NETWORK SECURITY AND MONITORING

M.K.Khusanova, assistant,
Fergana branch of TUIT named after Muhammad Al-Khorazmiy,
Uzbekistan, Fergana

https://doi.org/10.5281/zenodo.7516648

Abstract: *This article describes common LAN security threats and how to mitigate them. It also describes the SNMP protocol and shows how to enable it for network monitoring and how to locally implement Switched Port Analyzer technology to capture and monitor traffic using port analyzers or IPS devices.*

Keywords: *Network devices, MAC address, VLAN attacks, security, DHCP Attacks, Securing device, passwords, protocol, port security.*

МОНИТОРИНГ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ

Аннотация: *В этой статье описываются распространенные угрозы безопасности локальной сети и способы их минимизации. А также, описывается протокол SNMP и показывается, как включить его для мониторинга сети и как локально реализовать технологию анализатора коммутируемых портов для захвата и мониторинга трафика с помощью анализаторов портов или устройств IPS.*

Ключевые слова: *Сетевые устройства, MAC-адрес, VLAN-атаки, безопасность, DHCP-атаки, Защитное устройство, пароли, протокол, безопасность порта.*

INTRODUCTION

A secure network is only as strong as its weakest link and Layer 2 is potentially the weakest link. Common Layer 2 attacks include CDP reconnaissance, Telnet exploitation, MAC address table flooding, VLAN attacks, and DHCP related attacks. Network administrators must know how to mitigate these attacks, and well as securing administrative access using AAA and securing port access using 802.1X.

Monitoring an operational network can provide a network administrator with information to proactively manage the network and to report network usage statistics to others. Link activity, error rates, and link status are a few of the factors that help a network administrator determine the health and usage of a network. Collecting and reviewing this information over time enables a network administrator to see and project growth, and may enable the administrator to detect and replace a failing part before it completely fails. SNMP is commonly used to collect device information.

RESEARCH MATERIALS AND METHODOLOGY

Network traffic must be monitored for malicious traffic. Network administrators use port analyzers and IPS devices to help with this task. However, the switched infrastructure does not enable port mirroring by default. Cisco SPAN must be implemented to enable port mirroring. This enables the switch to send duplicate traffic to port analyzers or IPS devices for monitoring of malicious, or questionable traffic.

Organizations commonly implement security solutions using routers, firewalls, Intrusion Prevention System (IPSs), and VPN devices. These protect the elements in Layer 3 up through Layer 7.

Layer 2 LANs are often considered to be a safe and secure environment. However, as shown in the figure, if Layer 2 is compromised then all layers above it are also affected. Today, with BYOD and more sophisticated attacks, LANs have become more vulnerable.

For example, a disgruntled employee with internal network access could capture Layer 2 frames. This could render all of the security implemented in layers 3 and above useless. The attacker could also wreak havoc on the Layer 2 LAN networking infrastructure and create DoS situations. Therefore, in addition to protecting Layer 3 to Layer 7, network security professionals must also mitigate threats against the Layer 2 LAN infrastructure.

The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the threats posed by the Layer 2 infrastructure.

Common attacks against the Layer 2 LAN infrastructure include:

- CDP Reconnaissance Attack
- Telnet Attacks
- MAC Address Table Flooding Attack
- VLAN Attacks
- DHCP Attacks

The first two attacks are focused on gaining administrative access to the network device. The remaining attacks are focused on disrupting the network operation. Other more sophisticated attacks exist. However, the focus of this section is on common Layer 2 attacks.

Telnet Attacks

The ability to remotely manage a switched LAN infrastructure is an operational requirement; therefore, it must be supported.

However, the Telnet protocol is inherently insecure and can be leveraged by an attacker to gain remote access to a Cisco network device. There are tools available that allow an attacker to launch attacks against the vty lines on the switch.

There are two types of Telnet attacks:

- **Brute Force Password Attack -** The attacker may use a list of common passwords, dictionary words, and variations of words to discover the administrative password. If the password is not discovered by the first phase, a second phase begins. The attacker uses specialized password auditing tools such as those shown in the figure. The software creates sequential character combinations in an attempt to guess the password. Given enough time and the right conditions, a brute force password attack can crack almost all passwords.
- **Telnet DoS Attack -** The attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable and preventing an administrator from remotely accessing a switch. This can be combined with other direct attacks on the network as part of a coordinated attempt to prevent the network administrator from accessing core devices during the breach.

There are several way to mitigate against Telnet attacks:

- Use SSH, rather than Telnet for remote management connections.
- 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).
- Limit access to the vty lines using an access control list (ACL) permitting only administrator devices and denying all other devices.
- Authenticate and authorize administrative access to the device using AAA with either TACACS+ or RADIUS protocols.

MAC Address Table Flooding Attack

One of the most basic and common LAN switch attacks is the MAC address flooding attack. This attack is also known as a MAC address table overflow attack, or a CAM table overflow attack.

RESEARCH RESULTS AND DISCUSSION

Consider what happens when a switch receives incoming frames. The MAC address table in a switch contains the MAC addresses associated with each physical port, and the associated VLAN for each port. When a Layer 2 switch receives a frame, the switch looks in the MAC address table for the destination MAC address. All Catalyst switch models use a MAC address table for Layer 2 switching. As frames arrive on switch ports, the source MAC addresses are recorded in the MAC address table. If an entry exists for the MAC address, the switch forwards the frame to the correct port. If the MAC address does not exist in the MAC address table, the switch floods the frame out of every port on the switch, except the port where the frame was received.

Figures 1 through 3 illustrate this default switch behaviour.

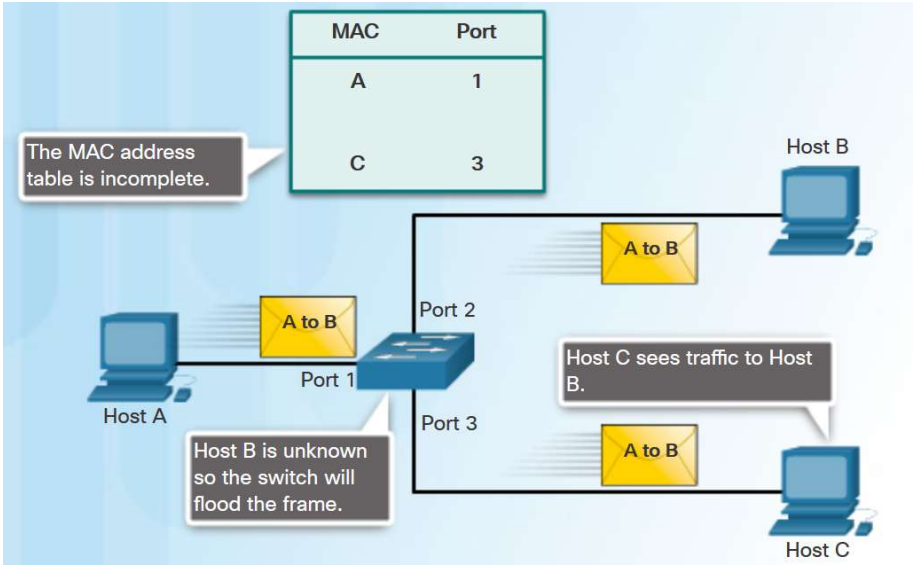

Figure 1. Switch Floods Frame for Unknown MAC.

In Figure 1, host A sends traffic to host B. The switch receives the frames and adds the source MAC address of host A to its MAC address table. The switch then looks up the destination MAC address in its MAC address table. If the switch does not find the destination MAC in the MAC address table, it copies the frame and floods (broadcasts) it out of every switch port, except the port where it was received.

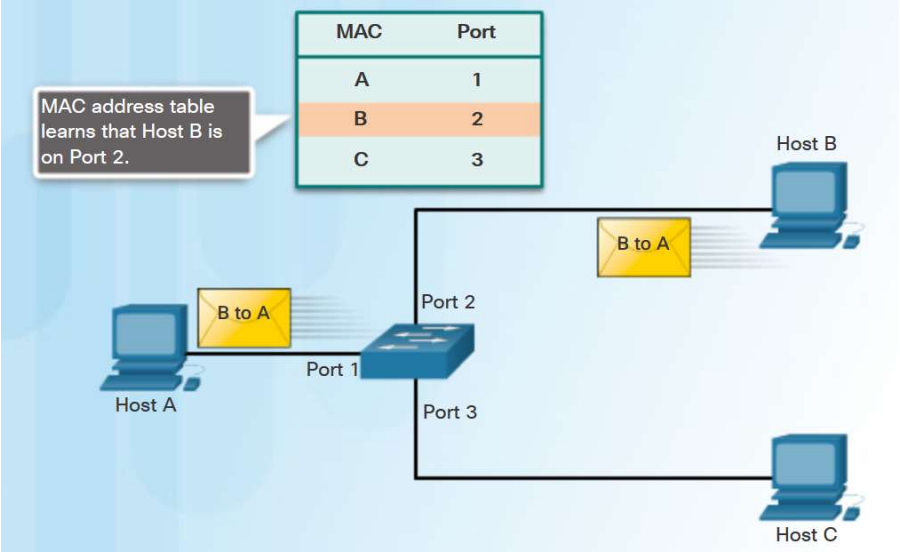

Figure 2. Switch Records MAC address.

In Figure 2, host B receives and processes the frame. It then sends a reply to host A. The switch receives the incoming frame from host B. The switch then adds the source MAC address and port assignment for host B to its MAC address table. The switch then looks for the destination MAC address in its MAC address table and forwards the frames out of Port 1 towards host A.

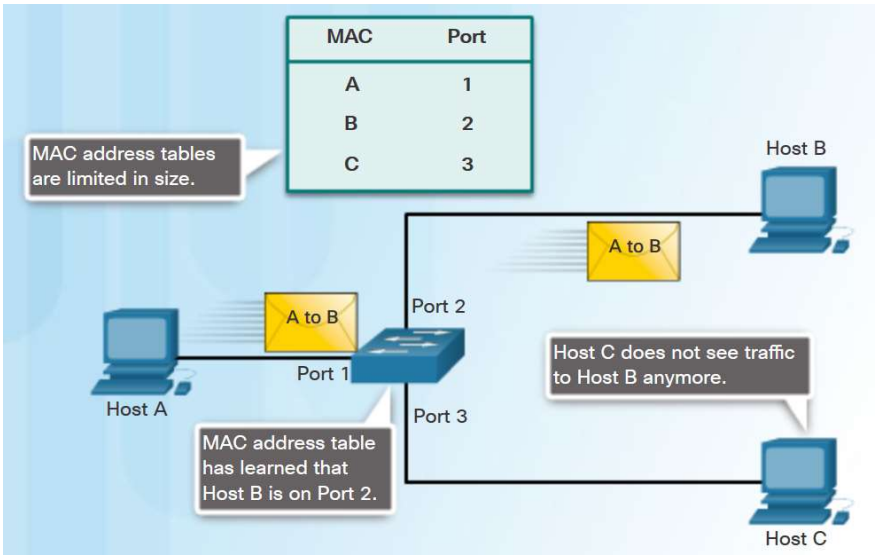

Figure 3. Switch Uses MAC address Table to Forward Traffic.

The MAC address table of the switch eventually learns all MAC addresses connected to it and forwards frames between communicating ports only. In Figure 3 for example, any frame sent by host A (or any other host) to host B is forwarded out port 2 of the switch. It is not broadcasted out every port because the switch knows the location of the destination MAC address.

An attacker can exploit this default switch behaviour to create a MAC address flooding attack. MAC address tables are limited in size. MAC flooding attacks exploit this limitation with fake source MAC addresses until the switch MAC address table is full and the switch is overwhelmed.

Figures 4 and 5 illustrate how a MAC address table flooding attack is generated.

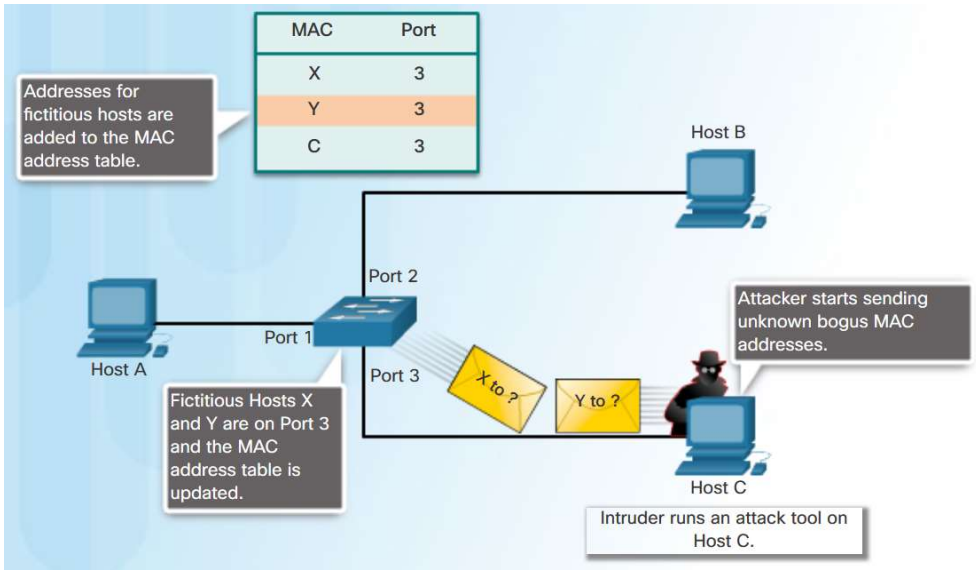

Figure 4. Attacker Initiates MAC address Flooding Attack.

In Figure 4, an attacker uses a network attack tool and continuously sends frames with fake, randomly-generated source and destination MAC addresses to the switch. The switch keeps updating its MAC address table with the information in the fake frames.

Eventually, the MAC address table becomes full of fake MAC addresses and enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can capture all of the frames, even frames that are not addressed to its MAC address table.

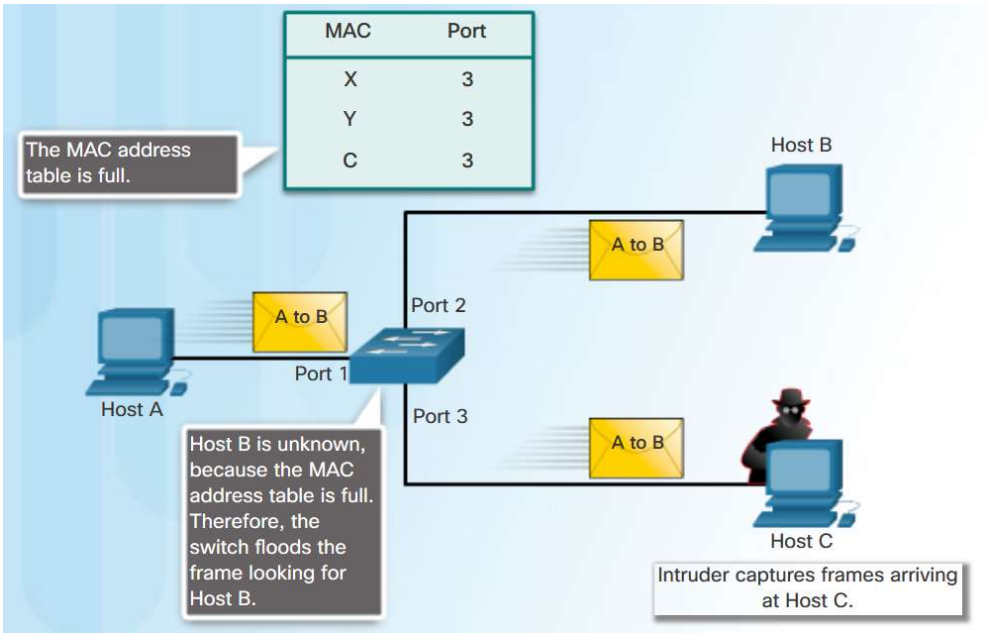

Figure 5. Switch is Compromised.

In Figure 5, the switch is in fail-open mode and broadcasts all received frames out of every port. Therefore, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker.

In order to prevent MAC address table overflow attacks, need to configure the port security settings on the switch.

Execution of works

Switch>enable

Switch#configure terminal
Switch(config)#hostname Sw1
Sw1(config)#interface fa0/1

1. Set the port to access mode

Sw1(config-if)#switchport mode access

2. Activate port-security on the port

Sw1 (config-if)#switchport port-security

3. Set the dynamic definition of secure-mac

Sw1 (config-if)#switchport port-security mac-address sticky
Sw1 (config-if)#exit

4. Set the static definition of secure-mac

Sw1(config)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security mac-address 000B.BE9B.EE4A
Sw1(config-if)#end

5. Setting the security breach response mode

Sw1(config)#interface fastEthernet 0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security mac-address sticky
Sw1(config-if)#switchport port-security violation protect
Sw1(config-if)#end

6. Disable unused ports

Sw1(config)#interface range fastEthernet 0/5-24
Sw1(config-if-range)#shutdown

7. Checking the result

Switch#show port-security interface fa 0/1

8. Save the configuration

Switch#copy running-config startup-config

The simplest and most effective method to prevent MAC table flooding attacks is to enable port security.

Port security allows an administrator to statically specify MAC addresses for a port, or to permit the switch to dynamically learn a limited number of MAC addresses. By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized expansion of the network, as shown in the figure.

CONCLUSION

When MAC addresses are assigned to a secure port, the port does not forward frames with source MAC addresses outside the group of defined addresses. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source addresses that were manually configured, or auto configured (learned), on the port.

If a port is configured as a secure port and the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation.

REFERENCES:

1. Khusanova M. K. ANALYSIS OF DISCRETE CONVOLUTION IN THE MATLAB PROGRAM //Scientific progress. – 2021. – T. 2. – №. 4. – C. 1023-1028.

2. Khusanova M. K. USING DECIMATION AND INTERPOLATION WHEN PROCESSING SIGNALS IN MATLAB //Scientific progress. – 2021. – T. 2. – №. 5. – C. 300-306.

3. Khusanova M. K. COMPARISON OF FILTERS WITH FINITE PULSE CHARACTERISTICS AND INFINITE PULSE CHARACTERISTICS IN MATLAB //Scientific progress. – 2021. – T. 2. – №. 5. – C. 292-299.

4. Bakhrom, B. (2022). Information technologies in physical culture and sports. *Asian Journal of Multidimensional Research*, *11*(10), 288-292.

5. Karimov, U., & Abdurakhmon, A. (2017). INNOVATIVE INFORMATION TECHNOLOGY IN EDUCATION. *Форум молодых ученых*, (5), 9-12.

6. Karimov, U. U., & Karimova, G. Y. (2021). THE IMPORTANCE OF INNOVATIVE TECHNOLOGIES IN ACHIEVING EDUCATIONAL EFFECTIVENESS. *Журнал естественных наук, 1*(1).