Layer 2 Network Design Lab

Part 3: Switch Security

Part 3: Switch Security

Lab Objectives.

Set up two additional Switch Virtual Interfaces (SVI) on the distribution switches, use the following parameters.

BBX1		**BBX2**	
Interface Vlan 64	10.X.64.11/24	Interface Vlan 64	10.X.64.12/24
Interface Vlan 65	10.X.65.11/24	Interface Vlan 65	10.X.65.12/24

Make sure you can ping these addresses from all the switches before you move onto the next task.

Configure all access switches with the following features.

1. Port security should be configured on all access switch ports which are not connected to other switches. Limit the maximum number of mac addresses on a port to 1.

   ```
   Switch(config-if)# switchport mode access
   Switch(config-if)# switchport port-security
   Switch(config-if)# switchport port-security maximum 1
   ```
   Switchport port-security violation restrict
2. Mac addresses should be dynamically learnt and any address violation should be filtered and a trap message sent.
3. Configure access port on VLAN 64 and VLAN 65 on switch SWX1 AND SWX2 respectively
4. Telnet into BBX1 and BBX2 from the access port configured with Vlans 64 and 65 on SWX1 and SWX2 respectively
5. Create a VACL on the distribution switches to prevent any client in Vlans 64 or 65 from performing Telnet sessions. Test the VACL
   IP access-list extended TELNET_HOST 10
   Permit IP 10.0.0.0 0.255.255.255.255 any any eq telnet

   Vlan access-map NO_TELNET 10
   Match IP address TELNET_HOST
   Action drop
   Vlan access-map NO_TELNET 20

   Vlan filter NO_TELNET vlan-list 64-5

6. Create a VACL on the distribution switches to allow only client 10.X.64.30 to perform Telnet sessions. Test the VACL

COMMANDS

Show access-lists

Show vlan access-map

.