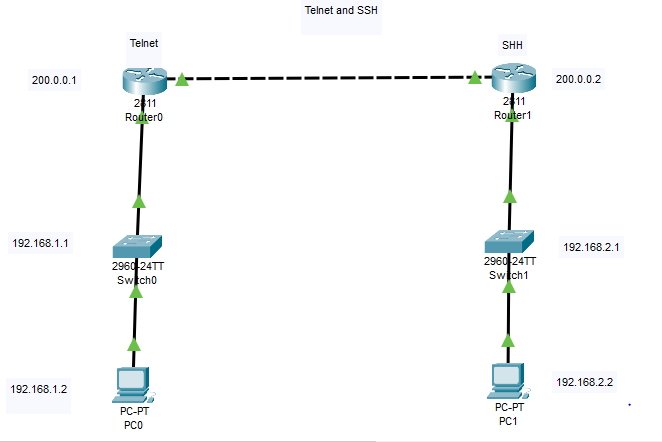
***Task 2 - Network Security***

**Introduction -**

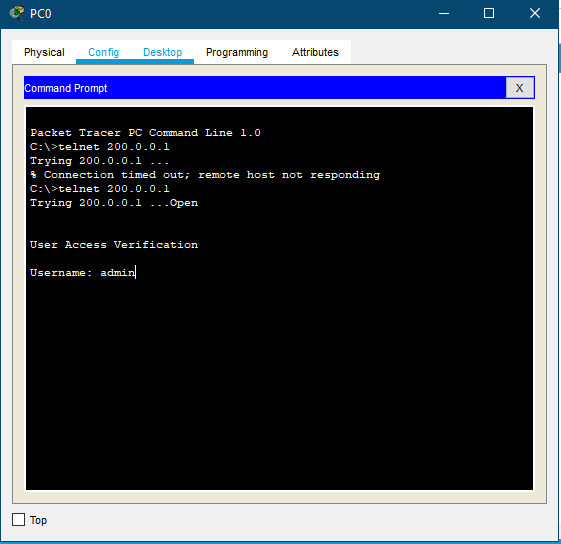
This report will demonstrate an understanding of the fundamentals of Cloud Computing and its architectures. It will also analyse the evolution and fundamental concepts of Cloud Computing. It will show a design of a secure network for a corporate environment and investigate the purpose and requirements 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**

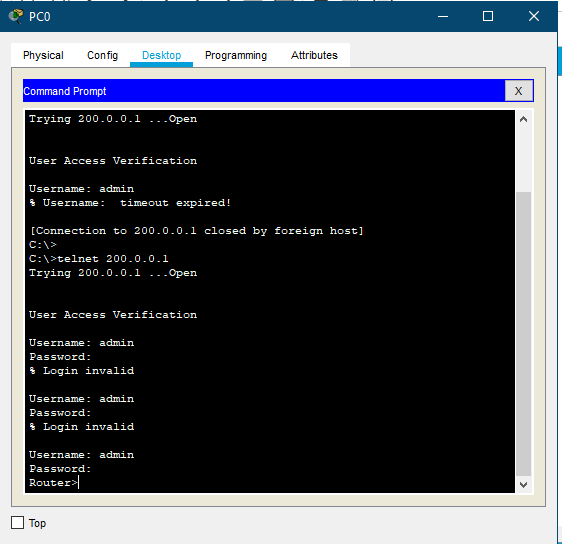
**Telnet and SSH Network Design**



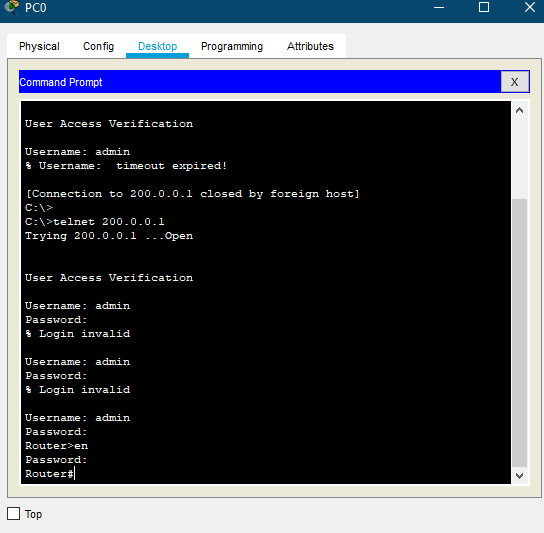
**PC0 Telnet User Access Verification**

****

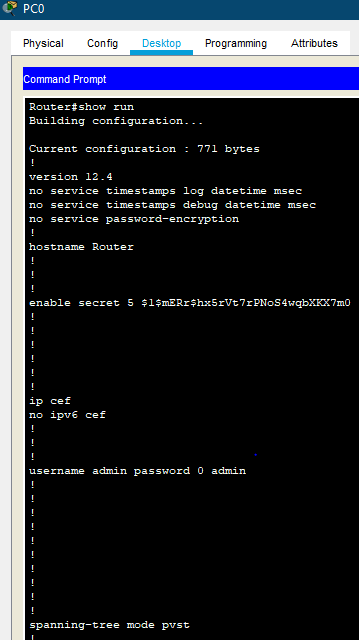
**PC0 Telnet Username and Password Verification**

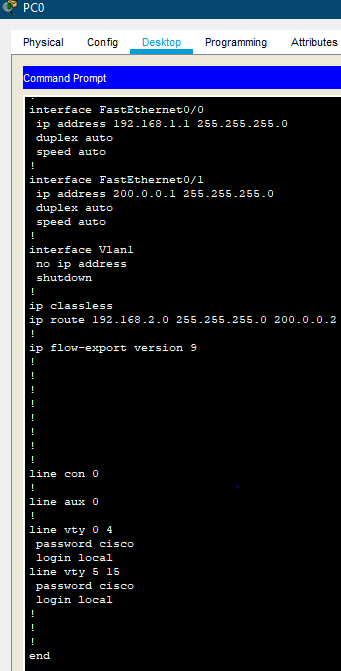
****

**PC0 Enabling Router access**

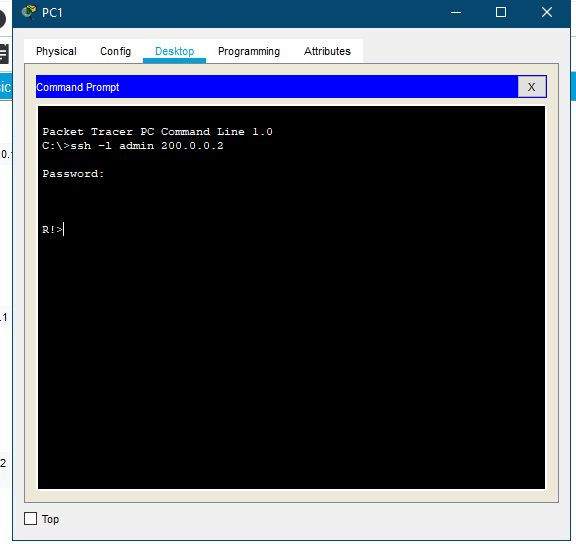
****

**PC0 Router Settings - “Show run”**

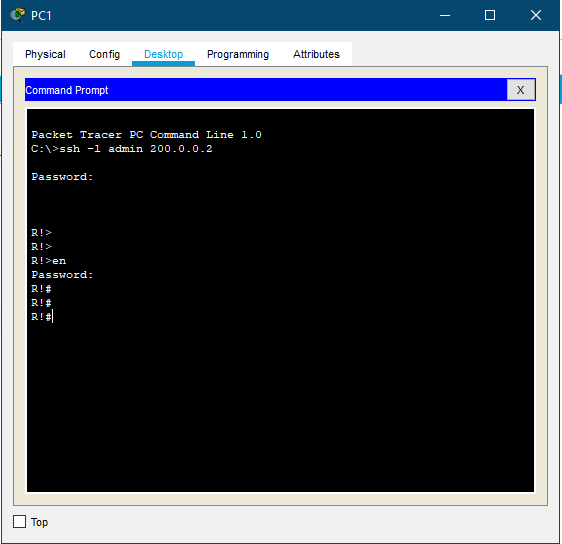
****

****

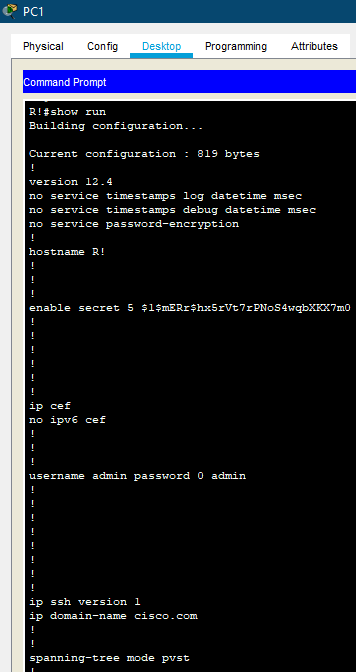
**PC1 SSH-1 password Verification**

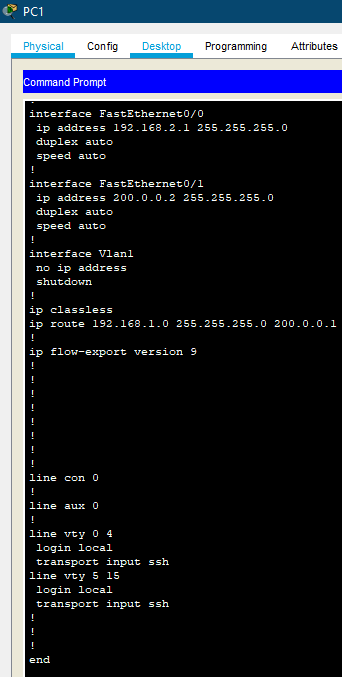
****

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

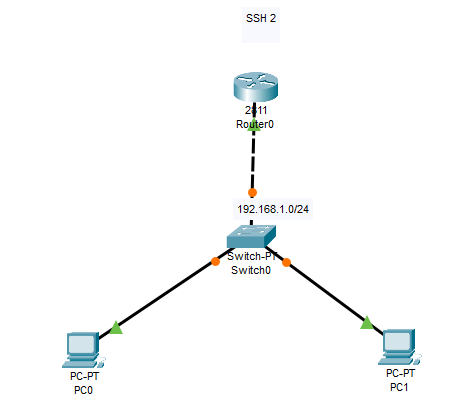
****

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

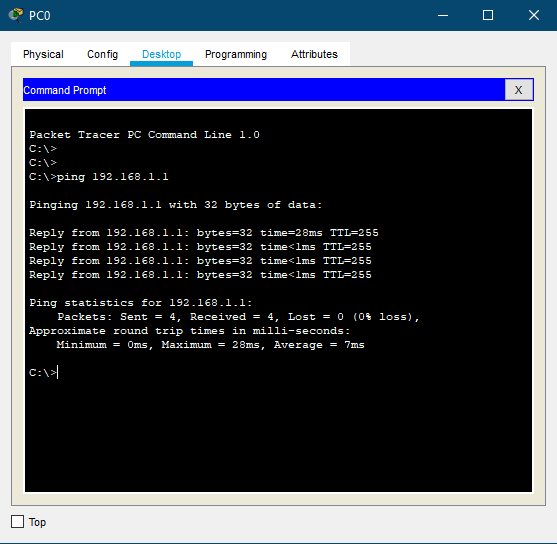
****

****

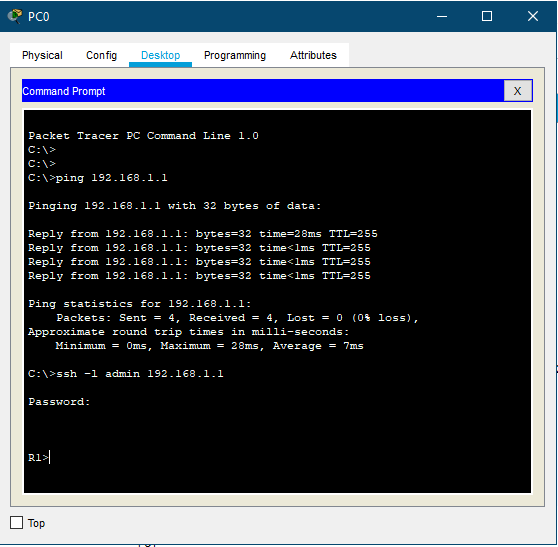
**SSH-2 Network Design**

****

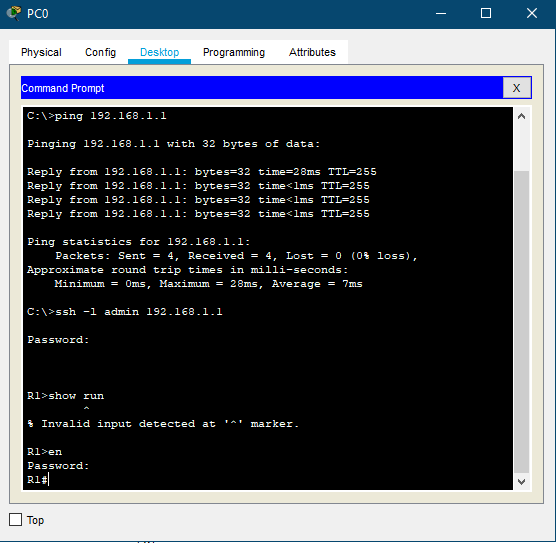
**SSH-2 Ping testing PC0**

****

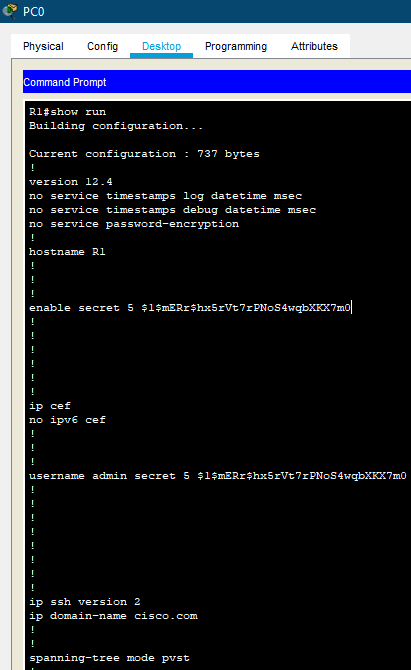
**SSH-2 admin access verification**

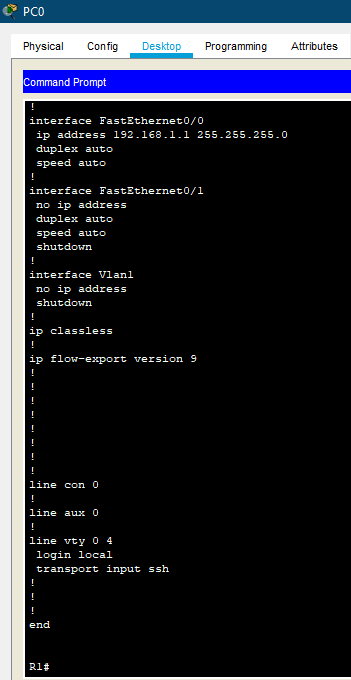
****

**SSH-2 Enabling Router verification**

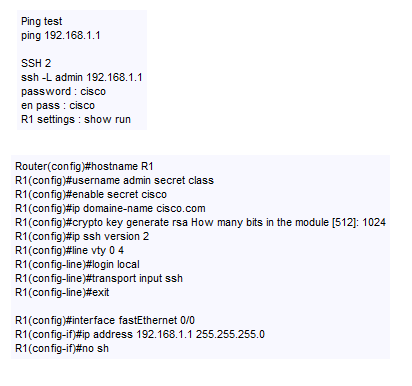
****

**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 comparing SSH2 to SSH1, it's important to note that SSH2 is not simply SSH1 with new protocols plugged in. It's a complete rewrite of the original protocol and has now incorporated built-in protections against a number of known vulnerabilities in SSH1.

In the early days of SSH, users were able to freely download and use SSH1 despite the fact that it contained patented technologies. With the advent of SSH2, the creators restricted the license. The firm that holds the license, SSH Communications Security, re-released the SSH client as SSH Tectia and no longer directly offers free downloads. Those who qualify for a non-commercial license can download an older version of SSH2 (SSH 3.2) from a variety of Web sites. Search for "SSH noncommercial" on Google and you'll find a variety of sites that allow users to download older versions of SSH for Unix, Windows and Macintosh systems.

The major differences between SSH1 and SSH2 fall into two main categories: technical and licensing. Technically speaking, SSH2 uses different encryption and authentication algorithms. SSH1 offers four encryption algorithms (DES, 3DES, IDEA and Blowfish), while SSH2 dropped support for DES and IDEA, but added three new algorithms. SSH1 also utilized the RSA authentication algorithm, while SSH2 switched to the Digital Signature Algorithm (DSA). These changes were designed to both circumvent intellectual property issues surrounding the use of IDEA and RSA, and increase the base level of security in SSH2 by utilizing stronger algorithms.

**SSH2**

SSH2 also provides added functionality. Most notably, it adds the sftp program to the SSH suite. This program uses the SSH protocol's encryption technology to provide a secure means for file transfer between remote systems. It's also rapidly approaching acceptance as an industry standard by the Internet Engineering Task Force's Secure Shell Working Group.

**Why upgrade to SSH2 ?**

* SSH1 is no longer supported by an active development community. This limits the availability of future upgrades and defenses against new threats.
* SSH1 has documented vulnerabilities, including susceptibility to a variant of the cryptographic man-in-the-middle attack.

SSH2 provides security professionals with a powerful means to facilitate secure connections. Don't forget the importance of educating your user base on the proper use of these tools.

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 established before the widespread adoption of the Web, Telnet does not use any form of encryption on its own, rendering it redundant in terms of modern technology. It has mostly overlapped with the Secure Shell (SSH) standard, at least on the public Internet, but in situations where Telnet is still in use, there are a few ways to secure the communications.

The consumer connects to the server using the Telnet interface, which involves accessing the Telnet command prompt using the following syntax: telnet hostname link. The consumer then performs commands on the computer using different Telnet commands on the Telnet request. The administrator terminates the Telnet order via Telnet to cancel the connexion 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 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 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].