**EXPERIMENT NO. 10**

**AIM**: To configure SSH using Cisco Packet Tracer.

**OBJECTIVES:** Part 1: To Simulate BGP routing protocol, check the updated routing tables and check the connectivity among devices.

**REQUIREMENT**: cisco packet tracer

**THEORY:** The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the nonprotected login protocols (such as [TELNET,](https://www.ssh.com/ssh/telnet) rlogin) and insecure file transfer methods (such as FTP).

The protocol is used in corporate networks for:

* Providing secure access for users and automated processes
* Interactive and automated file transfers
* Issuing remote commands
* Managing network infrastructure and other mission-critical system components.

The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server. The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server. After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server. There are several options that can be used for user authentication. The most common ones are passwords and public key authentication.

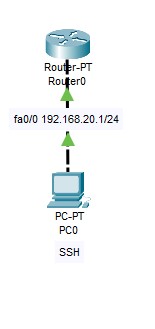
The public key authentication method is primarily used for automation and sometimes by system administrators for single sign-on. It has turned out to be much more widely used than we ever anticipated. The idea is to have a cryptographic key pair - public key and private key - and configure the public key on a server to [authorize access](https://www.ssh.com/ssh/authorized_keys/) and grant anyone who has a copy of the private key access to the server. The keys used for authentication are called [SSH keys.](https://www.ssh.com/ssh/key/) Public key authentication is also used with smartcards.

The main use of key-based authentication is to enable secure automation. Automated secure shell file transfers are used to seamlessly integrate applications and also for automated systems & configuration management.

Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted according to the parameters negotiated in the setup. During the negotiation the client and server agree on the symmetric encryption algorithm to be used and generate the encryption key that will be used. The traffic between the communicating parties is protected with industry standard strong encryption algorithms (such as AES (Advanced Encryption Standard)), and the SSH protocol also includes a mechanism that ensures the integrity of the transmitted data by using standard hash algorithms (such as SHA-2 (Standard Hashing Algorithm)).

**Scenario**

**Part 1: Scenario for SSH:**



**Procedure for SSH:**

Step 1: Configure router interface for IP address

Step 2: Set up a hostname and a domain name

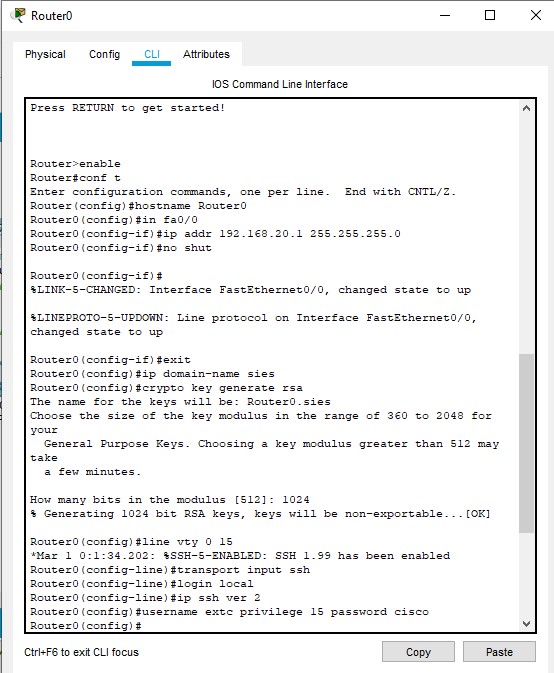
Step 3: Configure local username and password

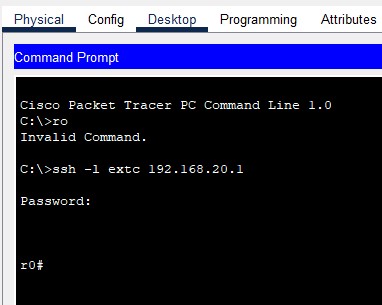
Step 4: generate RSA public and private key

Step 5: Allow on SSH access

Step 6: Apply enable password

Step 7: Now go to PC assign IP address and login on router using SSH.





**CONCLUSION**: The configuration of SSH using Cisco Packet Tracer was performed successfully.

**Questions on SSH:**

1. Secure shell (SSH) network protocol is used for \_\_\_\_\_\_\_\_\_\_
   1. secure data communication
   2. remote command-line login
   3. remote command execution
   4. all of the mentioned
2. SSH can be used in only \_\_\_\_\_\_\_\_\_\_\_\_\_
   1. unix-like operating systems
   2. windows
   3. both unix-like and windows systems
   4. none of the mentioned
3. SSH uses \_\_\_\_\_\_\_\_\_\_\_ to authenticate the remote computer.
   1. public-key cryptography
   2. private-key cryptography
   3. any of public-key or private-key
   4. both public-key & private-key
4. Which standard TCP port is assigned for contacting SSH servers? a) port 21
   1. port 22
   2. port 23
   3. port 24
5. Which one of the following protocol can be used for login to a shell on a remote host except SSH?
   1. telnet
   2. rlogin
   3. both telnet and rlogin
   4. none of the mentioned
6. Which one of the following is a file transfer protocol using SSH?
   1. SCP
   2. SFTP
   3. Rsync
   4. All of the mentioned
7. Which one of the following authentication method is used by SSH?
   1. public-key
   2. host based