Port Security Mechanism on Switch

Sanjeev Gangwar, Santosh Kumar Yadav,Ashok Kumar Yadav and Shravan Kumar Yadav

Umanath Singh Institute of Engineering and Technology, VBS Purvanchal University Jaunpur

(E-mail: gangwar.sanjeev@gmail.com,santosh.yadavo8@gmail.com,ashok231988@gmail.com, shravan.yadav08@gmail.com)

Abstract— Upgrade the security concept on the switch, we apply some code and general concept of switch security. By reduce the possibility of security problem, simply ignore the invalid device and improve the switch performance.

Keywords— *hub, collisiondomain, switch, bridge.*

I. INTRODUCTION

This Hub is use shared communication medium which is the reason of collision domain because medium are shared by all devices. We want to remove the collision we use another electronic device bridge. That processing decision is handling by operating system, By using this concept processing is slowdown, we use another device switch is use which is better than hub, bridge because both are not used shared medium, it provide dedicated link to all device. Any data are come to near to the switch. Then recently take decision and forward. It is not based on operating system. Decision making handle by ASIC special device .all node are joined to switch and take entry in CAM table. if any node want to communicate to another node then first entry in CAM table after that switch find the packet, then broadcast to all node, only left the source node which already connected and device give the reply to switch means that is new just connected. Which device are Not give the reply means that is already connected or already entry in CAM table by this process switch find the new node, when node that is connected to switch. On this a security concept is very necessary that which node is valid or invalid.

Any node are want to connect to with switch then simply switch connect all type of node .that is not able to categories that which is valid are invalid, for recognized valid port switch port is used port security tricky mechanism.

If you want see an about of any switch you run the ‘switch run show command’, then display that the specific port will enabled and disable port is shut down. How to show how many system are connected at that port at a time. another command is available which show all information of switch such as all information of MAC address which is connected to switch ,types of nodes ,on which port and how many time to live. together port security we also need switch security because without switch you cannot able to secure port security, in series of switch security always escape the switch password use console cable at align time does not display any attractive message and unused port always should be blocked by doing this we find port security in network.

II. LITERATURE REVIEW

Hub is an electronic device on which limited number of computer are connected on a single cooper wire means hub provide shared communication between devices, shared communications means available mbps are divided to all connected devices into equal mbps.

When two are more devices are used shared communication medium then all shared communication device are the part of collision domain. We are going to understand the concept collision domain by example we see the physical structure of hub .physical structure inside the hub.

Hub backbone is a copper wire, on the copper wire all devices are connected, if hub bandwidth is 100 mbps and 5 computers are connected. All computer find 20 mbps speed .these sharing are called shared medium.

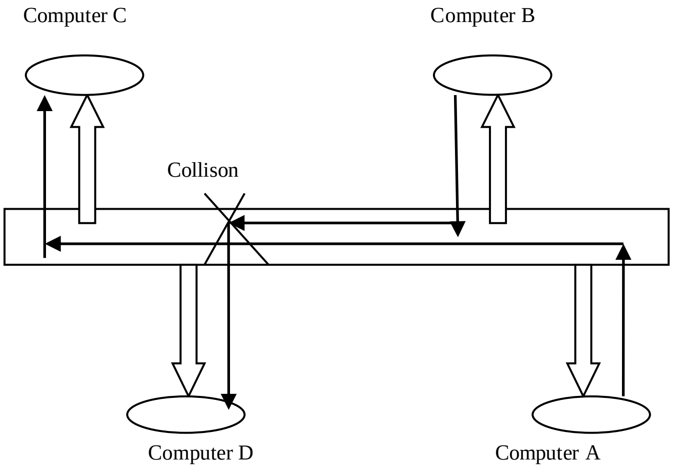

Fig. 1. Collision on Hub

Hub is collision domain devices the reason behind is that physical structure of hub. Collisions conditions occur when two devices used the signal on shared communication medium at same time then collision will occur.

A and C are used shared communication medium and A send data to C, but at time B and D also used the shared medium ,B send some data to D in this case collision occurred. Hub is a physical layer device you can say that hub is not intelligent device, it is a dump device, have two versions are come active hub and passive hub as shown in Fig. 1.

Bridge is a second layer device. it is an intelligent device and Based on self-operating system when any packet are come on the bridge, it learn the mac address and then forward to other device .

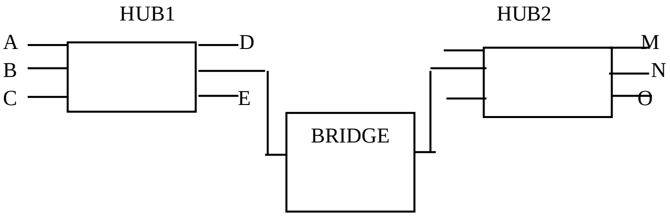

Fig.2. Simple Working of Bridge

In Fig. 2 A want to send a packet to device O. Hub A broadcast to all connected link left only sender device. A broadcast packet contains the destination device address of (O) MAC address and IP address. Hub a not found the device O on the hub. Then device A go to bridge, bridge also have a MAC table then forward the packet to hub2. Hub have no any MAC table then this reason hub2 forward packet to all connected node left on coming link .Match for the destination node then make the connection to O .bridge has less port no compassion to hub. Bridge take to decision to forward the packet is based on operation system so is slow.

Switch is a special type of device which provides a dedicated link to all connected device and works on ASIC based service. For this system increase the decision capability in comparison to hub and bridge .ASIC is a special type of circuit. which is establish in switch the main work of ASIC is any packet are come near the switch then take decision recently and forward the data it is establish on switch for decision making, not relation with operating system .so it is fast.

Any device is near to the switch for the purpose of data forwarding .switch take the entry of device in MAC table and if any new device wants to take a packet before establishing a connection it does not take any packet because entry is not in switch MAC table. switch follow the mechanism that is forward the packet to all remaining connected node on switch left only source node .which port give the reply .that mean is destination port, and which port is not give any reply means that node is already connected to the switch.

In Fig. 3 Suppose device 11,12,13 are on the switch ,device 11,12,13 entry in MAC table after some time device 14 are connect to switch and device 12 ,14 want to communicate to each other device 12 send to on switch device 14 are reply to switch after then switch store the MAC address and then device 12,14 are make connection

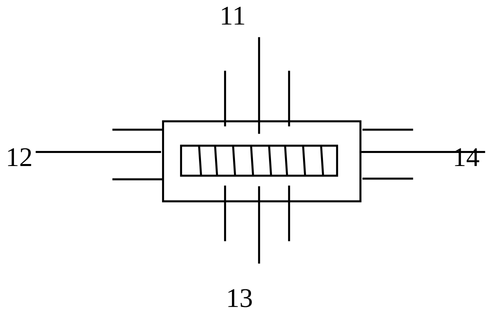

Fig.3. Simple Switch Working.

Switch have entry table and keep MAC address to all connected node a simple broadcasting problem is that, if any node want to send any packet to any node then broadcast to all node leave only source node. Switch broadcast a packet to all nodes. The reason is that. Some node joins the network and some node left the network. For this create a authentication problem. Which node is valid and which node is not valid. If new node wants to join on switch remove the old node on that port. Your old authenticated node left to the network. New Unauthenticated node make a connection on that port and take data.so need a port security.

III. PORT SECURITY AND NEED OF PORT SECURITY

Switch provide the security on the second layer which port is authorized and which port is not authorized .for this applied on some mechanism in this security series. If any node want to make a connection and which is not register on port means is invalid node. Port security blocks that port.

When unauthorized user want to access the reserve port (cable) which is already registered by any other system then a need of port security as shown in Fig. 4.

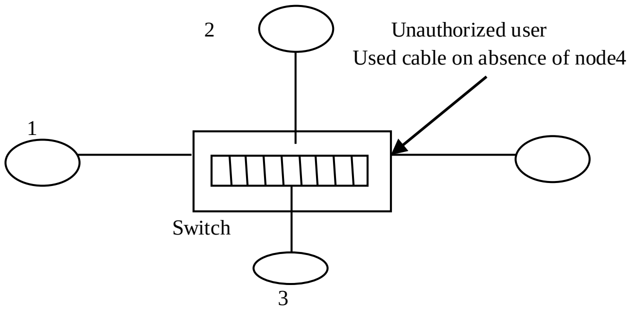

Fig. 4. Unauthorized User on Switch.

We apply the switch port security code on a switch for protecting unauthorized user and also apply some code on intelligent switch code panel.

In switch port security, on a port only one system connected at a time.

SwitchX (config-if) # interface fa0/5

We use advance and fast Ethernet. We have numbers of ports, and all port is enabling. And we apply path value and port security.

We run the command

switchX(config) # switch port mod access.

Access port is normal port where computer is connected by running this code.

SwitchxX(config-if) # switch port port-security.

We apply the security on the particular port from this code.

SwitchX(config-if)#switch port port security maximum,(max 1024).

This code means on this particular port only one device connected at this port no learn more address.

SwitchX(config-if)#switch port port security mod address stricky.

Which device connects first time then MAC table store all connected MAC address in MAC table. Only one MAC address store on particular port, not more than two MAC address on that port number.

SwitchX(config-if)#switch port port security violation shutdown.

If any device want to make a connection on the place of any other port number. First Match the MAC address, if MAC address match then allow either shutdown the port.

This code does not allow any other device on that port because only single port allow on single MAC address. Learn the MAC address. If change means violation, then shutdown that port.

In port security user and privileged password are used. Any device does not login directly in switch. We do designed some user id and password. For this we can find some security.

First level of security is physical. In this level security we physically enter in switch by console cable.

The login banner can be used to display a massage before the user is prompted for a user name.

User does not provide any legal information about the switch, which is useful information for the hacker. We can reserve MAC address on switch port according to our requirement and the remaining unreserved port must be shut down.

IV. RESULT

In the switch security, we apply security concept in the form of some code and general concept both. We find the security on switch and decrease the possibility of security problem .this ignore the connectivity of invalid device on switch and also improve the processing and capability of the switch.

REFERENCES

[1] Aastrup J, Halldórsson A (2008) Epistelmological role of case studies in logistics: a critical realist perspective. Int J Phys Distrib Logist Manag 38(10):746–763.
[2] PortID Consortium, “Study for the Analysis and the Conceptual Development of an European port Access Identification Card (EPAIC)”, Final Report, QINETIC/07/03289,19 Dec 2007.
[3] Ntouskas, T., Polemi, N., "Collaborative security management services for Port Information Systems", Proc. of International Conference on eBusiness, ICE-B 2012, Rome, Italy, SciTePress, pp. 305-308.
[4] Harrald J, Stephens H, Dorp JV (2004) A framework for sustainable port security. J Homel Sec Emerg Manag 1(2).
[5] Kabay, M. E.2002.Computer Security Handbook: Using Social Psychology to Implement Security Policies 4th ed. Wiley & Son, New York, 35.1-6.
[6] Edgerton, M. 2013. “A Practitioner's Guide to Effective Maritime and Port Security”, John Wiley &Sons, Inc., Hoboken, New Jersey.
[7] Christopher, K .2014.Port Security Management.2nd ed. Boca Raton, Florida: Taylor &Frances Group, 67.
[8] Bichou K (2004) The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management. Marit Econ Logist 6:322–348.
[9] F. Andritsos, M. Mosconi, “Port Security in EU: a Systemic Approach”, 2nd International Conference on Waterside Security (WSS 2010), Marina di Carrara, Italy, November 2010.
[10] I.Vakalis, B.Hosgood, P.Chawdry, “Biometrics for Border Security – An Overview”, Technical Report EUR 22359 EN, European Communities 2006.

Sanjeev Gangwar is assistant professor in the department of computer application, VBS Purvanchal University Jaunpur (U.P.). He obtained his MCA degree from MJP Rohilkhand University Bareilly and M.Phil in computer science. He has more than 10 years teaching experience in different organization. He is member of different reputed journals: (1) International Association of Engineers (IANEG) (Id:116368); (2) International Association of Computer Science and Information Technology (IACSIT) (Id: 80343128). He has got published eleven papers in reputed national/international journals. His research interests are in the field of mobile Ad hoc networks.

Santosh Kumar Yadav is lecturer in the department of information technology, VBS Purvanchal University Jaunpur (U.P.). He has master of technology in computer science and engineering from Uttar Pradesh Technical University Lucknow. He has more than eight years teaching experience in different organizations. He has published three papers in national journals. His current research interests are computer network, network security, algorithm design and mobile Ad hoc networks.

Ashok Kumar Yadav is lecturer in the department of information technology, VBS Purvanchal UniversityJaunpur (U.P.). He has master of technology in computer science and engineering from Uttar Pradesh Technical University Lucknow. He has got international certification in Oracle 9i (OCA). He has more than four years teaching experience in different organizations. He has published two papers in international journals. His current research interests are computer network, mobile Ad hoc networks and parallel algorithm.

Shravan Kumar Yadav is lecturer in the department of Computer Science & Engineering, VBS Purvanchal University Jaunpur (U.P.). He has master of technology in computer science and engineering from Uttar Pradesh Technical University Lucknow. He has more than three years teaching experience in different organizations. He has published two papers in national/international journals. His current research interests are computer network, network security and mobile Ad hoc networks.