

Network Professionals Bootcamp

LEC-080: SWITCHPORT SECURITY

Outline

- Switch Port Security

Switch Port Security

- Normally, there are no restrictions on the device attached to the switch ports.
- We can connect any device to any switch port any time.
- With switch port security, we allow specific devices to use a given port using the MAC address of the device.
- Any device, not specifically allowed will not be able to send frames through that port.
- The port must be access port when we want to apply switch port security on the port.

Switch Port Security

Command	Function
<code>switch(config-if)#switchport mode access</code>	Identifies the port as an access port.
<code>switch(config-if)#switchport port-security</code>	Enables port security.
<code>switch(config-if)#switchport port-security mac-address h.h.h</code>	Identifies the allowed MAC address (<u>h.h.h</u> is a hexadecimal number).
<code>switch(config-if)#switchport port-security maximum number</code>	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 this command to increase the number allowed.
<code>switch(config-if)#switchport port-security mac-address sticky</code>	Configures the switch to dynamically identify the allowed MAC address. The address in the first frame received by the switch port is the allowed MAC address for the port. Note: The Catalyst switch can sticky learn a maximum of 132 MAC addresses.
<code>switch(config-if)#switchport port-security violation action</code>	Identifies the action the switch will take when an unauthorized device attempts to use the port. Action keywords are: • protect drops the frames from the unauthorized device • restrict does the same as protect and also generates an SNMP trap • shutdown disables the port
<code>switch#show port-security interface interfacetype and number</code>	Shows port security information for the specified port. 4

Configuration

- SW(config-if)#switchport mode access
- SW(config-if)#switchport port-security
- SW(config-if)#switchport port-security maximum 1
- SW(config-if)#switchport port-security mac-address 0000.12cb.f902
- SW(config-if)#switchport port-security mac-address sticky
- SW(config-if)#switchport port-security violation shutdown
- SW#show port-security int eth 0/0

Default Switch Configuration

- All ports are up. (Not shutdown)
- All ports will perform automatic trunk negotiation
- Spanning-tree is enabled.
- All ports are member of VLAN 1
- VTP mode is server.
- VLANs 1, 1002-1005 are built-in

REFERENCES

THANK YOU