INCREASING NETWORK EFFICIENCY BY PREVENTING ATTACKS AT ACCESS LAYER

G.Narasimha[1], M. Jithender Reddy[2]

[1]*Assoc. Professor, JNTU Nachupally*
[2]*Asst. Professor and Cisco, Instructor, VCE*

Abstract

The design of complex Networks follows three layer architecture, which is scalable and provides redundant paths for data transmission. The layers include: Access Layer, Distribution Layer and Core Layer. Access layer devices are used to connect end devices on the same network and Distribution Layer uses multi layer switches, which provides features like redundant paths, link aggregation, access control lists, and quality of services(QOS). And Core layer devices transfers data as fast as possible to various networks without much delay.

At Access layer, switches are used to connect multiple devices on the network. They are mainly vulnerable to attacks within the network by malicious users. Generally, networks are secured by using firewalls or implementing access control lists on a router. Routers or firewalls can prevent illegitimate traffic entering the network. But, they cannot prevent attacks within the network. Switches are vulnerable to attacks like MAC address flooding, DHCP starvation, DHCP snooping , denial-of-service and etc. In this paper I would like to provide necessary configuration required to protect network resources and also to give an insight to design networks, to improve throughput and reduce broadcast traffic.

To address the above issues, a topology is designed using PACKET TRACER (network simulator) to demonstrate the vulnerabilities at access layer, and also shows the configuration required to protect the network from the above said attacks. Further, it also addresses the issue of increasing the efficiency of the network.

Keywords- *Content Addressable MAC, Virtual LAN, Medium Access Control Table, Switch Port Security, Dynamic Host Configuration Protocol, DHCP starvation, DHCP snooping.*

----------***----------

1. INTRODUCTION:

At access layer, switches are used to connect end devices to the same network. Access layer switches controls data flow at the access layer to networked resources. Switches send unicast traffic to the desired node only. It won`t be sending unicast traffic to all the nodes. And at same time it allows multiple communications to take place simultaneously. But, they do not have any control on the broadcast traffic. To control broadcast traffic, layer 3 devices such as Routers are required.

Switches work at layer 2, which is an intelligent device as compared to layer 1 devices. Switches maintains database, known as MAC address table which consists of MAC-ADDRESS and PORT address. With the help of this table, it guides the frame to reach the desired node. When switch receives a frame, it checks for the destination address in the MAC table. If destination address is found in the table, it determines the port address. Then, it forwards the frame through the port. If destination address is not found in the table, forwards the frame through all the ports except the incoming port.

Switches contains an operating system called Internetwork operation system(IOS), switches run IOS and can be manually configured to better meet the needs of the network. Additional configurations are necessary for them to protect from malicious users. This includes port security, configuring SSH, removing TELNET, adjusting port speed, bandwidth and security requirements.

Additionally, Cisco switches can be managed both locally and remotely. To remotely manage a switch, it needs to have an IP address and default gateway configured. Switches operate at the access layer, where client network devices connect directly to the network. It is one of the most vulnerable areas of the network because it is so exposed to the user. Switches need to be configured to be resilient to attacks of all types while they are protecting user data and allowing for high speed connections. Port security is one of the security features, switches provide.

In the figure1 shown, the switch virtual interface (SVI) on S1 should be assigned an IP address. The SVI is a virtual interface, not a physical port on the switch.

Basic switch security does not stop malicious attacks. Security is a continuous process, that is essentially never complete. The network administrator must be well aware about security attacks and the dangers they pose. Some types of security attacks are listed here.

- MAC Address Flooding
- DHCP Starvation
- DHCP snooping and
- Telnet Denial-of-service

2. MAC ADDRESS FLOODING

The MAC address table in a switch, contains the MAC addresses associated with each physical port. The switch maintains MAC address database to guide the received frame. It sends the frame to the desired port if the destination address is found in the table. Otherwise, it floods the frame out of every port on the switch, except the port where the frame was received.

The MAC address flooding behavior of a switch for unknown addresses can be used to attack a switch. This type of attack is called a MAC address table overflow attack. MAC address table overflow attacks are sometimes referred to as MAC flooding attacks, and CAM table overflow attacks. The figures show how this type of attack works.

In the figure1 , the MAC ADDRESS table is populated with device MAC address and the number of the port to which the device is connected. The below topology depicts the scenario of MAC table which is not attacked by the rogue user. In the given topology, when the PC1 sends traffic to PC3. The switch receives the frames and looks up the destination MAC address in its MAC address table. If there is a match for destination MAC address, it sends the frame through the port to which the device is connected.

If the switch cannot find the destination MAC in the MAC address table, then the switch floods (broadcasts) it out of every switch port, except the port where it was received. Here, PC3 is connected to port 3 shown in the MAC table.

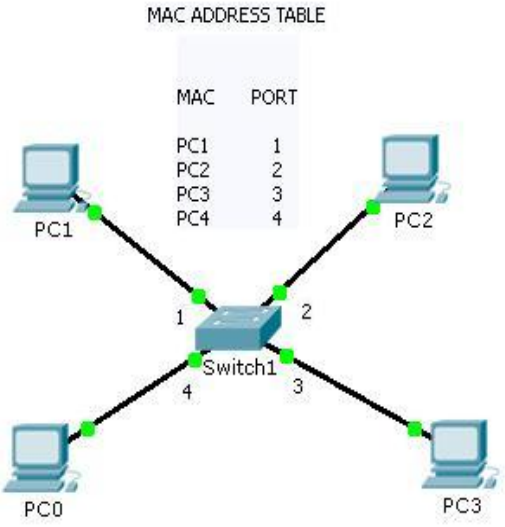

Fig 1

In the figure 1, PC3 receives the frame and sends a reply to PC1. The switch then learns that the MAC address for PC1 is located on port 1.

As shown in figure 1, any frame sent by PC0 (or any other host) to PC2 is forwarded to port 2 of the switch and not broadcast out every port.MAC address tables are limited in size. MAC flooding attacks make use of this limitation to overwhelm the switch with fake source MAC addresses until the switch MAC address table is full.

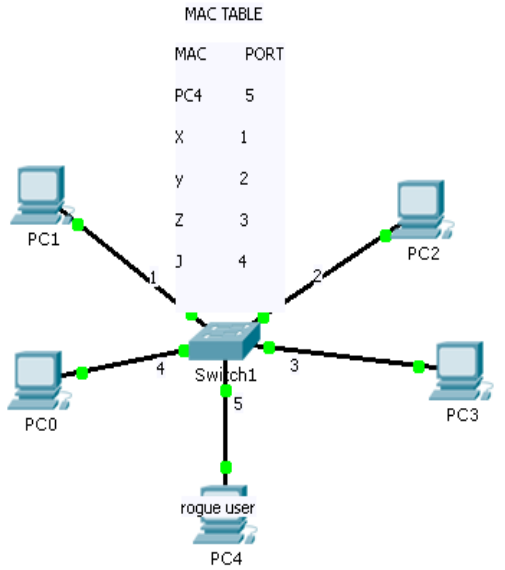

Fig 2

As shown in figure 2, an attacker (rogue user) at PC4 can send frames with fake, randomly-generated source and destination MAC addresses to the switch. The switch populates the MAC address table with the fake frames. When the MAC address table is full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. This operation is similar to layer 1 device such as HUB. As a result, the attacker can see all of the frames.

As shown in figure 2, as long as the MAC address table on the switch remains full, the switch broadcasts all received frames out of every port. In this example, frames sent from PC2 to PC4 are also broadcast out of port 5 on the switch and seen by the attacker at PC4.

2.1 DHCP Starvation

This is another attack, which is done at access layer by the malicious user within the network. DHCP is the service which has been in use extensively for providing IP configuration to the client machines. To obtain configuration information from the DHCP server clients sends a request as a broadcast packet in the network. If any DHCP server is present, it responds with the offer of IP address configuration.

Two types of DHCP attacks can be performed against a switched network: DHCP starvation attacks and DHCP spoofing.

In DHCP starvation attacks, an attacker floods the DHCP server with DHCP requests persistently to obtain all the available IP addresses that the DHCP server can issue. After these IP addresses are issued, the server cannot issue any more addresses, and this situation produces a denial-of-service (DoS) attack as new clients cannot obtain network access. A DoS attack is any attack that is used to overload specific devices and network services with illegitimate traffic, thereby preventing legitimate traffic from reaching those resources.

3. DHCP SPOOFING

After the DHCP server is attacked and led to starvation then the attacker configures a fake DHCP server on the network to issue DHCP addresses to clients. Thel reason for this attack is to force the clients to use false Domain Name System (DNS) servers and to make the clients use the attacker, or a machine under the control of the attacker, as their default gateway.

DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server, making it easier to introduce a fake DHCP server into the network.

4. TELNET ATTACKS

The Telnet protocol is insecure because it does not employ encryption mechanism. This loop-hole is used by an attacker to gain remote access to a network device. There are tools available that allow an attacker to launch a brute force password-cracking attack against the VTY(virtual terminal) lines on the switch or Router.

4.1 Telnet DoS Attack

In a Telnet DoS(denial-of-service) attack, the attacker exploits a flaw in the Telnet server software running on the switch by sending the ping packets continuously with that the Telnet service becomes unavailable. This sort of attack prevents an administrator or the genuine user from remotely accessing network resources.

To protect our network against attack requires vigilance and education. The following are best practices for securing a network:

- Shut down unused services and ports.
- Use strong passwords and change them often.
- Control physical access to devices.
- Educate employees about social engineering attacks, and develop policies
- Implement security hardware and software, such as firewalls.

These methods are only a starting point for security management. Organizations must remain vigilant at all times to defend against continually evolving threats. Use network security tools to measure the vulnerability of the current network.

Network security testing techniques may be manually initiated by the administrator. The administrator who conducts the security testing should have extensive security and networking knowledge. This includes expertise in the following areas:

- Network security
- Firewalls
- Intrusion prevention systems
- Operating systems

5. SOLUTIONS TO PREVENT ATTACKS AT ACCESS LAYER

Access layer is prone to attacks like MAC-ADDRESS flooding, DHCP starvation, DHCP spoofing and Telnet denial-of-service attack. The following are the solutions to mitigate the above said attacks.

5.1 MAC-ADDRESS Flooding:

In IT organizations, a malicious user having grudge on the superiors, may attack MAC-ADDRESS table. To overcome from this attack, switch ports should be secured. One way to secure is, using a feature called switch port-security. Port security limits the number of valid MAC addresses allowed on a port. The MAC addresses of correct devices are allowed

access, while other MAC addresses are denied.Port security has to be configured to restrict or allow one or more MAC addresses. If the number of MAC addresses allowed on the port is limited to one, then only the device with that specific MAC address can successfully connect to the port.

A port can be configured to secure switch ports and if switch receives more MAC-ADDRESS than configured, it leads to security violation.There are a number of ways to configure port security.A switch port is configured to allow a particular device with a specific MAC-ADDRESS or certain number of MAC-ADDRESSes. If a port violation takes place then the switch takes following actions based on the configuration

Switch interfaces can be configured for one of three violation modes.
Protect - When the port reaches the maximum allowed MAC addresses limit allowed on the port, packets other than configured source addresses are dropped. There is no notification that a security violation has occurred.

Restrict - When the number of MAC addresses reaches the limit allowed on the port, packets from other source addresses are dropped. In this mode, there is a notification that a security violation has occurred.

Shutdown - In this mode, if a port reaches maximum allowed, a security violation occurs. If security violation occurs, then the port is disabled or shutdown.

The following is the configuration required to protect the access layer switch.

The below configuration shows the commands needed to configure port security on the Fast Ethernet F0/18 port on the S1 switch. To configure port security on switch S1 one has to be in global configuration mode.

S1(Config)#interface F0/18
S1(Config-if)#switchport mode access

Switches can be configured in two modes. One in access mode, wherein ports are allowed for access, and second one in trunk mode wherein it allows a particular port to send different VLAN(Virtual LAN) traffic to a switch or a router.

S1(Config-if)#switchport port-security maximum 50

The above command restricts the number of MAC-ADDRESSes allowed on port F0/18 to 50.

Unused ports on the switch have to be disabled by using the following command.

S1(Config)#interface range F0/19-24
S1(Config-if)#shutdown

In the above example, ports F0/19 to F0/24 are unused.

With the above shown configuration, access layer switches are secured from malicious users within the network from MAC-ADDRESS flooding.

5.2 DHCP Starvation:

Dynamic Host Configuration Protocol provides IP address configuration to the clients dynamically. A malicious user can perform two types of DHCP attacks: DHCP starvation and DHCP spoofing.

We can prevent DHCP attacks by configuring the port to which DHCP server connected as trusted port. And we can configure other ports as untrusted ports. Trusted ports only can only provide DHCP configuration to the clients and untrusted ports can send only request messages. With this no rogue attacker can attack DHCP starvation and DHCP spoofing attacks .

The following is the configuration required to prevent from rogue attacker.

S1(config)#ip dhcp snooping

This is the command required to make a port as trusted port.

S1(config)#interface F0/1

Here, port F0/1 is made as trusted port.

S1(config-if)#ip dhcp snooping trust

To make a port as untrusted, the following configuration is required.

S1(config-if)#interface F0/2

Here, port F0/2 is made as untrusted, that means it can only request IP configuration. By using the above configuration, we can make DHCP servers provide IP configuration services to the clients through the trusted ports only. So, no rogue user is given chance to attack DHCP sever. As port-security is configured for the used ports with certain limit, no rogue user is allowed to obtain all the IP addresses from one port. If he tries to access, it leads to port violation. With this, we can overcome DHCP starvation and DHCP snooping attack.

5.3 TELNET Denial of Service Attack:

To mitigate against brute force password attacks use strong passwords that are changed frequently. A strong password should have a mix of upper and lowercase letters and should include numerals and symbols (special characters). Access to the vty(virtual terminal) lines can also be limited using an access control list (ACL).

It is a best practice to use SSH, rather than Telnet for remote management connections.

SSH(secure shell) is used to access unix server, Linux server, switch or a router. As SSH employs encryption mechanism, it is safe to use SSH rather than TELNET.

6. EFFICIENT DESIGN OF NETWORKS

In recent times, the evolution of Internet has been faster and its usage has grown wide spread. The networks have to be scalable, efficient and robust against any attacks. Networks have to be designed to have less broadcast traffic. If more devices are connected to network, broadcast traffic increases. And performance of the network comes down. To reduce broadcast traffic, the technique used is to divide a big network into two or more networks. Routers are required to divide a network into two or more networks. Routers not only determine the path for data transmission, it also confines broadcast traffic within the network. Hence, it is known as broadcast domain. The technique used to increase the performance of a network is by reducing the broadcast domain size.

One can also improve the performance of the network by logically dividing a network into multiple virtual LANs. This division is done at layer two access layer device called "SWITCH".

7. CONCLUSIONS

Access layer devices are vulnerable to attacks like MAC-ADDRESS flooding, DHCP starvation, DHCP snooping and Telnet denial-of-service. we can prevent MAC-ADDRESS flooding attacks by configuring switch port security on access layer switches. In addition to that, unused ports have to be disabled.

Particularly, we can overcome DHCP starvation and DHCP snooping attack by configuring the port as service port, to which DHCP server is connected and rest all as request ports. With that attacker won`t be having any chance to provide IP address configuration and DHCP snooping.

If telnet is attacked by hacker, then users are denied services, hence, known as Telnet Denial-of-service attack. Telnet is more vulnerable to Denial-of-service attacks, as it does not use encryption mechanism. To overcome from this attack, replace telnet with SSH, which is more secured to access networking devices. SSH enforces strong encryption mechanism, therefore, it is better option to use rather than telnet.

This paper has provided solutions to the attacks at access layer, particularly switches. In this paper, problems at access layer are shown and demonstrated using a simulator called "PACKET TRACER". And in addition to that, suggested the ways to design complex networks. Perfect network design increases the efficiency of the network. With that throughput that utilization of the network increases. And also reduces the broadcasts traffic in a network by reducing the size of the network physically with routers or dividing a LAN into virtual LANs with switches at access layer.

Network performance is a key factor in the productivity of an organization. To improve performance, necessary steps have to be taken to mitigate attacks at access layer.

REFERENCES

[1] Mitigating worm protection on virtual LANS; Rajput,S,;xiaoguang Sun;Hsu,s, Publication Year: 2006 , Page(s): 555 - 556

[2] Protecting and controlling virtual lans by linux router-firewall; Katic,T,. T,;Sikic, M;Sikic, K ,Infofrmation Technology,Publication Year: 2005 , Page(s): 518 – 523

[3] IEEE Computer Society. IEEE std 802.1x-2001, Port Based Network Access Control, 2001.

[4] IEEE Computer Society. IEEE 802.1: 802.1Q - Virtual LANs. http://www.ieee802.org/1/pages/802.1Q.htm

[5] Application of dynamic port VLAN membership with auxillary VLAN in campus area network by Ning Ziang, Liancheng shan, Jing Zhao in International conference on Hybrid Intelligent systems.,August 2009, PP 279-282

[6] www..netacad.com

[7] www.juniper.net/in

[8] www.cisco.com