Please build LAN with three cisco 2960 and one cisco 4331 1) Switches must be named S1, S2, S3. S1, S2, S3 must be interconnected via Fast Ethernet ports 2) Router must be named R1. It is must be adjusted as router on a stick. 3) R1 must be connected to S1 via G0/0/0 3) There must be office network with five computers with IP 192.168.1.0 255.255.255.0 and DHCP. Computers from office network must be connected to S1. 4) There must be engineering network with two laptops with static IP 192.168.2.0 255.255.255.0. Laptops from engineering network must be connected to S2. 5) There must be security network with three computers IP 192.168.3.0 255.255.255.0. Computers from security network must be connected to S3. 6) There must be used VLAN, OSPF, STP for S1 and S2 and S3, SSH, Telnet, ACL. 7) Office network must be isolated from engineering network and security network. 8) Security network must be isolated from office network and engineering network . 9) laptops from engineering network must get access to office network and security network.

Please build LAN with three cisco 2960 and one cisco 4331 1) Switches must be named S1, S2, S3. S1, S2, S3 must be interconnected via Fast Ethernet ports 2) Router must be named R1. It is must be adjusted as router on a stick. 3) R1 must be connected to S1 via Gigabit port 3) There must be office network with five computers with IP 192.168.1.0 255.255.255.0 and DHCP. Computers from office network must be connected to S1. 4) There must be engineering network with two laptops with static IP 192.168.2.0 255.255.255.0. Laptops from engineering network must be connected to S2. 5) There must be security network with three computers IP 192.168.3.0 255.255.255.0. Computers from security network must be connected to S3. 6) There must be used VLAN, OSPF, STP for S1 and S2 and S3, SSH, Telnet, ACL. 7) Office network must be isolated from engineering network and security network. 8) Security network must be isolated from office network and engineering network . 9) laptops from engineering network must get access to office network and security network.

2 / 2

To build the LAN as per your requirements, we need to configure VLANs, OSPF, STP, SSH, Telnet, ACLs, and DHCP. Below is a step-by-step guide to configure the network using Cisco 2960 switches (S1, S2, S3) and a Cisco 4331 router (R1).

**Topology Overview**

1. **Switches:**
   * S1, S2, and S3 are interconnected via Fast Ethernet ports.
   * S1 is connected to R1 via a Gigabit Ethernet port.
   * S1 hosts the office network (VLAN 10).
   * S2 hosts the engineering network (VLAN 20).
   * S3 hosts the security network (VLAN 30).
2. **Router:**
   * R1 is configured as a router-on-a-stick to route traffic between VLANs.
   * R1 provides DHCP for the office network (VLAN 10).
3. **Networks:**
   * Office Network: VLAN 10, 192.168.1.0/24, DHCP-enabled.
   * Engineering Network: VLAN 20, 192.168.2.0/24, static IPs.
   * Security Network: VLAN 30, 192.168.3.0/24, static IPs.
4. **Isolation:**
   * Office network (VLAN 10) is isolated from engineering (VLAN 20) and security (VLAN 30) networks using ACLs.
   * Security network (VLAN 30) is isolated from office (VLAN 10) and engineering (VLAN 20) networks using ACLs.
   * Engineering network (VLAN 20) can access office (VLAN 10) and security (VLAN 30) networks.

**Configuration Steps**

**1. Configure Switches (S1, S2, S3)**

**Step 1: Basic Switch Configuration**

bash

Copy

# Configure hostnames

Switch> enable

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

# Repeat for S2 and S3

**Step 2: Configure VLANs**

bash

Copy

# Create VLANs on S1, S2, and S3

S1(config)# vlan 10

S1(config-vlan)# name Office

S1(config-vlan)# exit

S1(config)# vlan 20

S1(config-vlan)# name Engineering

S1(config-vlan)# exit

S1(config)# vlan 30

S1(config-vlan)# name Security

S1(config-vlan)# exit

# Repeat VLAN creation on S2 and S3

**Step 3: Assign VLANs to Ports**

bash

Copy

# On S1 (Office Network)

S1(config)# interface range fa0/1 - 5

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport access vlan 10

S1(config-if-range)# exit

# On S2 (Engineering Network)

S2(config)# interface range fa0/1 - 2

S2(config-if-range)# switchport mode access

S2(config-if-range)# switchport access vlan 20

S2(config-if-range)# exit

# On S3 (Security Network)

S3(config)# interface range fa0/1 - 3

S3(config-if-range)# switchport mode access

S3(config-if-range)# switchport access vlan 30

S3(config-if-range)# exit

**Step 4: Configure Trunk Links**

bash

Copy

# On S1 (Trunk to R1 and other switches)

S1(config)# interface gig0/1

S1(config-if)# switchport mode trunk

S1(config-if)# exit

S1(config)# interface range fa0/6 - 7

S1(config-if-range)# switchport mode trunk

S1(config-if-range)# exit

# On S2 (Trunk to other switches)

S2(config)# interface range fa0/6 - 7

S2(config-if-range)# switchport mode trunk

S2(config-if-range)# exit

# On S3 (Trunk to other switches)

S3(config)# interface range fa0/6 - 7

S3(config-if-range)# switchport mode trunk

S3(config-if-range)# exit

**Step 5: Configure STP**

bash

Copy

# Enable Rapid PVST+ on all switches

S1(config)# spanning-tree mode rapid-pvst

S2(config)# spanning-tree mode rapid-pvst

S3(config)# spanning-tree mode rapid-pvst

# Set S1 as the root bridge for VLANs 10, 20, and 30

S1(config)# spanning-tree vlan 10 root primary

S1(config)# spanning-tree vlan 20 root primary

S1(config)# spanning-tree vlan 30 root primary

**Step 6: Configure SSH and Telnet**

bash

Copy

# On S1, S2, and S3

S1(config)# username admin privilege 15 secret cisco123

S1(config)# line vty 0 4

S1(config-line)# login local

S1(config-line)# transport input ssh telnet

S1(config-line)# exit

S1(config)# ip domain-name example.com

S1(config)# crypto key generate rsa

S1(config)# ip ssh version 2

**2. Configure Router (R1)**

**Step 1: Basic Router Configuration**

bash

Copy

Router> enable

Router# configure terminal

Router(config)# hostname R1

R1(config)# exit

**Step 2: Configure Subinterfaces for VLANs**

bash

Copy

# Configure subinterfaces for VLANs

R1(config)# interface gig0/0.10

R1(config-subif)# encapsulation dot1Q 10

R1(config-subif)# ip address 192.168.1.1 255.255.255.0

R1(config-subif)# exit

R1(config)# interface gig0/0.20

R1(config-subif)# encapsulation dot1Q 20

R1(config-subif)# ip address 192.168.2.1 255.255.255.0

R1(config-subif)# exit

R1(config)# interface gig0/0.30

R1(config-subif)# encapsulation dot1Q 30

R1(config-subif)# ip address 192.168.3.1 255.255.255.0

R1(config-subif)# exit

**Step 3: Configure DHCP for Office Network**

bash

Copy

R1(config)# ip dhcp pool Office

R1(dhcp-config)# network 192.168.1.0 255.255.255.0

R1(dhcp-config)# default-router 192.168.1.1

R1(dhcp-config)# dns-server 8.8.8.8

R1(dhcp-config)# exit

**Step 4: Configure OSPF**

bash

Copy

R1(config)# router ospf 1

R1(config-router)# network 192.168.1.0 0.0.0.255 area 0

R1(config-router)# network 192.168.2.0 0.0.0.255 area 0

R1(config-router)# network 192.168.3.0 0.0.0.255 area 0

R1(config-router)# exit

**Step 5: Configure ACLs**

bash

Copy

# Block Office (VLAN 10) from accessing Engineering (VLAN 20) and Security (VLAN 30)

R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

R1(config)# access-list 100 permit ip any any

# Block Security (VLAN 30) from accessing Office (VLAN 10) and Engineering (VLAN 20)

R1(config)# access-list 101 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

R1(config)# access-list 101 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255

R1(config)# access-list 101 permit ip any any

# Apply ACLs to subinterfaces

R1(config)# interface gig0/0.10

R1(config-subif)# ip access-group 100 in

R1(config-subif)# exit

R1(config)# interface gig0/0.30

R1(config-subif)# ip access-group 101 in

R1(config-subif)# exit

**Verification**

1. Verify VLANs:

bash

Copy

show vlan brief

1. Verify STP:

bash

Copy

show spanning-tree

1. Verify OSPF:

bash

Copy

show ip ospf neighbor

1. Verify DHCP:

bash

Copy

show ip dhcp binding

1. Verify ACLs:

bash

Copy

show access-lists

This configuration meets all your requirements. Let me know if you need further assistance!