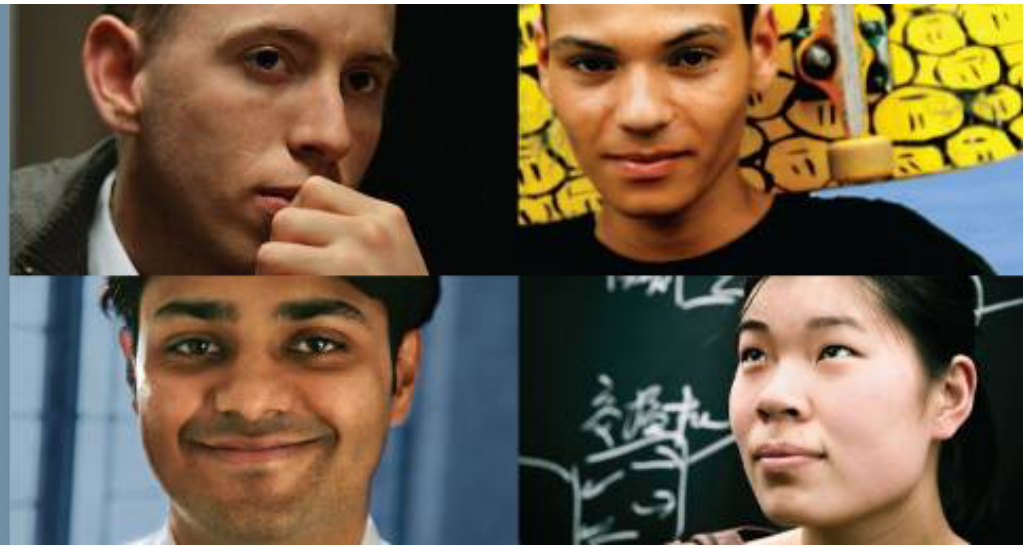
TNE10006/TNE60006: Networks and Switching



Switch Configuration – Best Practices

Cisco | Networking Academy®
Mind Wide Open™

Outline

- Disabling Ports
- Blackhole VLANs
- Forcing Switchport Mode
- Switchport Security

SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

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
```

Blackhole VLANs

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

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
```

SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Forcing Switchport Mode

- Default port mode is DTP dynamic auto
- 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

Best Practice

- Trunk ports should be forced to be trunk

```
switchport mode trunk
```

- Access ports should be forced access

```
switchport mode access
```

- Unused ports should be forced access

```
switchport mode access
```

Switch Port Security

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** – Programmed MAC addresses
  - **Dynamic** – Current MAC addresses programmed
  - **Sticky** – Switch auto-adds MAC addresses 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 **error-disabled** state

SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Default Port Security Settings

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.

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
```

SWIN BUR NE — CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Summary

In this lecture, we covered:

- Disabling Ports
- Blackhole VLANs
- Forcing Switchport Mode
- Switchport Security