17.8.2 Packet Tracer – Skills Integration Challenge (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0	**192.168.0.1 / 25**	N/A
		2001:db8:acad::1/64	
		fe80::1	
	G0/1	**192.168.0.129 /26**	N/A
		2001:db8:acad:1::1/64	
		fe80::1	
	G0/2	**192.168.0.193 /27**	N/A
		2001:db8:acad:2::1/64	
		fe80::1	
	S0/0/1	172.16.1.2 /30	N/A
		2001:db8:2::1/64	
		fe80::1	
Central	S0/0/0	209.165.200.226 /30	N/A
		2001:db8:1::1/64	
		fe80::2	
	S0/0/1	172.16.1.1 /30	N/A
		2001:db8:2::2/64	
		fe80::2	
S1	VLAN 1	**192.168.0.2 /25**	**192.168.0.1**
S2	VLAN 1	**192.168.0.130 /26**	**192.168.0.129**
S3	VLAN 1	**192.168.0.194 /27**	**192.168.0.193**
Staff	NIC	**192.168.0.3 /25**	**192.168.0.1**
		2001:db8:acad::2/64	fe80::1
		fe80::2	
Sales	NIC	**192.168.0.131 /26**	**192.168.0.129**
		2001:db8:acad:1::2/64	fe80::1
		fe80::2	
IT	NIC	**192.168.0.195 /27**	**192.168.0.193**

Device	Interface	IP Address / Prefix	Default Gateway
		2001:db8:acad:2::2/64	fe80::1
		fe80::2	
Web	NIC	64.100.0.3 /29	64.100.0.1
		2001:db8:cafe::3/64	fe80::1
		fe80::2	

Background / Scenario

The router Central, ISP cluster, and the Web server are completely configured. You must create a new IPv4 addressing scheme that will accommodate 4 subnets using the 192.168.0.0/24 network. The IT department requires 25 hosts. The Sales department needs 50 hosts. The subnet for the rest of the staff requires 100 hosts. A Guest subnet will be added in the future to accommodate 25 hosts. You must also finish the basic security settings and interface configurations on R1. Then, you will configure the SVI interface and basic security settings on switches S1, S2, and S3.

Instructions

IPv4 Addressing

- Use 192.168.0.0/24 to create subnets that meet the host requirements.
  - Staff: 100 hosts
  - Sales: 50 hosts
  - IT: 25 hosts
  - Guest network to be added later: 25 hosts
- Document the IPv4 addresses that have been assigned in the Addressing Table.
- Record the subnet for the Guest network:

192.168.0.224/27

PC Configurations

- Configure the assigned IPv4 address, subnet mask, and default gateway settings on the Staff, Sales, and IT PCs using your addressing scheme.
- Assign the IPv6 unicast and link local addresses and default gateways to the Staff, Sales, and IT networks according to the Addressing Table.

R1 Configurations

- Configure the device name according to the Addressing Table.
- Disable DNS lookup.
- Assign **Ciscoenpa55** as the encrypted privileged EXEC mode password.
- Assign **Ciscoconpa55** as the console password and enable login.
- Require that a minimum of **10** characters be used for all passwords.
- Encrypt all plaintext passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

- Configure and enable all the Gigabit Ethernet interfaces.
  - Configure the IPv4 addresses according to your addressing scheme.
  - Configure the IPv6 addresses according to the Addressing Table.
- Configure SSH on R1:
  - Set the domain name to **CCNA-lab.com**
  - Generate a **1024**-bit RSA key.
  - Configure the VTY lines for SSH access.
  - Use the local user profiles for authentication.
  - Create a user **Admin1** with a privilege level of **15** and use the encrypted password of **Admin1pa55**.
- Configure the console and VTY lines to log out after five minutes of inactivity.
- Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

Switch Configuration

- Configure the device name according to the Addressing Table.
- Configure the SVI interface with the IPv4 address and subnet mask according your addressing scheme.
- Configure the default gateway.
- Disable DNS lookup.
- Assign **Ciscoenpa55** as the encrypted privileged EXEC mode password.
- Assign **Ciscoconpa55** as the console password and enable login.
- Configure the console and VTY lines to log out after five minutes of inactivity.
- Encrypt all plaintext passwords.

Connectivity Requirements

- Use the web browser on the Staff, Sales, and IT PCs to navigate to **www.cisco.pka**.
- Use the web browser on the Staff, Sales, and IT PCs to navigate to **www.cisco6.pka**.
- All PCs should be able to ping all other the devices.

Running Scripts

R1 Configuration

```
enable
config t
service password-encryption
security passwords min-length 10
hostname R1
login block-for 180 attempts 4 within 120
enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60
ipv6 unicast-routing
username Admin1 secret 5 $1$mERr$Ty/EkWXcSXEwIckISrps8/
no ip domain-lookup
ip domain-name CCNA-lab.com
interface GigabitEthernet0/0
```

```
 ip address 192.168.0.1 255.255.255.128
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD::1/64
 no shutdown
interface GigabitEthernet0/1
 ip address 192.168.0.129 255.255.255.192
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
 no shutdown
interface GigabitEthernet0/2
 ip address 192.168.0.193 255.255.255.224
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:2::1/64
 no shutdown
interface Serial0/0/1
 ip address 172.16.1.2 255.255.255.252
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:2::1/64
 no shutdown
banner motd ^CAny text^C
line con 0
 exec-timeout 5 0
 password 7 0802455D0A1606181C1B0D517F
 login
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
exit
crypto key generate rsa general-keys modulus 1024
end
```

S1 Configuration

```
enable
conf t
service password-encryption
hostname S1
enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60
no ip domain-lookup
interface Vlan1
 ip address 192.168.0.2 255.255.255.128
 no shutdown
ip default-gateway 192.168.0.1
```

```
line con 0
 password 7 0802455D0A1606181C1B0D517F
 login
 exec-timeout 5 0
line vty 0 4
 exec-timeout 5 0
 login
line vty 5 15
 exec-timeout 5 0
 login
end
```

S2 Configuration

```
enable
conf t
service password-encryption
hostname S2
enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60
no ip domain-lookup
interface Vlan1
 ip address 192.168.0.130 255.255.255.192
 no shutdown
ip default-gateway 192.168.0.129
line con 0
 password 7 0802455D0A1606181C1B0D517F
 login
 exec-timeout 5 0
line vty 0 4
 exec-timeout 5 0
 login
line vty 5 15
 exec-timeout 5 0
 login
end
```

S3 Configuration

```
enable
conf t
service password-encryption
hostname S3
enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60
no ip domain-lookup
interface Vlan1
 ip address 192.168.0.194 255.255.255.224
 no shut
ip default-gateway 192.168.0.193
line con 0
 password 7 0802455D0A1606181C1B0D517F
 login
 exec-timeout 5 0
line vty 0 4
 exec-timeout 5 0
 login
line vty 5 15
 exec-timeout 5 0
 login
end
```