# 1.**6** – ITN - PacketKnows – Configuring Secure Passwords and SSH

## Addressing Table

| Device | Interface | Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| RTA | Fa0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| S1 | Vlan 1 | 192.168.1.2 | 255.255.255.0 | N/A |

**NOTE**

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device.**
- **Always type "save" when configuring IP addresses of PC's.**

## Scenario

The network administrator has asked you to prepare RTA for deployment. Before it can be connected to the network, security measures must be enabled.

## Requirements

- Configure IP addressing on **S1** according to the Addressing Table.
- Configure IP addressing on **RTA** and enable the interface.
- Configure the hostname as **RTA**.
- Encrypt all plaintext passwords.
- Configure SSH on RTA and Switch0

**Configuration Guide: Setting Up IP Addressing, VLAN, Hostname, Password Encryption, and SSH**

**Part 1: Configuring RTA Router**

**Steps:**

1. **Configure IP Addressing on RTA:**
    - Enter global configuration mode:
    - Change hostname of R1 to **RTA** and Access the FastEthernet interface and assign IP address and subnet mask:
2. **Set Up Hostname and Password Encryption:**
    - Set hostname to RTA:
    - Encrypt passwords:
3. **Generate RSA Keys and Configure SSH:**
    - Generate RSA keys (choose 1024 bits when prompted):
    - Configure SSH version 2 and set the domain name:
    - Create a local username and password for SSH login:
4. **Configure SSH Access:**
    - Set up login failure rate limiting:
    - Access VTY lines, allow SSH access, and enable local login:
5. **Save Configuration and Exit:**
    - Save the configuration changes:

**Part 2: Configuring S1**

**Steps:**

1. **Configure VLAN and IP Addressing:**
    - Enter global configuration mode:
        - Access VLAN 1 and assign IP address and subnet mask:
2. **Enable SSH and Set Up Local Login:**
        - Set the domain name:
        - Create a local username and password for SSH login:
        - Generate RSA keys (choose 1024 bits when prompted):
        - Configure SSH version 2:
        - Access VTY lines, allow SSH access, and enable local login:
3. **Save Configuration and Exit:**
        - Save the configuration changes:

**Note:** Ensure that you are in the appropriate configuration mode before executing commands. Verify connectivity after the configurations to confirm proper setup.

**Part 3: Verifying SSH Connection between RTA and S1**

After configuring SSH on RTA and Switch0, it's important to verify that SSH connectivity is successfully established between the RTA router and S1 switch. Here's how you can do it:

**Test SSH Connectivity:**

- From RTA, attempt to SSH into S1 using the configured username and password:

RTA#ssh -l any_user192.168.1.2

password: cisco

Verify successful SSH login and access to S1.

S1>