Volume 5, Issue 8, August 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Limiting Traffic on Local Area Networks through Switch Port Security

Krishna Priyusha Maddipatla, Shraddha Agarwal
Department of Computer Science and Engineering,
JNTU Hyderabad, India

Abstract— Network Security can be provided at gateway-level, in which a security component that augments a firewall employed in a computer network controls the incoming and outgoing network traffic based on applied rule set. We propose the concept of switch-port security to limit the traffic on Local Area Networks (LANs). The switch interfaces can be provided with protection using which the traffic on them can be restricted by identifying and limiting the access based on source Ethernet MAC addresses. On assigning MAC addresses to a switch port, it does not forward packets with source addresses outside the group of defined addresses. When the MAC address of a workstation attempting to access the configured port is found to be outside the identified secure MAC addresses, a security violation occurs. The illicit access is denied and the switch-port automatically shuts down. It remains inactive for any further usage until the conflict is resolved.

Keywords— Network security, Local Area Networks, port security, switch-port access, Ethernet MAC addresses

I. INTRODUCTION

One of the most unheeded security areas is the configuration of individual port security configuration. The reason may be that it requires a more granular configuration; this is because a typical configuration requires the knowledge of the specific MAC addresses that will be connecting to each switch port. Keeping track of all of this information in a medium to large organization can be quite time consuming. The port security feature offers the ability to configure a switch port so that traffic can be limited to only a specific configured MAC address or list of MAC addresses. Using this feature one can restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

A. Secure MAC Address types

There are three different types of secure MAC address

1) *Static:* This type of secure MAC address is statically configured on a switch port and is stored in an address table and in the running configuration.
2) *Dynamic:* This type of secure MAC address is learned dynamically from the traffic that is sent through the switch port. These types of addresses are kept only in an address table and not in the running configuration.
3) *Sticky:* This type of secure MAC address can be manually configured or dynamically learned. These types of addresses are kept in an address table and in the running configuration.

The type of secure MAC address that is configured depends on the intended end result. Static secure MAC addresses are typically used when the MAC addresses used are known and do not change often. For example, if a single host is always connected to the same switch port. Dynamic secure MAC addresses are typically used when the hosts connecting to a specific switch port is constantly changing, and the intention is to limit the port to only be used by a specific number of hosts at once. For example, a switch port can be configured to only allow a single MAC address to be learned at a time and not permit hosts other than the one initially learned; the only way to change the host that connects to the switch port is to disable switch port security and re-enable it, to delete the learned MAC address from the table directly, or to wait for the port-security aging time to expire if configured. *Sticky* secure MAC addresses are a bit of a combination between the two prior secure MAC address types; not only can these addresses be statically-configured but they can also be dynamically learned. The key difference here is that dynamically-learned addresses are automatically put into the running-configuration; if the engineer wants these addresses to be saved on device reboot, the option is available to save the running-configuration into the startup configuration, thus effectively making these addresses static.

B. Security Violations

An important piece of switch port security that must be understood is the security violation including what it is that causes it and what are the different violation modes that exist. A switch port violation occurs in one of two situations

1) When the maximum number of secure MAC addresses has been reached. By default, the maximum number of secure MAC addresses per switch port is limited to one.
2) An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

C. *Actions*

The action that the device takes when one of above violations occurs can be configured by the network administrator. These actions include

1) *Protect:* This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, no notification action is taken when traffic is dropped.
2) *Restrict:* This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, a syslog message is logged, a Simple Network Management Protocol (SNMP) trap is sent, and a violation counter is incremented when traffic is dropped.
3) *Shutdown:* This mode is the default violation mode; when in this mode, the switch will automatically force the switch port into an error disabled *(err-disable)* state when a violation occurs. While in this state, the switch port forwards no traffic. The switch port can be brought out of this error disabled state by issuing the *err-disable recovery cause* CLI command or by disabling and re enabling the switch port.
4) *Shutdown VLAN:* This mode mimics the behaviour of the shutdown mode but limits the error disabled state the specific violating VLAN.

D. *Port Security Aging*

Another option that is available when configuring Port Security is the use of an aging timer. This provides for a MAC address to be removed from being learned after a configured amount of time. By default, aging is not enabled and addresses are not deleted unless the device is rebooted or the MAC addresses are cleared through a removal command being issued. There are two different methods of implementing secure MAC address aging, these include

1) *Absolute:* When using this method, secure MAC addresses are deleted after a specific aging time expires.
2) *Inactivity*: When using this method, secure MAC addresses are deleted only if the secure MAC address is inactive for a specific aging time.

II. LITERATURE SURVEY

This paper presents a new approach for limiting the traffic on local area networks by applying the concept of switch port security. Several existing security measures like firewalls and application-level gateways which are widely used implementations of security at the gateway level have been studied, their effectiveness has been evaluated and shortcomings have been described.

A. *Firewalls*

A computer network is prone to different types of outside attacks which can be classified into interruption, interception, modification and fabrication. These lead to either leakage of information or addition of outside elements to the data such as viruses and worms. One of the techniques used to avoid the outsider attacks on the corporate network is Firewall. A firewall establishes a barrier between a trusted, secure internal network and another network that is not assumed to be secure and trusted. The decision of allowing data exchange or its restriction is decided by the firewall. Without security protections in place, unauthorized devices could access your network through open and unprotected switch interfaces. All traffic between the internal and other network must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Only authorized traffic as defined by the local security policy will be allowed to pass. The firewall itself is immune to penetration by the usage of trusted systems. The permissions given decide the access of data by the user. A firewall has a single choke point. It provides protection from various kinds of IP spoofing and routing attacks. It also provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system. A firewall offers a convenient platform for several internet functions that are not security related such as NAT. Firewalls cannot protect the corporate network against the attacks those bypass the firewall. In addition, it does not provide security when the network has dial-out capability to connect to the ISP. When an internal LAN may support a modem pool that provides dial-in capability for users a firewall can provide no appropriate protection. The variety of operating systems and applications that are capable of transferring virus infected data are not inhibited by a firewall as it would be impractical for the firewall to scan all incoming files, emails, messages for viruses.

B. *Application Level Gateway*

An Application-level gateway consists of a security component that augments a firewall employed in a computer network which is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. Also known as application proxy or application-level proxy, an application gateway is an application program that runs on a firewall system between two networks. When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected. While this is considered a highly secure method of firewall protection, application gateways require great memory and processor resources compared to other firewall technologies. An overhead in terms of connections is seen between the two sets of connections: one between the user and the application gateway and the other is between the application gateway and the remote host. Also, the application level gateway must examine and forward all the traffic in both the directions.

III. PROPOSED SYSTEM

Our proposed method helps regulate the network traffic by providing security to the switch interfaces thereby restricting the traffic on the switch interface. The use of switch port security provides another level of security that can help in securing locally connected computers and the networks they connect to. It employs restriction of input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the switch port. The secure addresses of the switch ports can be tracked and any violations that occur can be handled. This method also serves as a measure to combat flooding attacks. We further present the software simulation of how the port security can be implemented on the desired switches. Cisco Packet Tracer is a network simulation tool that allows to experiment with network behaviour. The Packet Tracer software provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the implementation of our proposed mechanism. The Cisco Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, and EIGRP. It aims to provide a realistic simulation of functional networks using Layer2, Layer3 switches and routers. These configurable devices enable us to implement the proposed switch port security and also check the violation mechanism and outcome.

IV. RESULTS

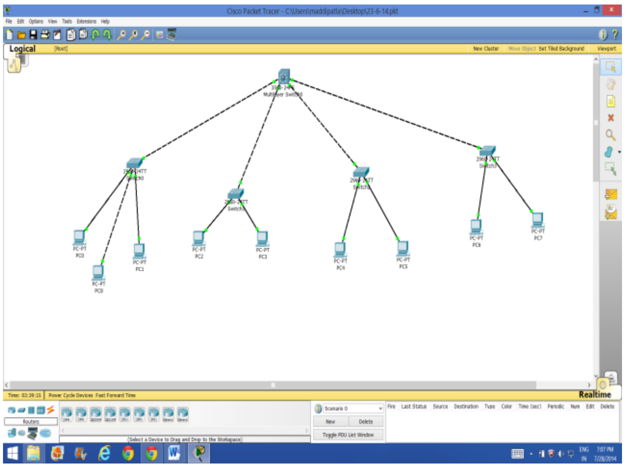
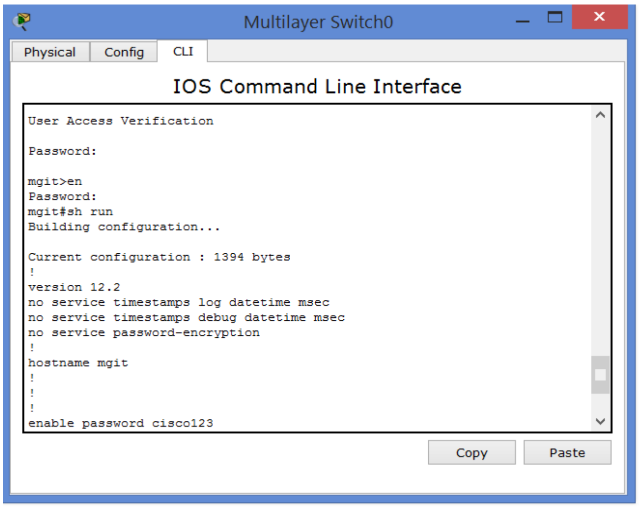


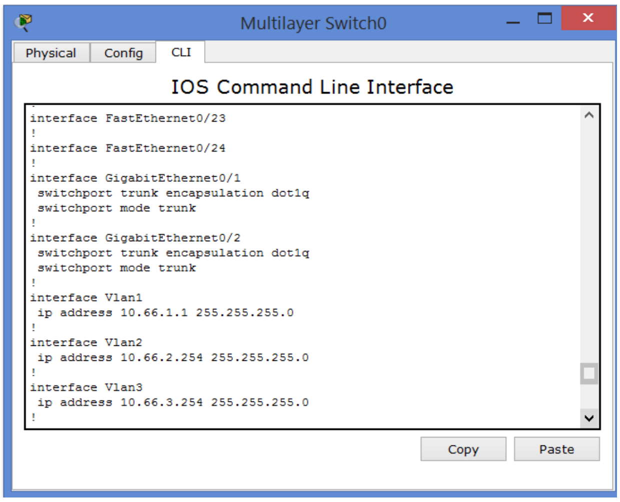
Fig.1The simulated network consisting of Layer 2 and Layer3 switches

The above figure shows the simulated network in Packet Tracer which was used to implement port security. The network features switches and personal computers configured to communicate through the switch ports.



```
User Access Verification

Password:

mgit>en
Password:
mgit#sh run
Building configuration...

Current configuration : 1394 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname mgit
!
!
!
enable password cisco123
```

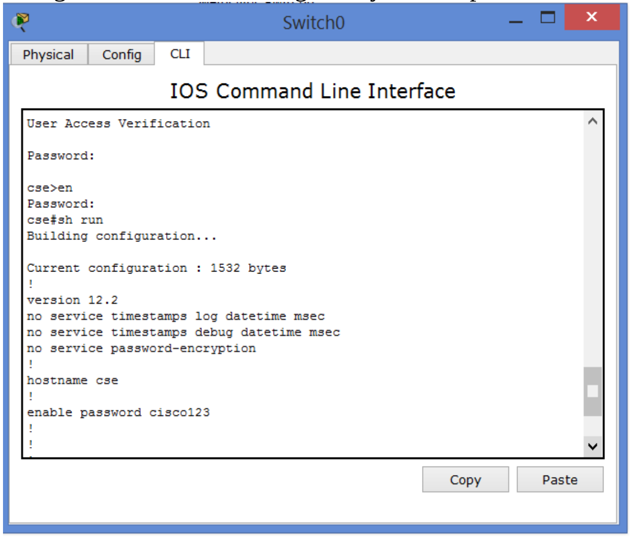
Fig 2. Command line interface to configure the Layer 3 switch which acts as a router



```
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 ip address 10.66.1.1 255.255.255.0
!
interface Vlan2
 ip address 10.66.2.254 255.255.255.0
!
interface Vlan3
 ip address 10.66.3.254 255.255.255.0
!
```

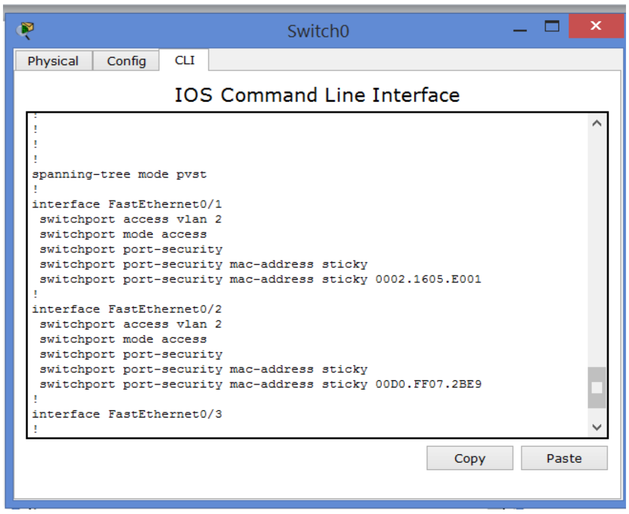
Fig 3. Configuration of the Layer 3 switch showing the configured virtual lan and ethernet ports

The above figures show the command line interface of the Layer 3 switch. This switch acts as the router and enables communication between the Layer 2 switches and personal coputers. The switches are trunked to the gigabitethernet ports and the virtual LANs are configured with the default gateways andrespective subnet masks.



```
User Access Verification

Password:

cse>en
Password:
cse#sh run
Building configuration...

Current configuration : 1532 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname cse
!
enable password cisco123
!
!
```

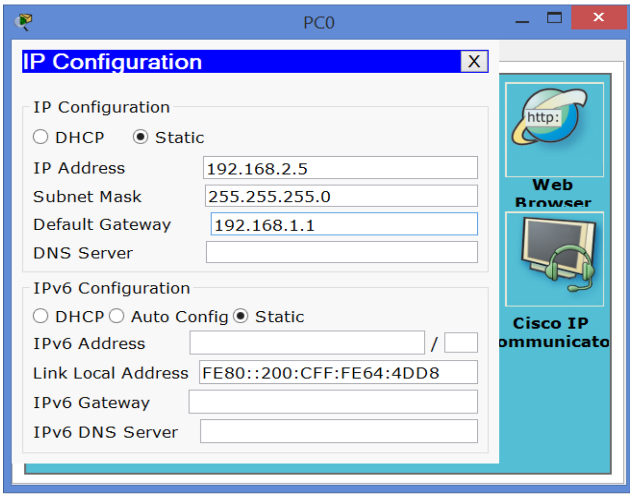
Fig 4. Command line interface to configure the Layer 2 switch to whose ports the PCs are connected



```
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0002.1605.E001
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.FF07.2BE9
!
interface FastEthernet0/3
!
```

Fig 5. Layer 2 switch configuration showing the MAC addresses of the computers binded to the fastethernet ports

The above figures show the configuration of the Layer 2 switches. The implementation of port security feature is done and this displays the MAC address of the computers which are binded to the Fastethernet ports. The virtual lan to which the switch is connected is also displayed in its running configuration.



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.2.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

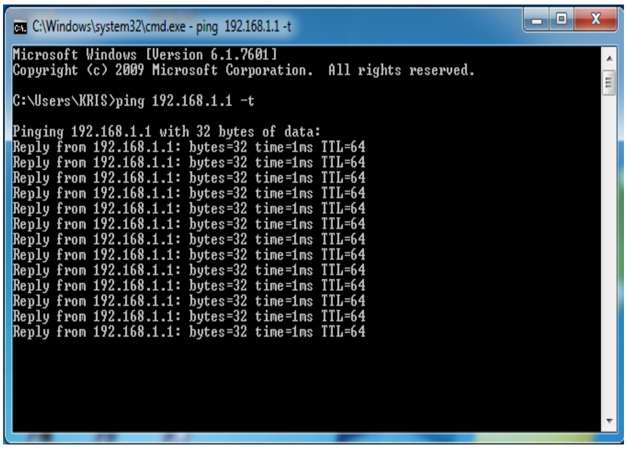
Link Local Address FE80::200:CFF:FE64:4DD8

IPv6 Gateway

IPv6 DNS Server

Fig 6. The IP configuration of the computers which are connected to the switch ports

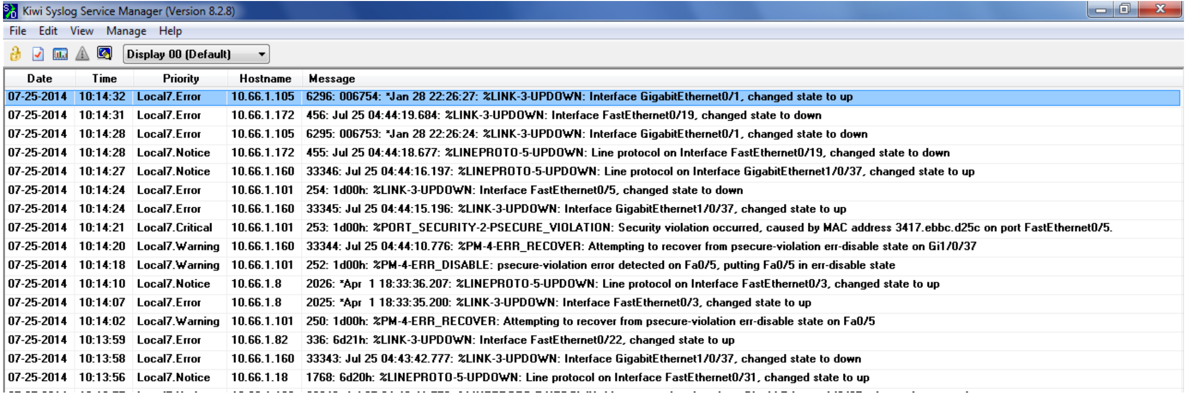
The above screen gives the IP configuration details of the connected computers. The IP address , subnet mask and the IP address of the connected switch is entered as the default gateway of the computer. The link local address is the MAC address of the computer.



```
C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\KRIS>ping 192.168.1.1 -t

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

Fig 7. Verification of communication between the computer and router

The above screen shows the communication between the router and personal computer in the command prompt. This verifies the connections between the components.


Kiwi Syslog Service Manager (Version 8.2.8)
File Edit View Manage Help
Display 00 (Default)

```
Date        Time      Priority        Hostname     Message
07-25-2014  10:14:32  Local7.Error    10.66.1.105  6296: 006754: *Jan 28 22:26:27: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
07-25-2014  10:14:31  Local7.Error    10.66.1.172  456: Jul 25 04:44:19.684: %LINK-3-UPDOWN: Interface FastEthernet0/19, changed state to down
07-25-2014  10:14:28  Local7.Error    10.66.1.105  6295: 006753: *Jan 28 22:26:24: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
07-25-2014  10:14:28  Local7.Notice   10.66.1.172  455: Jul 25 04:44:18.677: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/19, changed state to down
07-25-2014  10:14:27  Local7.Notice   10.66.1.160  33346: Jul 25 04:44:16.197: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/37, changed state to up
07-25-2014  10:14:24  Local7.Error    10.66.1.101  254: 1d00h: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
07-25-2014  10:14:24  Local7.Error    10.66.1.160  33345: Jul 25 04:44:15.196: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/37, changed state to up
07-25-2014  10:14:21  Local7.Critical 10.66.1.101  253: 1d00h: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 3417.ebbc.d25c on port FastEthernet0/5.
07-25-2014  10:14:20  Local7.Warning  10.66.1.160  33344: Jul 25 04:44:10.776: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Gi1/0/37
07-25-2014  10:14:18  Local7.Warning  10.66.1.101  252: 1d00h: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5, putting Fa0/5 in err-disable state
07-25-2014  10:14:10  Local7.Notice   10.66.1.8    2026: *Apr  1 18:33:36.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
07-25-2014  10:14:07  Local7.Error    10.66.1.8    2025: *Apr  1 18:33:35.200: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
07-25-2014  10:14:02  Local7.Warning  10.66.1.101  250: 1d00h: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/5
07-25-2014  10:13:59  Local7.Error    10.66.1.82   336: 6d21h: %LINK-3-UPDOWN: Interface FastEthernet0/22, changed state to up
07-25-2014  10:13:58  Local7.Error    10.66.1.160  33343: Jul 25 04:43:42.777: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/37, changed state to down
07-25-2014  10:13:56  Local7.Notice   10.66.1.18   1768: 6d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/31, changed state to up
```

Fig 8. Shows the port security validation in the logs maintained by the server

V. CONCLUSION

A growing challenge facing network administrators is determining how to control who can access the organization's internal network and who can't. In its most basic form, the port security feature remembers the Ethernet MAC address connected to the switch port and allows only that MAC address to communicate on that port. If any other MAC address tries to communicate through the port, port security will disable the port. The key benefit of port security is network availability which reduces campus wide network outages caused by broadcast storms by blocking nonstandard hubs and switches. Network reliability and network port bandwidth can be guaranteed if limited to one MAC address. Bandwidth can't be guaranteed if other network devices are sharing the network port. Also, port security implementation in the case of DHCP availability reduces the risk of over subscription of DHCP IP address per VLAN by limiting one MAC address per port. In addition, network security is maintained by limiting one MAC address per switch port which serves as an attack mitigation strategy. It also stops flooding attacks which force the switch to enter into repeater mode. These attacks are launched with the use of tools like macof. The above mentioned advantages of our suggested method port security make its implementation advantageous and effective.

REFERENCES

[1] Ray Hunt, "Internet/Intranet firewall Security-policy, Architecture and transaction services", Computer Communications, Vol.21, August 1998, pp.1107-1123.

[2] A. Aziz and W. Diffie "Privacy and Authentication for Wireless Local Area Networks", *IEEE Personal Communications*, vol. 1, no. 1, pp.25 -31 1994

[3] V. Bharghavan "Secure Wireless LANs", *Proceedings of the 2nd ACM Conf. on Computer Communications Security*, pp.10 -17 1994.

[4] K. Pahlavan, T. Probert and M. Chase "Trends in Local Wireless Networks", *IEEE Communications Magazine*, vol. 33, pp.88 -95 1995

[5] D. Mahony "Security Considerations in a Network Management Environment", *IEEE Network*, vol. 8, no. 3, pp.12 -17 1994.

[6] JesiekB., "Internet Security- Firewalls", Internet: http:/www.ee.mtu.edu/course/ee465/groupb/fwll.html.

[7] D. L. Lanthrop "Security Aspects of Wireless Local Area Networks", *Computers and Security*, vol. 11, pp.421 -426 1992.

[8] William stalling, "Cryptography and network Security", Prentice Hall, Second Edition, 2000

[9] Sandry kay Miller "Facing challenge of the wireless security ". IEEE Transaction on Computer, July 2001, pp 16-18.

[10] Randall K. Nichols "Wireless security", McGraw-Hill Telecom International Edition, 02.