**Configuration guide on Secure Network System Design**

Switch on floor-1

Basic Settings: Configure fundamental device settings, including hostnames and console passwords,enable passwords and banner messages,password encryption and disable IP domain lookup.

Basic settings to all devices + SSH + standard ACL for SSH

Only allow Management network to remotely access the devices.

We are going to create an Access Control List rule that only allows management network to manage the networking devices, all other networks will be denied.

We will normally configure one device step by step all right and then we will write commands on notepad and copy paste to all other remaining devices.

We will start with Sales & Marketing switch and then we will come to CLI

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

To configure SSH there are some basic settings that we have to configure

1. So first we need to configure username and password

A computer screen shot of a computer

AI-generated content may be incorrect.

Lets enable IP SSH version 2

We have configured SSH but we have not appended SSH on the vty interface

So vty interface it’s that interface that the remote user uses to remotely access the device so you have to append the SSH setting on that interface, so just say

Line vty 0 15

A screenshot of a computer

AI-generated content may be incorrect.

We created the access control rule to only allow the management network

A number on a white background

AI-generated content may be incorrect.

We need the append the rule on the VTY interface

A computer screen shot of a computer screen

AI-generated content may be incorrect.

We are done with the basic configuration on the switch

Now lets write commands on the notepad and copy paste to all other remaining switches,

We are not going to touch firewall, we have routers actually, but we don’t need to configure basic settings

So I will just configure multilayer switches and this access layer switches

Configuration of multilayer switches

en

conf t

hostname HL-SW

line console 0

password cisco

login

logging synchronous

exec-timeout 3 0

exit

enable password cisco

banner motd &NO UNAUTHORISED ACCESS!!!&

no ip domain-lookup

service password-encryption

**For SSH configuration we need to configure username and password**

Settings

username cisco password cisco

ip domain-name cisco.com

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

Now put the SSH configuration on the VTY interface

line vty 0 15

login local

transport input ssh

exit

Whenever you want to remotely access the device you have to use SSH and you have to use the local database which are username and password

**Configure Access Control List for SSH**

**Because we want the management network to remotely manage these devices**

access-list 1 permit 192.168.10.0 0.0.0.255

access-list 1 deny any

**Now lets append this rule on this interface**

line vty 0 15

access-class 1 in

exit

do wr

We are just going to modify hostname of the switch everything will remain the same

A screenshot of a computer

AI-generated content may be incorrect.

**Multilayer Switches**

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

Done the basic settings for the Core switch-1

A screenshot of a computer program

AI-generated content may be incorrect.

Done the basic settings for the Core Switch -2

A screenshot of a computer program

AI-generated content may be incorrect.

VLAN assignment plus all access and trunk ports on l2 and l3 switches

Whenever I start with the access layer switches, whenever I am connecting the device, I always ensure that the first two ports fa1 and fa2 connects to them such that they become the trunk.

Whenever we are going to configure trunk the first two ports should be trunks.

We have several VLANs, 1. Management VLAN, LAN VLAN, WLAN VLAN, VOIP VLAN, BlackHole VLAN. Any unused port will be put into Black Hole and they should be turned off, such that some one cannot connect to them

A computer screen shot of a diagram

AI-generated content may be incorrect.

For fa0/1 and fa0/2

A screenshot of a computer program

AI-generated content may be incorrect.

Now lets create VLAN after specifying that these are trunks

A screenshot of a computer

AI-generated content may be incorrect.

Any port that connects to access point will come under



A screenshot of a computer

AI-generated content may be incorrect.

Any port that connects to IP Phone will come under this



As for now we can send any port on these switches, the Management network, We are only going to assign a port in ICT department, a management network but not any other department

So as we know the computers and printers will be under LAN VLAN -20

Int fa0/3-4----🡪 printer and laptop

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.