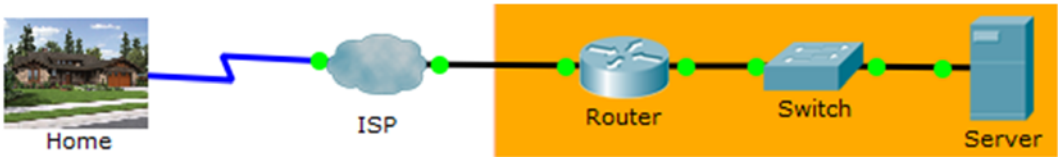
Packet Tracer – Putting it All Together

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	209.165.201.1	255.255.255.224	N/A
S1	VLAN 1	209.165.201.2	255.255.255.224	N/A
Server	NIC	209.165.201.30	255.255.255.224	209.165.201.1

Background / Scenario

This activity includes many of the skills that you have acquired during your Networking Essentials studies. First, you will configure the IP addresses on network devices in a simplified network. Second, you will set up the wireless configurations in home network. Finally, you will verify your implementation by testing end-to-end connectivity by accessing the web server, www.server.pka, and router R1 using SSH in the simplified network.

Implementation

Router R1

- Configure the device name according to the Addressing Table.
- Configure the IP address on G0/1 interface according to the IP addressing table and enable the interface.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited. Make sure to include the word **warning** in the banner.
- Assign **cisco** as the console password and enable login.
- Assign **class** as the encrypted privileged EXEC mode password.
- Encrypt all plaintext passwords.

Configure SSH on R1:

- Set the domain name to **networking.pka**
- Generate a **1024**-bit RSA key.
- Create a user with a username **admin** with password **cisco123**
- Configure the VTY lines for SSH access.
- Use the local user profiles for authentication.

Switch S1

- Configure the device name according to the Addressing Table.

- Configure the IP address of the switch on SVI interface according to the IP addressing table and enable the interface.

Server

Configure the IP address of the server according to the IP addressing table.

Wireless Router in the Home

Enter the **Home** cluster. From the web browser on PC, configure the following:

Initial Wireless Router IP Address: **192.168.1.1**

Username / Password: ..... **admin** / **admin**

SSID: ..... **MyHome**

Security Mode: ..... **WPA2 Personal**

Passphrase: **123Cisco**

DHCP Configuration:

Wireless Router IP Address: **192.168.20.1**

Starting IP Address: **192.168.20.101**

Maximum Number: **100**

DNS 1: **209.165.201.30**

End Devices in the Home

Configure the wireless settings so the end devices can access www.server.pka.

SSID: ..... **MyHome**

Security Mode: ..... **WPA2 Personal** or **WPA2-PSK**

Passphrase: **123Cisco**

Note: For Tablet PC and Pda, use the Config tab for the wireless configurations.

Verify Connectivity

- Verify that IP addresses are in the correct networks. All the end devices should be in 192.168.20.0/24 network. If they are not in the correct network, enter the following commands at the command prompt.

  PC> **ipconfig /release**

  PC> **ipconfig /renew**

- Verify that all end devices in the Home can access www.server.pka.
- Verify that all end devices in the Home can access R1 via SSH with password **cisco123**.

  PC> **ssh –l admin 209.165.201.1**