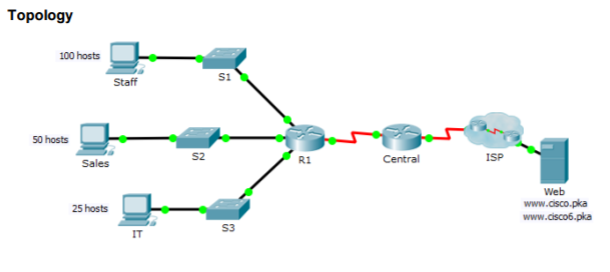
**Liberty University**

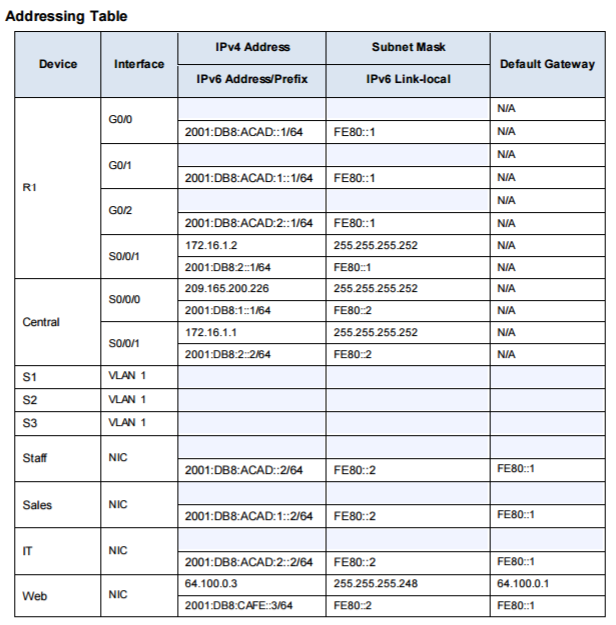
**CSIS 331**

**Lab 7 Instructions**

**Packet Tracer:**

*[Adapted from Cisco Networking Academy Intro to Networking 11.4.1.2]*





**Overview**

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

**Configuration 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 on your Lab 7 Answer Sheet

*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 and Input on your Answer Sheet.

• Using the web browser from Staff, Sales, and IT PCs, navigate to [www.cisco.pka](http://www.cisco.pka). Take a screenshot of each and and it to your Answer Sheet.

• Using the web browser from Staff, Sales, and IT PCs, navigate to [www.cisco6.pka](http://www.cisco6.pka).

• All PCs should be able to IPv6 and IPv4 ping all the devices. Input your results in your Answer Sheet.