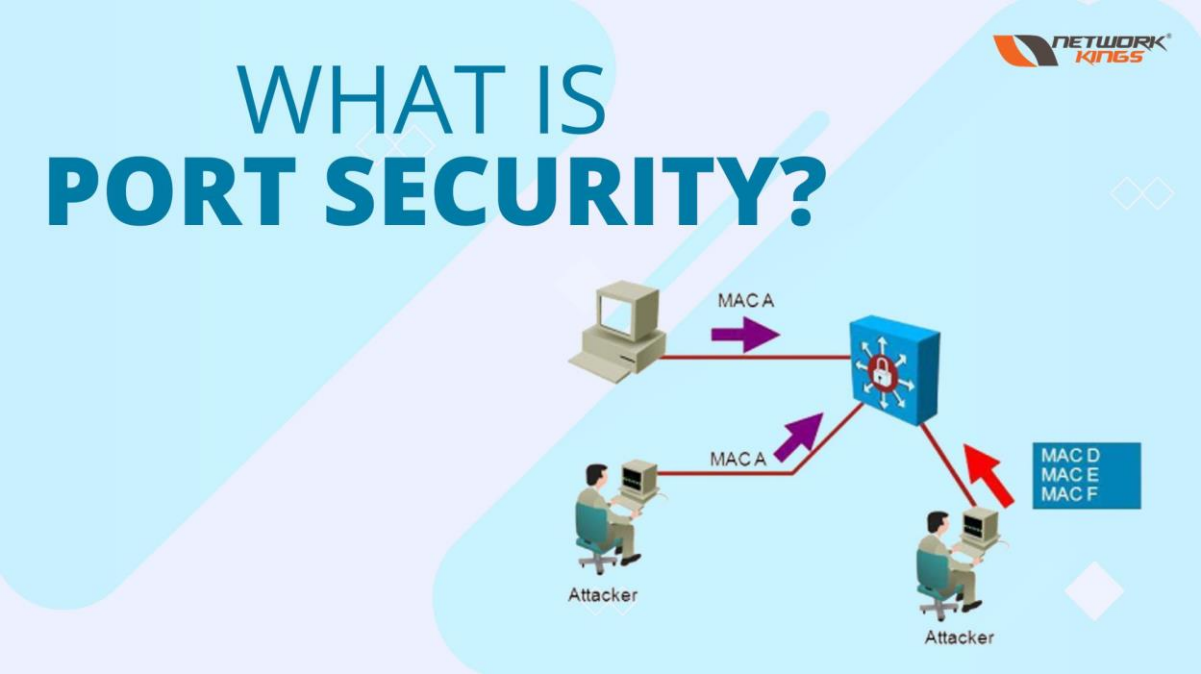
ITEC442 IOT & Cyber Security

Week 5-6 – Port Security

What is Port Security?



Port security is a security measure that is designed to protect ports, harbors, and other marine facilities from security threats such as terrorism, smuggling, and piracy. Port security may involve a variety of measures, including the use of physical barriers, security personnel, and security technology such as surveillance cameras and sensors. The goal of port security is to prevent unauthorized access to port facilities, and to ensure the safety and security of the people and cargo that are present in the port. Port security is a critical component of national security, and is often managed by a combination of government agencies and private security companies.

To configure port security, three steps are required:

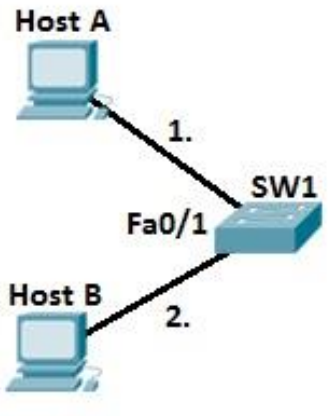
1. define the interface as an access interface by using the *switchport mode access* interface subcommand
2. enable port security by using the *switchport port-security* interface subcommand
3. define which MAC addresses are allowed to send frames through this interface by using the *switchport port-security mac-address MAC_ADDRESS* interface

subcommand or using the *swichport port-security mac-address sticky* interface subcommand to dynamically learn the MAC address of the currently connected host

Two steps are optional:

1. define what action the switch will take when receiving a frame from an unauthorized device by using the *port security violation {protect | restrict | shutdown}* interface subcommand. All three options discard the traffic from the unauthorized device. The restrict and shutdown options send log messages when a violation occurs. Shut down mode also shuts down the port.
2. define the maximum number of MAC addresses that can be used on the port by using the *switchport port-security maximum NUMBER* interface submode command

The following example shows the configuration of port security on a Cisco switch:



First, we need to enable port security and define which MAC addresses are allowed to send frames:

```
SW1(config)#interface fastEthernet0/1

SW1(config-if)#switchport mode access

SW1(config-if)#switchport port-security

SW1(config-if)#switchport port-security mac-address sticky
```

Next, by using the *show port-security interface fa0/1* we can see that the switch has learned the MAC address of host A:

```
SW1#show port-security interface fastEthernet0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown
```

```
Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 000A.4188.D0C3:1

Security Violation Count : 0
```

By default, the maximum number of allowed MAC addresses is one, so if we connect another host to the same port, the security violation will occur:

```
SW1#show interfaces fastEthernet0/1

FastEthernet0/1 is down, line protocol is down (err-disabled)

Hardware is Lance, address is 0001.c79a.4501 (bia 0001.c79a.4501)

BW 100000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255
```

My Reflection:

Port security is a vital component of national security, as ports are often major hubs for the movement of people and goods. The protection of ports and other marine facilities from security threats such as terrorism, smuggling, and piracy is essential to maintaining the flow of international trade and commerce, as well as the safety and security of the people who work in and visit these facilities.

One of the challenges of port security is the need to balance the need for security with the need for accessibility and efficiency. Ports must be able to accommodate the movement of large volumes of people and cargo, while also ensuring that security measures are in place to prevent unauthorized access and detect any security threats. This requires the use of a variety of security technologies and practices, as well as the coordination of efforts between government agencies and private security companies.

Overall, the importance of port security cannot be overstated. By protecting our ports and marine facilities, we are able to maintain the flow of international trade and commerce, and ensure the safety and security of the people and communities that depend on these vital resources.

References:

https://study-ccna.com/port-security/

https://kb.netgear.com/21786/What-is-port-security-and-how-does-it-work-with-my-managed-switch