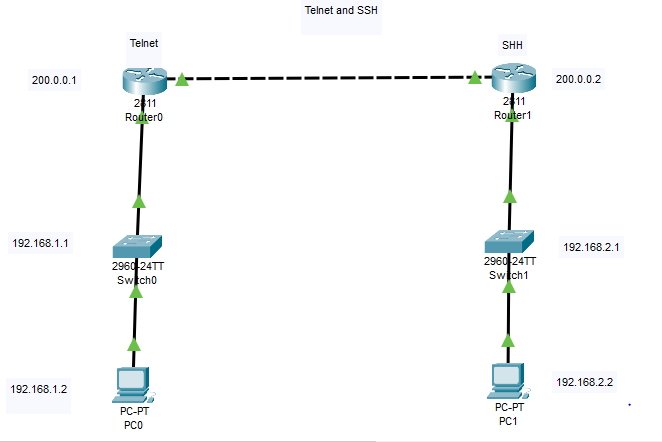
***Task 2 - Network Security***

**Introduction -**

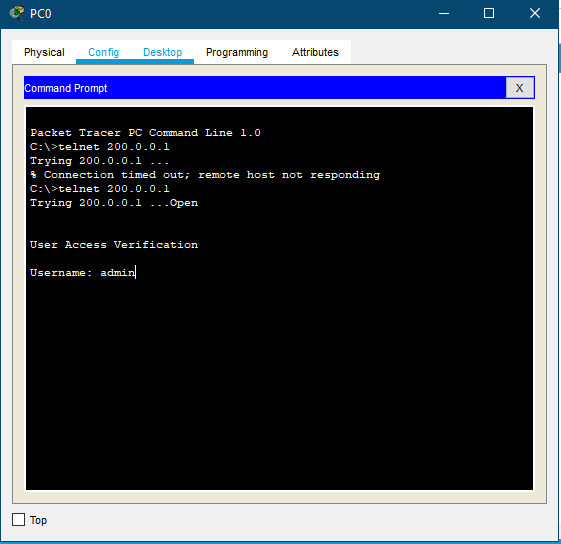
This report will demonstrate an understanding of the fundamentals of Cloud Computing and its architectures. It will also analyse the evolution and fundamental concepts of Cloud Computing. It will show a design of a secure network for a corporate environment and investigate the purpose and requirements of a secure network according to a given scenario and will determine which network hardware and software to use in this network. It will show the design of a secure network according to a given scenario. It will also discuss, using examples, the importance of Network Security.

**Task - 2**

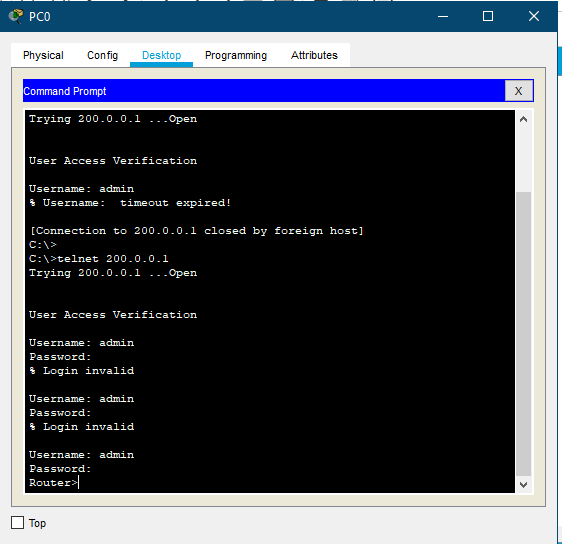
**Telnet and SSH Network Design**



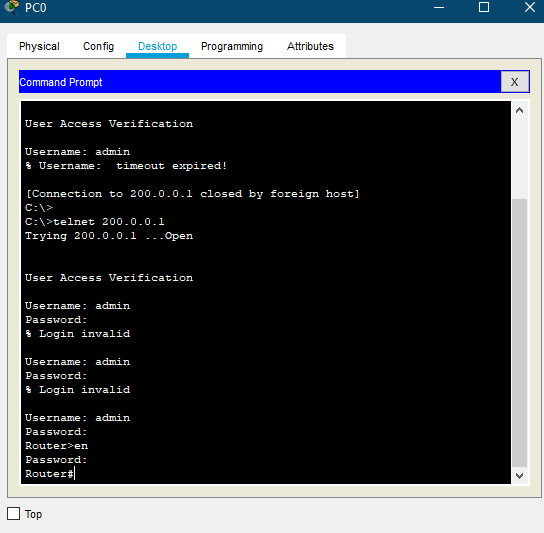
**PC0 Telnet User Access Verification**

****

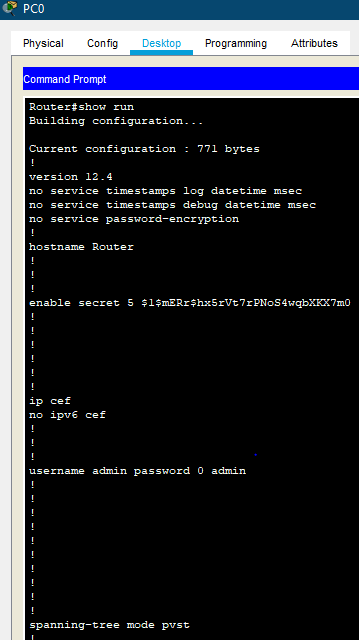
**PC0 Telnet Username and Password Verification**

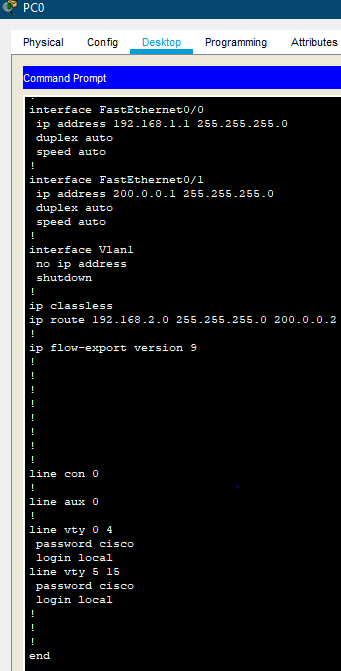
****

**PC0 Enabling Router access**

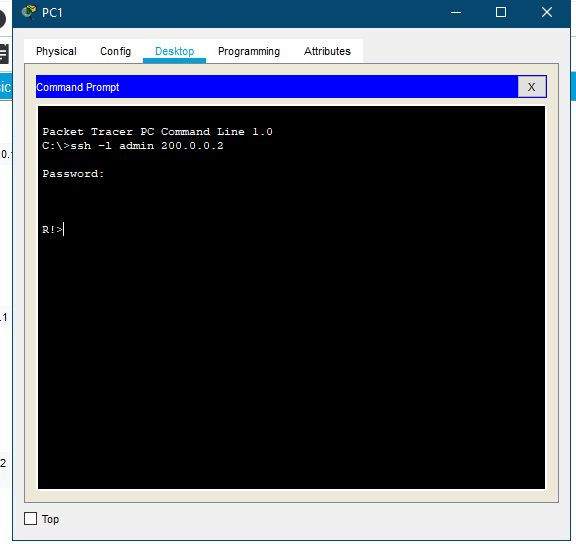
****

**PC0 Router Settings - “Show run”**

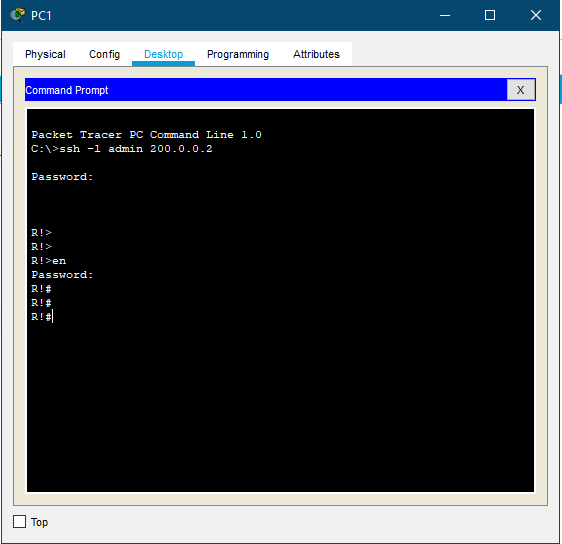
****

****

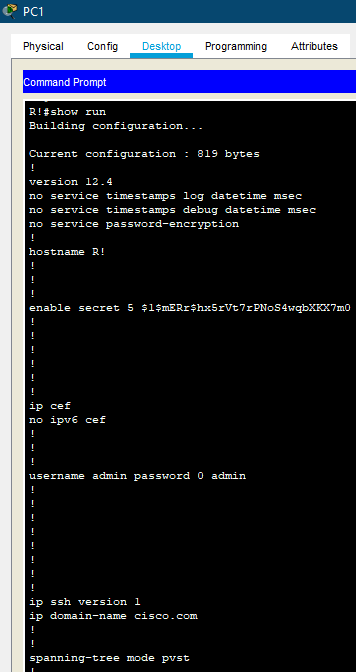
**PC1 SSH-1 password Verification**

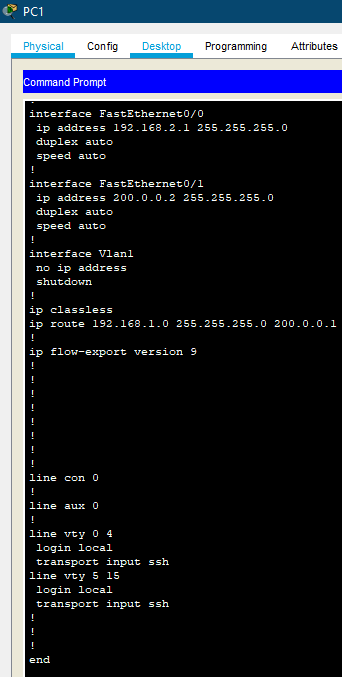
****

**PC1 SSH-1 Enabling R1 router password verification**

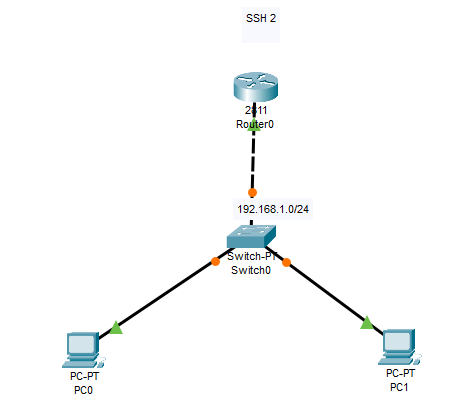
****

**PC1 SSH-1 Router Settings - “show run”**

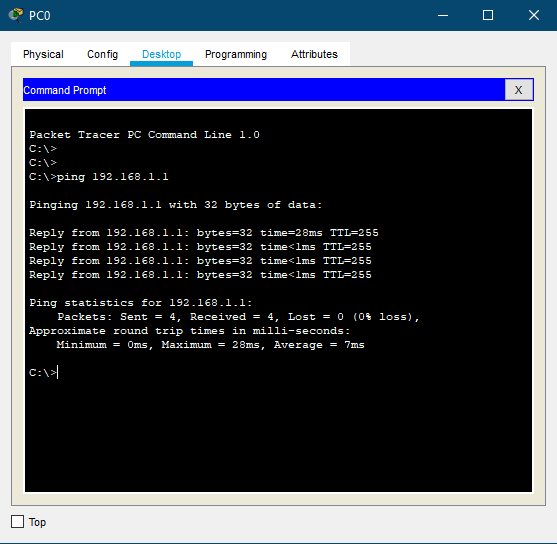
****

****

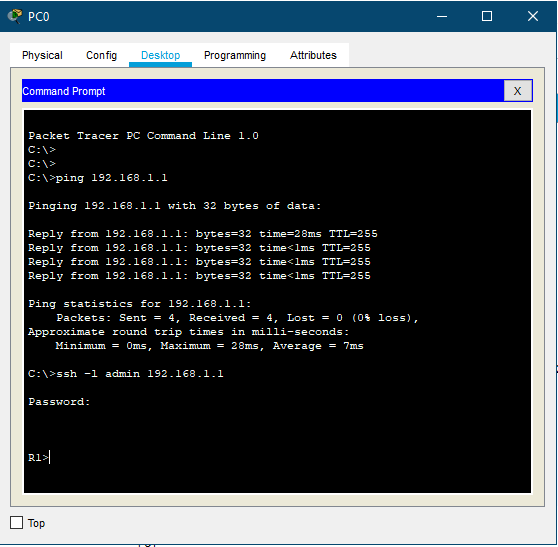
**SSH-2 Network Design**

****

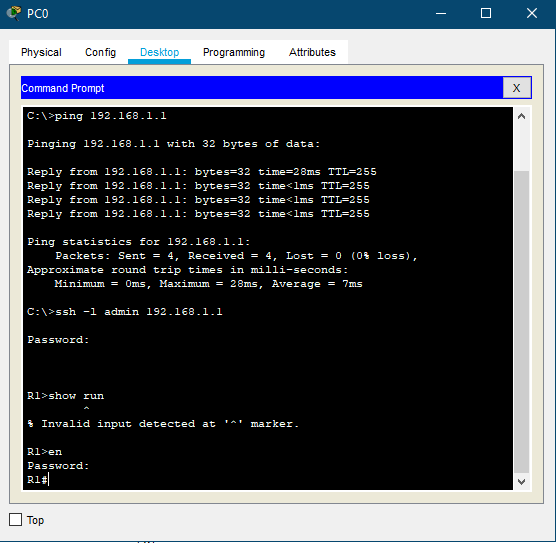
**SSH-2 Ping testing PC0**

****

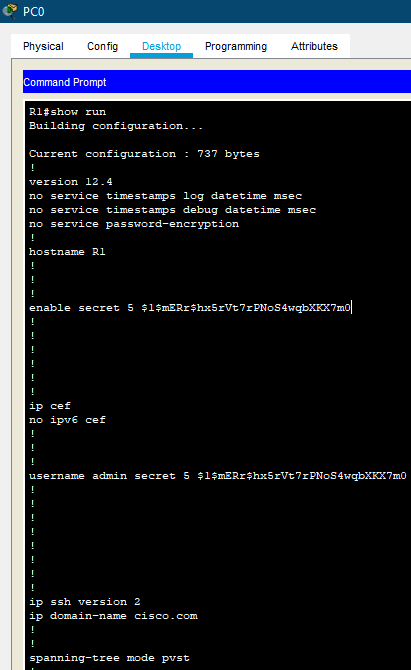
**SSH-2 admin access verification**

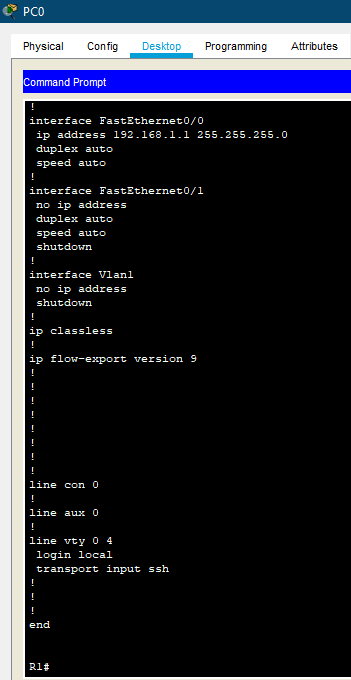
****

**SSH-2 Enabling Router verification**

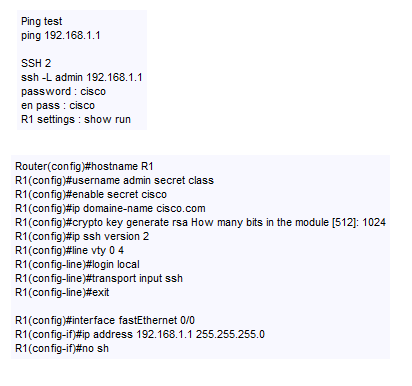
****

**PC0 SSH-2 Router Settings - “show run”**

****

****

**SSH-2 Command list**

****

**find out what other security measures, such as: SSH1, SSH2, etc. can be implemented to remotely access your network, with strong encryption using Packet Tracer and why.**

When differentiating SSH2 with SSH1, it's basic to require note that SSH2 isn't as it were SSH1 with modern conventions connected. it may be a wrapped up adjustment of the essential tradition and has presently joined inalienable securities against different known vulnerabilities in SSH1.

Inside the early days of SSH, clients were able to energetically download and utilize SSH1 in show disdain toward of the reality that it contained secured developments. With the coming of SSH2, the creators restricted the allow. The firm that holds the allow, SSH Communications Security, re-released the SSH client as SSH Tectia and no longer particularly offers free downloads. Those who qualify for a non-commercial license can download a more prepared frame of SSH2 (SSH 3.2) from an assortment of Web goals. Rummage around for "SSH noncommercial" on Google and you'll find a grouping of regions that allow clients to download more prepared adjustments of SSH for Unix, Windows and Mac systems.

The major contrasts between SSH1 and SSH2 drop into two crucial categories: specialized and allowing. In truth, SSH2 businesses assorted encryption and affirmation calculations. SSH1 offers four encryption calculations (DES, 3DES, Thought and Blowfish), while SSH2 dropped back for DES and Thought, but included three present day calculations. SSH1 additionally utilized the RSA confirmation calculation, though SSH2 traded to the Progressed Signature Calculation (DSA). These changes were laid out to both outsmart mental property issues enveloping the utilization of Thought and RSA, and increase the base level of security in SSH2 by utilizing more grounded calculations.

**SSH2**

SSH2 as well gives included convenience. Most extraordinarily, it incorporates the sftp program to the SSH suite. This program survives the SSH protocol's encryption advancement to supply secure infers for record trade between blocked off systems. It's additionally rapidly drawing closer affirmation as an industry standard by the Internet Planning Task Force's Secure Shell Working Gather.

**Why upgrade to SSH2 ?**

* SSH1 isn't supported by an energetic headway community. This limits the availability of future upgrades and securities against present day threats.
* SSH1 has recorded vulnerabilities, checking defenselessness to a variety of the cryptographic man-in-the-middle attack.
* SSH2 gives security specialists success and encourages secure affiliations. Don't ignore the centrality of teaching your client base on the proper utilization of these instruments.

Discuss which **security measures** in Task 2 you would use for CCL, where and why.

The security measure that CCL would use would be DHCP Telnet with secure password for user verification into routers as -

**How does Telnet work compared to DHCP**

Since it was set up some time recently the broad appropriation of the Internet, Telnet does not utilize any shape of encryption on its possessor, rendering it excess in terms of present day innovation. It is generally covered with the Secure Shell (SSH) standard, at slightest on the open Web, but in circumstances where Telnet is still in use, there are a number of ways to secure the communications.

The buyer interfaces to the server utilizing the Telnet interface, which includes getting to the Telnet command provoke utilizing the taking after sentence structure: telnet hostname interface. The customer at that point performs commands on the computer utilizing distinctive Telnet commands on the Telnet ask. The director ends the Telnet arrangement by means of Telnet to cancel the association and sign off.

**Conclusion -**

In conclusion, this report demonstrates an understanding of the fundamentals of Cloud Computing and its architectures. It will also analyse the evolution and fundamental concepts of Cloud Computing. It shows a design of a secure network for a corporate environment and investigates the purpose and requirements of a secure network according to a given scenario and will determine which network hardware and software to use in this network. It shows the design of a secure network according to a given scenario. It also discusses, using examples, the importance of Network Security.

SearchSecurity. (2020). An introduction to SSH2. [online] Available at: https://searchsecurity.techtarget.com/tip/An-introduction-to-SSH2 [Accessed 23 Feb. 2020].