# Packet Tracer – Skills Integration Challenge
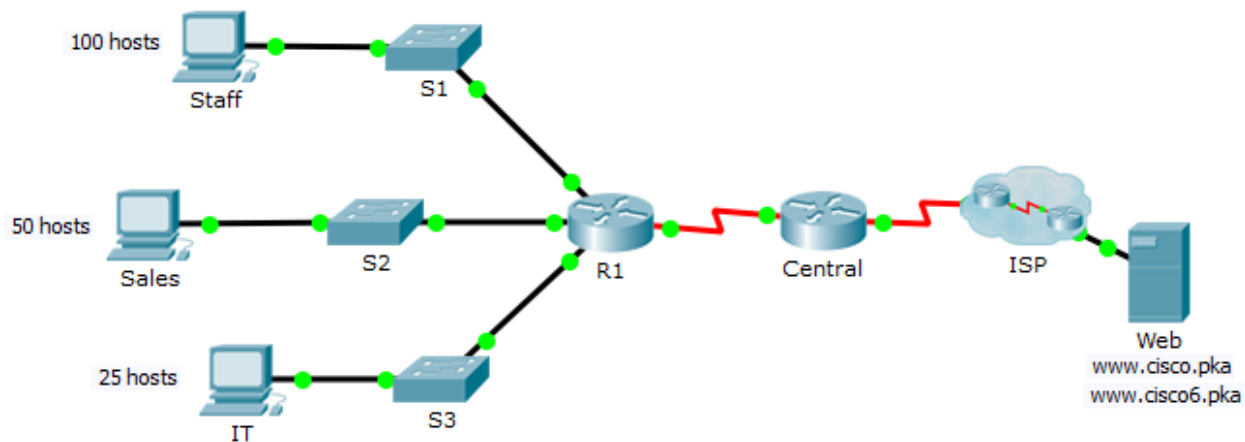
## Topology

## Addressing Table

| Device | Interface | IPv4 Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| | | **IPv6 Address/Prefix** | **IPv6 Link-local** | |
| R1 | G0/0 | | | N/A |
| | | 2001:DB8:ACAD::1/64 | FE80::1 | N/A |
| | G0/1 | | | N/A |
| | | 2001:DB8:ACAD:1::1/64 | FE80::1 | N/A |
| | G0/2 | | | N/A |
| | | 2001:DB8:ACAD:2::1/64 | FE80::1 | N/A |
| | S0/0/1 | 172.16.1.2 | 255.255.255.252 | N/A |
| | | 2001:DB8:2::1/64 | FE80::1 | N/A |
| Central | S0/0/0 | 209.165.200.226 | 255.255.255.252 | N/A |
| | | 2001:DB8:1::1/64 | FE80::2 | N/A |
| | S0/0/1 | 172.16.1.1 | 255.255.255.252 | N/A |
| | | 2001:DB8:2::2/64 | FE80::2 | N/A |
| S1 | VLAN 1 | | | |
| S2 | VLAN 1 | | | |
| S3 | VLAN 1 | | | |
| Staff | NIC | | | |
| | | 2001:DB8:ACAD::2/64 | FE80::2 | FE80::1 |
| Sales | NIC | | | |
| | | 2001:DB8:ACAD:1::2/64 | FE80::2 | FE80::1 |
| IT | NIC | | | |
| | | 2001:DB8:ACAD:2::2/64 | FE80::2 | FE80::1 |
| Web | NIC | 64.100.0.3 | 255.255.255.248 | 64.100.0.1 |
| | | 2001:DB8:CAFE::3/64 | FE80::2 | FE80::1 |

## Scenario / Background

The router Central, ISP cluster and the Web server are completely configured. You have been tasked with creating a new IPv4 addressing scheme that will accommodate 4 subnets using 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 are also tasked with finishing the basic security settings and interface configurations on R1. Furthermore, you will configure the SVI interface and basic security setting on switches S1, S2 and S3.

## Requirements

### IPv4 Addressing

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

### 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 IPv6 unicast and link local addresses and default gateway 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. Make sure to include the word **Warning** in the banner.
- Configure all the Gigabit Ethernet interfaces.
    - ο Configure the IPv4 addresses according to your addressing scheme.
    - ο Configure the IPv6 addresses according to the Addressing Table.
- Configure SSH on R1:
    - ο Set the domain name to **CCNA-lab.com**
    - ο Generate a **1024**-bit RSA key.
    - ο Configure the VTY lines for SSH access.
    - ο Use the local user profiles for authentication.
    - ο Create a user **Admin1** with a privilege level of **15** using the encrypted password for **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 Configurations

- 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.

## Verify Connectivity

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