Lecture 3b - Switch Configuration

Type	Lecture
Materials	Empty
Reviewed	☑

1. Securing Ports

1.1: Disabling Ports

- Switch ports are enabled by default
- Usually patched to outlets in semi-public spaces
- Any user can plug in a computer and get access to that VLAN

⇒ **Best Practice:**

- Switch ports that are connected to semi-public spaces that are not in use should be disabled

```
int f0/6
shutdown
```

1.2: Blackhole VLANs

- Even if a **port** is **disabled**, it may be **enabled** accidentally by a **network operator**
- Then provides access to nominated VLAN
- Default setting, **access** is granted to the switch **management VLAN**

💡 - In Cisco switches, all ports belong to VLAN 1 by default and the default management VLAN is VLAN 1
- The management VLAN carries critical information (i.e: layer 2 control traffic) and it should not be accessed by the attackers.

⇒ **Best Practice:**

- Create a VLAN that is not used for real network traffic
- Assign unused switch ports to be access ports in that VLAN (and shutdown)

```
int f0/6
shutdown
switchport mode access
switchport access vlan 200
```

1.3: Forcing Switchport Mode

- The default port mode is DTP **dynamic auto**

💡 - Trunk port contains all VLAN configurations.

- An attacker can **configure** a PC to talk DTP to the switch
  - Get access to a **trunk** link – **Switch spoofing**
  - Access all traffic on all VLANS

2. Switch Port Security

2.1: Concepts

- Limits the number of valid MAC addresses allowed on a port
- Only traffic from MAC addresses of legitimate devices is allowed
- **Configuring secure MAC addresses:**
  - **Static** – Specific MAC address(es) explicitly allowed via configuration command
  - **Dynamic** – Any connected MAC address(es) allowed up to limit **(Default setting)**
  - **Sticky** – Connected MAC address(es) auto-configure as static up to limit
- **Illegal traffic** causes a **security violation** occurs
- **Possible actions when a violation is detected:**
  - **Protect** – Invalid frames are **dropped**, valid frames are **sent**
  - **Restrict** – As per protect but **violation counter** is **incremented**
  - **Shutdown** – Port goes to the **error-disabled** state ⇒ Default

2.2: Default Port Security Settings

💡 ***Note:*** All port security settings will not be enabled if we haven't run the `switchport port-security` command

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

2.3: Ports In Error Disabled State

- A port in error-disabled state is effectively shutdown
  - Status communicated through console messages
- To re-enable an error-disabled port:

```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```