INOS202 Case Study

Instructions

Port Security

Port Security has not been configured on any of the switches.

Sw1 and Sw2 require the following:

Fa0/1-Fa0/15 - use port security to limit the number of MAC addresses to 1

- secure the port so that the MAC addresses of devices are dynamically learned and added to the running configuration

Sw3 and Sw4 require the following:

Fa0/1-Fa0/5 - use port security to limit the number of MAC addresses to 2

- set the violation mode so that the Fast Ethernet ports are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped

On *all* switches:

- Enable PortFast on all the access ports that are in use

ACLs

Configure ACLs to meet the following requirements:

- All users from North Campus should not be allowed to access Missionvale and Bird Street Campus.
- All users from South Campus should be allowed to FTP to the MVale Server (username: cisco; password: cisco), but should not be able to ping the server.
- Internet users should not be able to access the Enterprise Web Server on South Campus.
- All other traffic should be allowed.