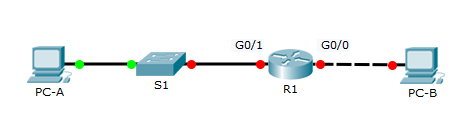
Packet Tracer – Building a Switch and Router Network

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

1. Objectives

* Configure the router and switch.
* Verify network connectivity.
* Configure and verify an SSH implementation.

1. Background / Scenario

In this lab, you will configure the devices to match the addressing table. After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment. You will also access the router remotely via SSH. If necessary, refer to previous Packet Tracer activities for help with configurations.

1. Requirements

* Configure the IP address, subnet mask, and default gateway settings on PC-A and PC-B.
* Establish a console connection to R1 and configure the following settings:
  1. The hostname is **R1**.
  2. Assign **class** as the privileged EXEC encrypted password and **cisco** as the console password.
  3. Encrypt plaintext passwords.
  4. Create an appropriate banner. Use the word **access** somewhere in the text of the banner.
  5. Configure the IP address according to the Addressing Table and activate both interfaces.
  6. Save the configuration.
  7. Verify the PC-A can now ping PC-B. If not, check your configurations.
* Establish a console connection to S1 and configure the following settings:
  1. The hostname is **S1**.
  2. Assign **class** as the privileged EXEC encrypted password and **cisco** as the console password.
  3. Encrypt plaintext passwords.
  4. Create an appropriate banner. Use the word **access** somewhere in the text of the banner.
  5. Configure the IP address for the SVI for VLAN 1 according to the Addressing Table and activate the interface.
  6. Configure the default gateway according to the Addressing Table.
  7. Save the configuration.
* Configure SSH on R1.
  1. Set the domain name to academy.net
  2. Generate RSA keys with a 1024 key length.
  3. Create a user with **SSHuser** as the username and **cisco** as the secret password.
  4. Configure the VTY lines to use the local username database for login credentials and allow on SSH for remote access.
* Verify PC-A can remotely access R1 using SSH.
  1. Click PC-A > Desktop > Command Prompt.
  2. Enter the command ssh -l SSHuser 192.168.1.1 to remotely access R1.   
     **Note**: -l is a lower case “L”, not a one.
  3. Enter the correct password.