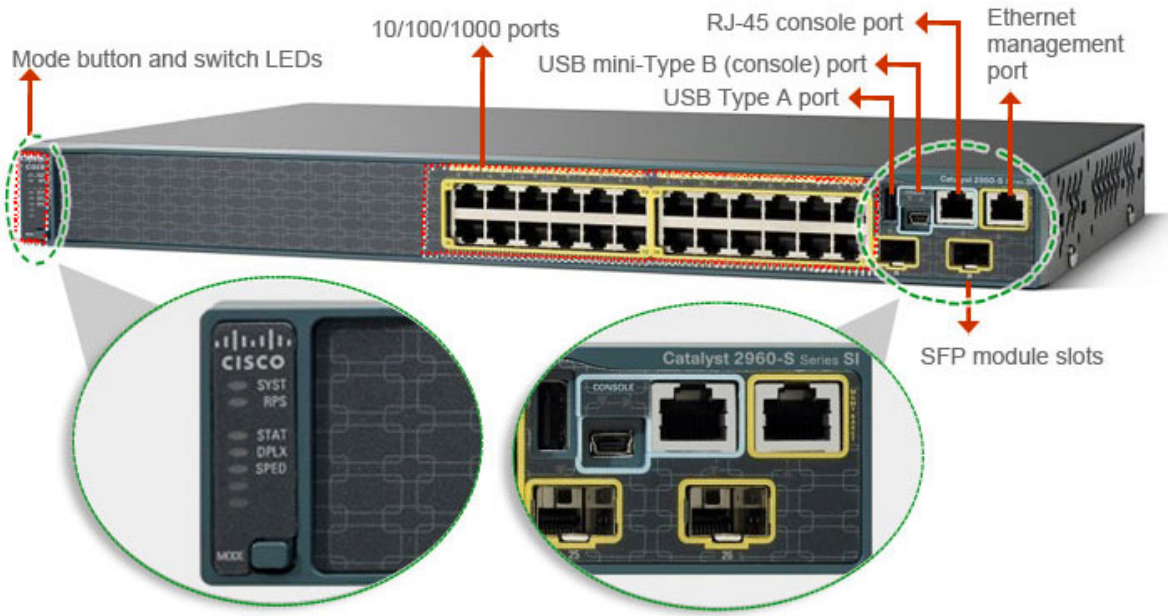
Switch Security

A quick overview and commands

Port-security

- Under normal circumstances, there are no restrictions on the devices that can be attached to a switch port.
- However, with switch port security enabled, the devices that can connect to a switch through the port are restricted:
  - Port security uses the MAC address to identify allowed and denied devices.
  - By default, port security allows only a single device to connect through a switch port. You can, however, modify the maximum number of allowed devices.



Port-security (2)

- MAC addresses are stored in RAM in the CAM table and are identified with the port and by a MAC address type. Port security uses the following three MAC address types:

Type	Description
SecureConfigured	A SecureConfigured address is a MAC address that has been manually identified as an allowed address. The address is configured in interface mode and stored in the running-config file.
SecureDynamic	A SecureDynamic address is a MAC address that has been dynamically learned and allowed by the switch: ○ When a device connects to the switch port, its MAC address is identified. ○ If the maximum number of allowed devices has not been reached, its MAC address is added to the table, and use of the port is allowed. SecureDynamic addresses are only saved in the MAC address table in RAM and are not added to the configuration file.
SecureSticky	A SecureSticky address is a MAC address that is manually configured or dynamically learned and saved. With sticky learning enabled: ○ When a device connects to the switch port, its MAC address is identified. ○ If the maximum number of allowed devices has not been reached, its MAC address is added to the table, and use of the port is allowed. ○ The MAC address is automatically entered into the running-config file as a sticky address. Be aware of the following: ○ You can manually configure an address and identify it as a sticky address. ○ If you disable the sticky feature, all sticky addresses are converted to SecureDynamic addresses. ○ If you enable the sticky feature, all SecureDynamic addresses are converted to SecureSticky addresses, even if they have been learned before the sticky feature was enabled.

Port-security (3)

- A *port violation* occurs when the maximum number of MAC addresses has been seen on the port, and an unknown MAC address is then seen.
- You can configure the switch to take one of the following actions when a violation occurs:
  - Shut down the port; this is the default setting.
  - Drop all frames from unauthorized MAC addresses.
  - Drop all frames and generate an SMNP trap.
    - **SNMP stands** for Simple Network Management Protocol and consists of three key components: managed devices, agents, and network-management systems (NMSs). A managed device is a node that has an **SNMP** agent and resides on a managed network.
    - **SNMP traps** are alert messages sent from a remote **SNMP**-enabled device to a central collector, the "**SNMP** manager". A **trap** might tell you that a device is overheating, for example. (As you'll recall, **SNMP** is one possible protocol that devices can use to communicate.)

Be aware of the following when using port security

- You can only enable port security on an access port.
- Port security does not protect against MAC address spoofing (where an attacker changes the MAC address to match the MAC address of an allowed device).
- If you do not manually configure allowed MAC addresses for a port, the switch will allow the first MAC addresses it detects to connect, up to the maximum number.
- Once the maximum number of MAC addresses for a port has been reached, either through manual, dynamic, or sticky learning, no more MAC addresses will be allowed, and a violation will occur.
- Save the running-config file to the startup-config to make manually-configured and sticky addresses available when the system restarts. Otherwise, the switch will need to relearn sticky addresses.
- When using Voice-over-IP phones and workstations on a single port, increase the maximum allowed number above 1, allowing at least one MAC address for the phone and one for the workstation. The recommended value is 3.

Configuration

Each switch port has its own port security settings. To configure port security, take the following general actions:

1. Explicitly configure the port as an *access* port.
2. Enable switch port security.
3. Optional: Configure MAC addresses and other settings. When you enable port security, the following default settings are used:
   - A maximum of 1 device
   - Violation mode is shutdown
   - Dynamic learning is enabled, but sticky learning is disabled

Commands

- The following commands configure Fast Ethernet port 0/15 to accept the first MAC address it receives as the allowed MAC address for the port:

```
switch(config)#interface fast 0/15
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address sticky
switch(config-if)#switchport port-security violation restrict
```

Command	Action
`switch(config-if)#switchport mode access`	Identifies the port as an access port. You can only configure port security after explicitly making the port an access port.
`switch(config-if)#switchport port-security`	Enables port security. You can enter port security commands for an interface without port security being enabled. However, port security will not be enforced (enabled) if this entry is missing.
`switch(config-if)#switchport port-security maximum [1-8320]`	Configures the maximum number of MAC addresses that can be allowed for a port. The default allows only a single MAC address per port. Use the no form of the command to reset the value to its default.
`switch(config-if)#switchport port-security mac-address sticky`	Enables sticky learning of MAC addresses. Without this command, addresses are dynamically learned but not recorded. With this command, learned addresses are added to the running-config file. Using the no form of the command disables sticky learning, removes any sticky entries from the configuration file, and converts the sticky addresses to dynamic addresses.

Command	Action
`switch(config-if)#switchport port-security mac-address [h.h.h]`	Identifies an allowed MAC address (h.h.h is a hexadecimal number).
`switch(config-if)#switchport port-security mac-address sticky [h.h.h]`	Identifies an allowed MAC address, making it a sticky address.
`switch(config-if)#switchport port-security violation [action]`	Identifies the action the switch will take when an unauthorized device attempts to use the port. The following are action keywords: • protect drops the frames from the unauthorized device • restrict does the same as protect and also generates an SNMP trap • shutdown disables the port
`switch#errdisable recovery cause psecure-violation`	Recovers from a port security violation (enables disabled ports). You can also enable disabled ports by using the shutdown/no shutdown commands for the interface.