Systems and Network Analysis Center
Information Assurance Directorat

# NATIONAL SECURITY AGENCY
# Port Security on Cisco Access Switches

## Port Security Basics

Without security protections in place, unauthorized devices could access your network through open and unprotected switch interfaces. The Port Security feature is used to restrict traffic on a switch interface (also called a "switchport" or "port") by identifying and limiting traffic allowed to enter that port based on source Ethernet MAC addresses. Those source MAC addresses that the Port Security feature learns are called "secure addresses."

There are three types of secure addresses:

- **Dynamic:** MAC addresses learned during switch operation and not retained,
- **Static:** MAC addresses added manually into the switch configuration, and
- **Sticky:** MAC addresses learned during switch operation and added automatically into the switch configuration.

In *sticky* mode, when the switch configuration is saved, all learned MAC addresses will be stored within the switch configuration file and remain persistent, even after reboot.

Limits can be set for the maximum number of secure addresses allowed, and individual secure addresses can be specified manually or learned dynamically up to that maximum. If fewer than the maximum number of secure addresses have been specified manually, the remaining will be learned dynamically. If the maximum number of secure addresses is set to one and a single secure address is specified manually only traffic with that source MAC address will be accepted. All other traffic will be dropped.

## Port Security in Action

The Port Security feature tracks the secure addresses for enabled ports. When a port's maximum is reached and traffic containing a new source MAC address is received, a security violation occurs. A violation will also occur after a secure address learned on one port appears on a different secure port.

If a violation should occur, the switch will respond according to one of three modes:

- **Shutdown** (default): immediately puts the port into the "error-disabled" state, drops all traffic, and sends a SNMP trap notification;
- **Protect:** silently drops traffic that is in violation until the number of secure addresses drop below the maximum value; and
- **Restrict:** behaves like *protect* but also increments the security violation counter for each violation and sends a SNMP trap notification.

Note: Users should be aware that while *shutdown* mode offers the highest level of protection, evaluation efforts have shown that all of these modes may not function as documented. When a Port Security violation occurs using the *protect* or *restrict* modes, approximately 40,000 frames may traverse the port and it may enter the "error-disabled" state. Frames may also traverse the port when using the default *shutdown* mode, but the number is drastically reduced to approximately 1,000.

## Replacing the Old with the New

An age limit can be set for all secure addresses on a port. This feature can be used to remove inactive secure addresses. There are two types of aging:

- **Absolute:** secure addresses are removed after the specified timeframe and
- **Inactivity:** secure addresses are removed when inactive for the specified timeframe.

The age limit can only be applied to *static* and *dynamic* secure addresses.

## The Virtual LAN (VLAN) Dimension

The Port Security feature is enabled on a per port basis and is also VLAN aware. Maximum limits, secure addresses, and violation responses can be configured to be VLAN specific. See the back for configuration examples, including VLAN based Port Security with an IP Phone.

## Configuration Examples (from a 3750E switch running IOS 12.2(37)SE)

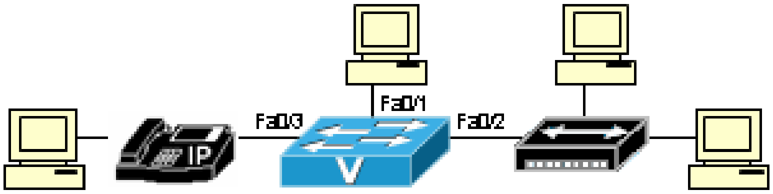

Figure 1. Example Network

**Example of a Static Secure MAC Address:**

```
   Switch#configure terminal
   Switch(config)#interface fastEthernet 0/1
   Switch(config-if)#switchport port-security
   Switch(config-if)#switchport port-security mac-address 0000.0102.0304
   Switch(config-if)#end
```

**Example of Dynamic Secure MAC Addresses:**

```
   Switch#configure terminal
   Switch(config)#interface fastEthernet 0/2
   Switch(config-if)#switchport port-security
   Switch(config-if)#switchport port-security maximum 2
   Switch(config-if)#switchport port-security aging type inactivity
   Switch(config-if)#switchport port-security aging time 5
   Switch(config-if)#end
```

**Example of Static Secure MAC Addresses with VLANs:**

```
   Switch#configure terminal
   Switch(config)#interface fastEthernet 0/3
   Switch(config-if)#switchport mode access
   Switch(config-if)#switchport access vlan 10
   Switch(config-if)#switchport voice vlan 101
   Switch(config-if)#switchport port-security
   Switch(config-if)#switchport port-security maximum 3
   Switch(config-if)#switchport port-security maximum 2 vlan access
   Switch(config-if)#switchport port-security maximum 1 vlan voice
   Switch(config-if)#switchport port-security violation shutdown vlan
   Switch(config-if)#switchport port-security mac-address 0000.0203.0405 vlan access
   Switch(config-if)#switchport port-security mac-address 0000.0304.0506 vlan voice
   Switch(config-if)#switchport port-security mac-address 0000.0304.0506 vlan access
   Switch(config-if)#end
```

**Useful Port Security Related IOS Commands:**

| | |
|---|---|
| `Switch#show port-security` | (shows MAC count and violation info) |
| `Switch#show port-security address` | (shows learned or static MAC addresses & aging info) |
| `Switch#show mac address-table` | (shows all MAC addresses seen on the switch) |
| `Switch#show mac address-table secure` | (shows all secure MAC addresses seen on the switch) |
| `Switch#show interfaces status` | (shows the status of all ports) |
| `Switch#show interfaces status err-disable` | (shows any ports in error-disable status) |
| Switch#clear errdisable interface *port* VLAN | (clears a port's VLAN from error-disable status) |
| `Switch(config)#errdisable recovery cause psecure-violation` | (clears all ports in error-disable status) |