University of Khartoum

Information technology & Network Administrator

Switch port security

Presented: by Ali Jbraldar
What is Network Security?

- National Security Telecommunications and Information Systems Security Committee (NSTISSC) Network security is the protection of information and systems and hardware that use, store, and transmit that information. Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resourc.
Network Security initiatives and network security specialists can be found in private and public, large and small companies and organizations. The need for network security and its growth are driven by many factors:

- Internet connectivity is 24/7 and is world wide
- Increase cyber crime
- Impact on business
- Proliferation of threats
- Sophistication of threats
Goals of an information security program

1. confidentiality
   Prevent the disclosure of sensitive information from unauthorized people, resources, and processes

2. integrity
   The protection of system information or processes from intentional or accidental modification

3. Availability
   The assurance that systems and data are accidental by unauthorized users when needed.
A potential danger to information or a system

- An example: the ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. There may be weaknesses that greatly increase the likelihood of a threat manifesting.
Types of Network Threats

1. Eavesdropping
2. Denial-of-service
3. Packet replay
4. Packet modification
Types of Attacks
Come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.
2. Unstructured attack

Consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker’s skills can still do serious damage to a company.
MAC Address attacks

- MAC spoofing
- 2-MAC address table overflow attacks

**MAC spoofing:**
is a technique for changing a factory-assigned Media Access Control (MAC) **address** of a network interface on a networked device. The **MAC address** that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the **MAC address** to be changed.
MAC Address Spoofing Attack

The switch keeps track of the endpoints by maintaining a MAC address table. In MAC spoofing, the attacker poses as another host—in this case, AABBcc.

I have associated Ports 1 and 2 with the MAC addresses of the devices attached. Traffic destined for each device will be forwarded directly.
MAC Address Spoofing Attack

I have changed the MAC address on my computer to match the server.

The device with MAC address AABBcc has changed locations to Port2. I must adjust my MAC address table accordingly.
MAC address flooding attack is very common security attack. MAC address table in a switch has the MAC addresses available on a given physical port of a switch and the associated VLAN parameters for each. MAC flooding attacks are sometimes called MAC address table overflow attacks. To understand the mechanism of a MAC address table overflow attack we must recall how does a switch work in the first place.

- **Switch before attack**
  When switch receives a frame, the switch looks in the MAC address table (sometimes called CAM table) for the destination MAC address. Cisco Catalyst switch models use a MAC address table for Layer 2 switching. When frames arrive on switch ports, the source MAC addresses are learned from Layer 2 packet header and recorded in the MAC address table. If the switch has already learned the mac address of the computer connected to his particular port then an entry exists for the MAC address. In this case the switch forwards the frame to the MAC address port designated in the MAC address table. If the MAC address does not exist, the switch acts like a hub and forwards the frame out every other port on the switch.
But this is where the attacker is coming into play. The key to understanding how MAC address table overflow attacks work is to know that MAC address tables are limited in size. MAC flooding makes use of this limitation to send to the switch a whole bunch of fake source MAC addresses until the switch MAC address table is fully loaded and cannot save any more MAC address – Port mapping entries. The switch then enters into a fail-open mode that means that it starts acting as a hub. In this situation switch will broadcasts all received packets to all the machines on the network. As a result, the attacker (in our case “PC”) can see all the frames sent from a victim host to another host without a MAC address table entry.
Port security is a layer 2 and 3 traffic control feature on Cisco Catalyst switches. It enables an administrator to configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. Anyone can access unsecure network resources by simply plugging his host into one of our available switch ports. A user can also change his physical location in LAN network without telling the admin. You can secure layer two accesses as well as keep users in their tracks by using port security. Thus port security feature enhances the LAN security.
To begin with, there are three different types of secure MAC address:

**Dynamic secure MAC addresses**
This type of secure MAC address is learned dynamically from the traffic that is sent through the switchport. These types of addresses are kept only in an address table and not in the running configuration.

**Static secure MAC addresses**
This type of secure MAC address is statically configured on a switchport and is stored in an address table and in the running configuration.

**Sticky secure MAC addresses**
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.
by default, the maximum number of secure MAC addresses per switchport is limited to 1) An address learned or configured on one secure interface is seen on another secure interface in the same VLAN
The second piece of switchport port-security that must be understood is a security violation including what it is, what causes it, and what the different violation modes that exist. A switchport violation occurs in one of two situations.

**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.

**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.

**Shutdown**
This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error disabled (err-disable) state when a violation occurs. While in this state, the switchport forwards no traffic. The switchport can be brought out of this error disabled state by issuing the `errdisable recovery cause` CLI command or by disabling and reenabling the switchport.
<table>
<thead>
<tr>
<th>Step 1</th>
<th>Switch(config)# interface interface_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Switch(config-if)# switchport mode (access)</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch(config-if)# switchport port-security</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch(config-if)# switchport port-security mac-address (static-sticky)</td>
</tr>
<tr>
<td>Step 5</td>
<td>Switch(config-if)# switchport port-security maximum value</td>
</tr>
<tr>
<td>Step 6</td>
<td>Switch(config-if)# switchport port-security violation {restrict</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>Port security verifications</strong></td>
</tr>
</tbody>
</table>

- show port-security
- show port-security interface_id
- show port-security address
Port Based Authentication
The AAA working group is chartered to work on authentication, authorization, and accounting solutions for the Internet. This work consists of a base protocol, applications, end-to-end security application, and a general architecture for providing these services.
Authentication: provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.
Authentication type

1- **Authentication password only**
   Uses a login and password combination on access lines
   - Easiest to implement, but most unsecure method
   - Provides no accountability

2- **Authentication local database**
   Creates individual user account/password on each device
   - Provides accountability
   - Secure
Authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication.
accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.
TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
Raduis: a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

- RADIUS stands for Remote Authentication Dial In User Service.
- Transactions between a client and a server are authenticated through the use of a shared key. This key is never sent over the network.
- Password is encrypted before sending it over the network.
- It uses Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) protocols to authenticate users.
- It look in text file, LDAP Servers, **Database for authentication**.
- SNMP is used for remote monitoring.
- It can be used as a proxy
- Uses UDP ports 1645 or 1812 for authentication and UDP ports 1646 or 1813 for accounting
RADIUS Authentication Process

1. Username?
2. JR-ADMIN
3. Password?
4. Str0ngPa55w0rd
5. Access-Request (JR_ADMIN, "Str0ngPa55w0rd")
6. Access-Accept
TACACS is a remote authentication protocol that is used to communicate with an authentication server commonly used in Unix networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

Provides separate AAA services
Utilizes TCP port 49
**TACACS+ Authentication Process**

1. **Connect**
2. **Username prompt?**
3. **Use “Username”**
4. **Username?**
5. **JR-ADMIN**
6. **JR-ADMIN**
7. **Password prompt?**
8. **Use “Password”**
9. **Password?**
10. **“Str0ngPa55w0rd”**
11. **Accept/Reject**
12. **“Str0ngPa55w0rd”**
<table>
<thead>
<tr>
<th>RADIUS</th>
<th>TACACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open/RFC standard</td>
<td>CISCO Supported</td>
</tr>
<tr>
<td>UDP</td>
<td>TCP</td>
</tr>
<tr>
<td>Password encrypted</td>
<td>Entire packet encrypted</td>
</tr>
</tbody>
</table>
- switch(config)# aaa new-model
- switch(config)#radius-server host (hostname - ip addresss) {key string}
- switch(config)#aaa authentication dot1x default group radius
- switch(config)#dot1x system-auth-control
- switch(config)#interface- id
- switch(config-if)#dot1x port-control {force-authoried- force-unauthoried- auto}
- switch(config-if)#dot1x host-mode multi-host
DHCP Spoofing Attack (Rogue DHCP)

DOS attack
Man in the middle attack
DHCP: Dynamic host configuration protocol

Allocates IP Addresses Dynamically
DHCP Snooping
The DHCP snooping binding database is also referred to as the DHCP snooping binding table. The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a.

Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

**Note:** DHCP snooping is disabled in the default configuration of the switching device.
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping vlan -id
switch(config)#interface type
switch(config-if)# ip dhcp snooping trust
switch(config)#interface type
switch(config-if)ip dhcp snooping limit rate
  - **show command**
switch# show ip dhcp snooping
switch# show ip dhcp snooping binding
Dedicated bandwidth If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.

Added security—Unknown devices cannot connect to the port.
The use of switchport port-security provides another level of security that can help in securing locally connected computers and the networks they connect to. This article was written to make the basic features of port-security more familiar to the reader and offered as an additional option when securing a network. Hopefully, the information contained within this article will help in this and be able to serve as a research base for securing the switched network of the reader.