Hospital Network

Configuration and Explanation

1. General Setup and Security Configuration

```
license boot module c2900 technology-package securityk9
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SSS
MER-SW(config)#enable password cisco
MER-SW(config)#no ip domain lookup
MER-SW(config)#banner motd #No Unathorised Acess!!!#
MER-SW(config)#line console 0
MER-SW(config-line)#password cisco
MER-SW(config-line)#login
MER-SW(config-line)#exit
MER-SW(config)#service password-encryption
```

This block performs the initial setup of the switch:

- **Enable Mode: Enters privileged mode (Switch>en).**
- **Hostname: Sets the hostname of the switch to SSS.**
- **Security:**
  - **The enable password is set to "cisco" for privileged access.**
  - **No IP domain lookup disables DNS lookups to speed up mistyped commands.**
  - **A message of the day (MOTD) banner warns unauthorized users.**
  - **Line console 0 password is set and login is required.**
  - **Password encryption ensures that plaintext passwords are hidden.**

2. SSH Configuration

```
ip domain name cisco.net

username admin password cisco

crypto key generate rsa

1024

line vty 0 15

login local

transport input ssh

exit

do wr
```

Here, SSH is configured for secure remote access:

- **Domain name is set to cisco.net.**
- **User "admin" with password "cisco" is created for login authentication.**
- **RSA key generation enables SSH.**
- **VTY lines (0 to 15) are configured for local login with SSH as the only allowed input.**
- **do wr saves the configuration.**

3. VLAN Configuration and Trunking

```
vlan 70

name SSS

int range fa0/1-2

switchport mode trunk

int range fa0/3-24

switchport mode access

switchport access vlan 70
```

This section creates VLANs and assigns ports:

- **VLAN 70 is created and named "SSS".**
- **Trunk ports (FastEthernet 0/1-2) are configured to allow multiple VLANs.**
- **Access ports (FastEthernet 0/3-24) are assigned to VLAN 70 to isolate traffic.**

4. Additional VLAN Configuration

```
VLAN 80

VLAN 90

VLAN 100

VLAN 110

VLAN 120

VLAN 130

int range gig1/0/2-7

switchport mode trunk

do wr
```

Here, VLANs 80, 90, 100, 110, 120, and 130 are created. GigabitEthernet ports (1/0/2-7) are configured as trunk ports, and the configuration is saved.

5. OSPF and Static Routing

```
ip routing

router ospf 10

network 195.136.17.4 0.0.0.3 area 0

network 195.136.17.12 0.0.0.3 area 0

do wr
```

OSPF Routing: OSPF process ID 10 is initiated. The network statements indicate which networks OSPF will advertise in area 0.

Static Routing: Sets the default routes using ip route.

6. IP Routing and OSPF Networks

```
ip routing
router ospf 10
network 195.168.102.80 0.0.0.3 area 0
network 195.168.102.84 0.0.0.3 area 0
network 195.168.102.88 0.0.0.3 area 0
network 195.168.102.64 0.0.0.3 area 0
network 195.136.17.4 0.0.0.3 area 0
network 195.136.17.0 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 195.136.17.2
ip route 0.0.0.0 0.0.0.0 195.136.17.6 70
do wr
```

Multiple networks are added to the OSPF process, covering different subnets and areas.

Two default static routes are configured.

7. VLAN IP Configuration

```
int vlan 80
ip address 192.168.101.129 255.255.255.224
ip helper-address 192.168.102.67

int vlan 90
ip address 192.168.101.161 255.255.255.224
ip helper-address 192.168.102.67

int vlan 100
ip address 192.168.101.193 255.255.255.224
ip helper-address 192.168.102.67
```

Each VLAN is assigned an IP address and DHCP relay (helper address), which forwards DHCP requests to the specified server at 192.168.102.67.

8. Route Aggregation

```
HQ ROUTE AGGREGATION
192.168.100.0/26
192.168.100.64/26
192.168.100.128/26
192.168.100.192/26
--- SUMMARISED 192.168.100.0/25
```

This section summarizes multiple subnets to a single larger network, reducing the number of routes advertised by OSPF and making the network more efficient.

9. VPN Configuration

```
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
crypto isakmp key vpnpa55 address 192.168.102.89
crypto ipse transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
set peer 192.168.102.89
set transform-set VPN-SET
match address 110
```

This block configures IPsec VPN between the hospital and HQ. ISAKMP policy uses AES 256 encryption and pre-shared keys. The VPN is secured with the VPN-SET transform set.