoncmg.com/images/ 9781587133183 /downloads /9781587 133183_chps1-3.pdf

[4] Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1, http:// www.cisco.com /c/en/us/td/docs/switches/ datacenter/sw/4_1/nx-os/security/configu ration/guide/sec_nx-os-cfg/sec_portsec. Html

[5] Matt Curtin, “Introduction to network security”, March 1997 reprinted with the permission of Kent information services.

[6] Salah Alabady, “Design and Implementation of a Network Security Model for Cooperative Network”, International Arab Journal of e-tchnology, Vol. 1, No. 2, June 2009, pp 26-36

[7] Nayak Umesh, Rao Hodeghatta, The InfoSec Handbook: An Introduction to Information Security.

[8] Overview of Network Security, http://www.cisco.com/web/learning/netacad/demos /FNS Demo1_1/ch1/1_1_1/content.html

[9] Meghanathan Natarajan,” A Tutorial on Network Security: Attacks and Controls” , https://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf

[10] Daya Bhavya Network Security: History, Importance, and Future, http://web.mit.edu /~bdaya/www/ Network%20Security.pdf

[11] Soceanu Ing. Alexandru, “Network Management”, http://w3-o.cs.hm.edu /mediapool/soceanu/pmcio/Network_Security_Vulnerabilities_Threats_Attacks.pdf

[12] Configuring Port Security, Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SG

[13] Gary A. Donahue, Network Warrior, "O'Reilly Media, Inc.", 21-Jun-2007 - Computers - 600 pages