



REMOTE ACCESS TO A ROUTER SECURELY USING SSH

Hadya.S.Hawedi^{*}, Omran Ali Bentaher^{**} and Kaled E. I. Abodhir^{***}

ABSTRACT

Routers in a computer network are responsible for managing much of the data flow. Therefore, it is important to properly configure routers, as this will help to resist attacks and maintain the security and confidentiality of network traffic. Using Telnet for accessing a router remotely is not secure enough. The aim of this paper is to demonstrate that using Secure Socket Shell protocol (SSH) to remote login a router is more secure. Cisco packet tracer simulation has been used for configure the router. The simulation showed that The SSH is provides a strong authentication and encryption, preserves the confidentiality and privacy of communications.

Keywords: Router, Remote access, Telnet, SSH, Security, VTY

1. INTRODUCTION

In a very short time , computer networks have expanded in both size and importance. There may be serious consequences if the protection of the network were breached, such as loss of privacy, theft of information and even legal liability. The types of possible threats to network security are constantly changing in order to make the situation even more difficult[1]. It is important to find the balance between being disconnected and open as e-business and internet applications continue to develop. Routers are networking machines running on Layer 3 on open system interconnection model network layer. They are responsible for receiving, processing, and transmitting data packets between networks of connected computers[2]. The router inspects the destination address when a data packet

* Faculty of Information Technology Al Asmarya University Zliten, Libya.

*corresponding author: hadia20008@asmarya.edu.ly

** Higher institute of science and technology Zliten, Libya.

E-mail: *omalbeta@yahoo.com*

*** Faculty of science Al Asmarya university Zliten, Libya.

E-mail: *k.abodhir @ asmarya. edu.ly*



arrives, consults its routing tables to determine the best path and then moves the packet along that path. The network may be exposed to attackers by a security hole in a network and the personal details would be at risk. A key element in any security implementation is router security. Routers are definite targets for attackers on a network[3]. It can be a possible help to them if an attacker is able to hack and access a router. An significant first step in protecting the network is protecting routers at the network perimeter. There are many protocols for accessing a router remotely such as Telnet and Secure Socket Shell (SSH) [4]. As Telnet is an unencrypted text-oriented protocol without authentication[5]. SSH is a network protocol that provides a safe way for administrators to access a remote computer[6]. The group of utilities which implement the protocol are also referred to by SSH[7]. Secure Shell provides authentication and secures the exchange of encrypted data between two computers that are connected via an unsafe network such as the Internet[8]. Network administrators are widely used by SSH to remotely manage organizations and applications, allowing them to log on to another computer over a network, perform commands, and move files from one computer to another[9].

2. ROUTERS SECURITY PROBLEMS

Since routers provide other networks with gateways, they are obvious targets and are subject to a number of attacks. Here are several instances of different security issues :

- Compromising access control will reveal specifics of network configuration, thereby enabling attacks against other components of the network.
- Compromising the route tables will reduce reliability, refuse communication services to the network, and reveal confidential information.
- Misconfiguring a router traffic filter will expose scans and attacks to internal network components, making it simpler for attackers to avoid detection[10].

In multiple ways, attackers can compromise routers, so there is no single solution that can be used by network administrators to fight them. Similar to the types of attacks such as IP spoofing and session hijacking, the forms that routers are hacked[11].

3. SECURITY ROUTER CATEGORIES

A significant first step in protecting the network is to protect routers at the network perimeter, some of these categories are:

Physical security Locate the router in a locked room, which is only open to authorized



staff, to provide physical security. They should also be free from any electrostatic or magnetic interference and have temperature and humidity controls. Install an uninterruptible power supply and keep spare components available to reduce the risk of DoS because of a power failure[12] [13] [14].

Update the router IOS whenever advisable The safety features develop over time in an operating system. However, the most stable version available may not be the most recent version of an operating system. Using the new stable update that meets the feature specifications of your network to get the best security value from your operating system.

Eliminate the potential abuse of unused ports and services To make it as safe as possible, harden the router. By default, a router has several services allowed. Many of these facilities are redundant and can be used for information collection or misuse by an attacker. By disabling unnecessary facilities.

4. ROUTERS LOCATION IN A NETWORK.

In modern networks, routers perform several different tasks and here where fundamental ways in which routers are employed.

4.1 Routers of the Interior

An interior router forwards traffic within an entity or company between two or more local networks. The networks linked by an indoor router also have the same security policy,[15] and there is generally a high degree of confidence between them, as shown in figure 1.

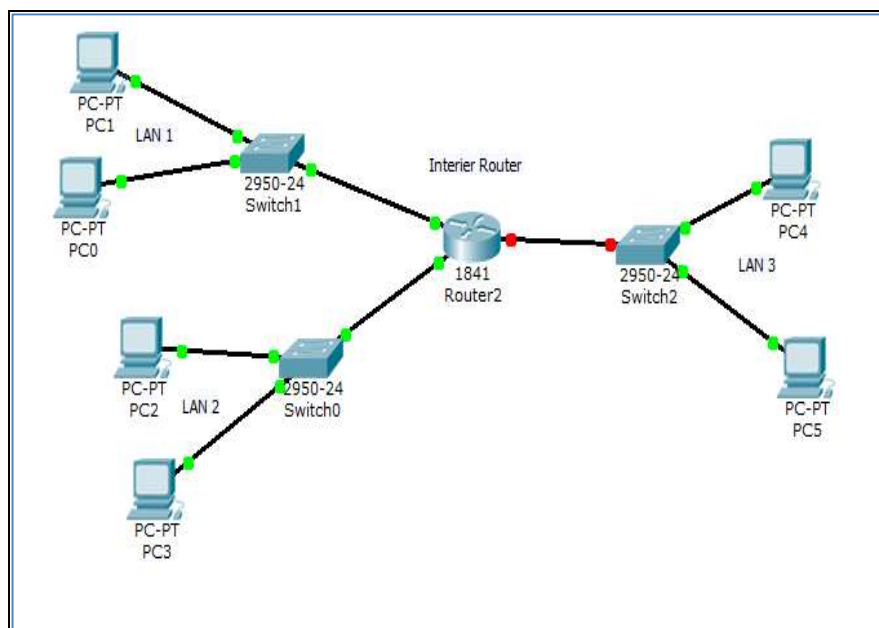


Figure 1: Routers of the interior

4.2 Routers of the Backbone

One that forwards traffic between various companies is a backbone or external router. Backbone routers direct the traffic between the various networks that make up the Internet as shown in figure 2.

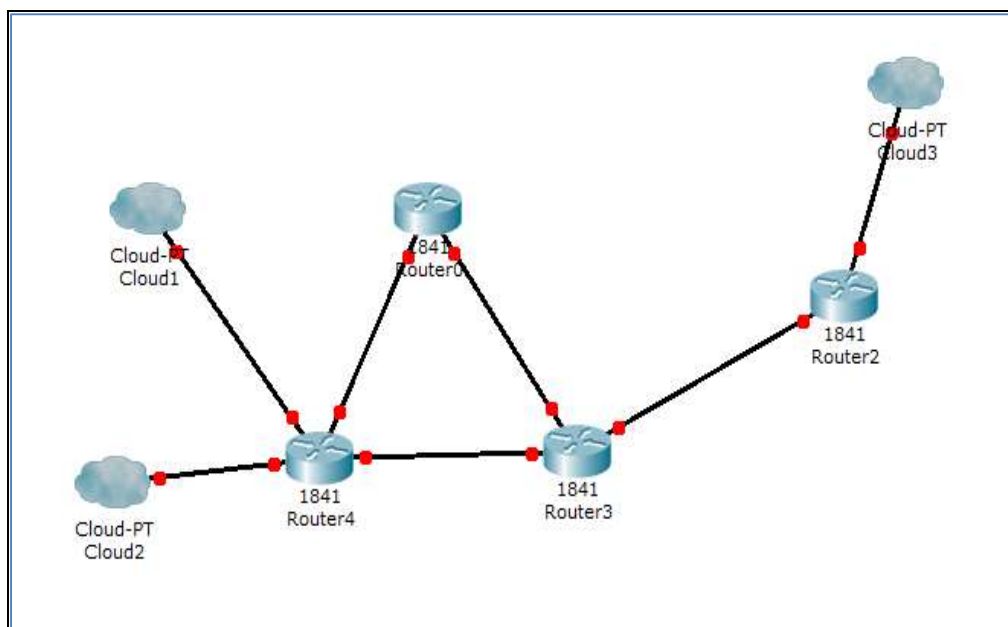


Figure 2: Routers of the Backbone

4.3 Border Routers



A border router forwards traffic between external networks and an enterprise. A border router's main feature is that it forms part of the boundary between an enterprise's trusted internal networks and untrusted external networks (e.g. the Internet), as shown in figure 3.

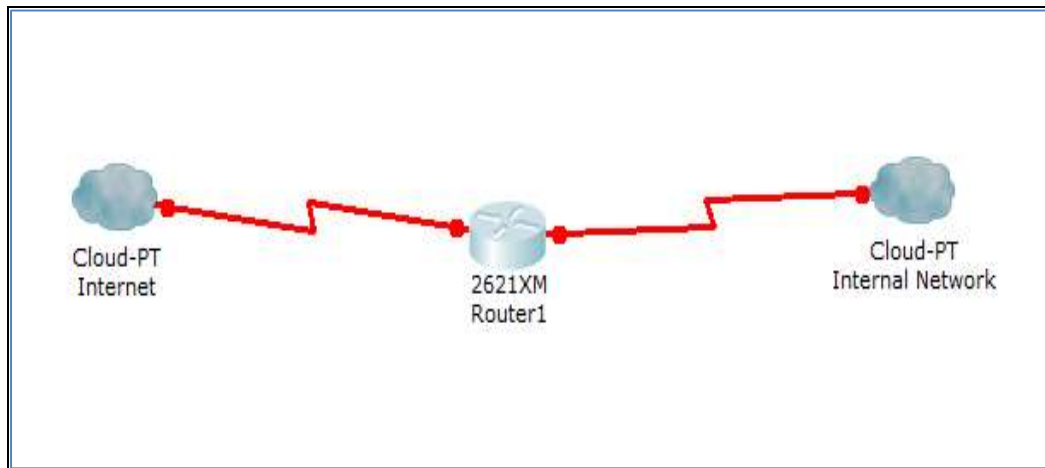


Figure 3: Border Router

5. MANAGE ROUTERS SECURITY

5.1 Password Setting

Basic router protection consists of password setup. The most fundamental factor in managing safe access to a router is a good password. Strong passwords should always be designed for this purpose[16].

5.2 Securing Router Administrative Access

Locally or remotely, network administrators may connect to a router. The preferred way for an administrator to link to a computer to handle it since it is safe is local access via the console port[17]. As businesses expand and the number of routers in the network increases, the workload of the administrator to connect locally to all the devices can become daunting. For administrators who have multiple devices to handle, remote administrative access is more convenient than local access. If it is not implemented securely, however sensitive confidential information may be collected by an intruder. The implementation of remote administrative access using Telnet. It's important for the successful management of a network to have remote access to network equipment. Usually, remote access includes supporting Telnet, SSH [18].

6. SYSTEM DESIGN AND RESULTS

In this section three steps was done to secure the router in easy way as follow:

6.1 Password Setting

As mentioned in section 5.1 that the password is the first step to secure a router. In this paper the Cisco packet Tracer has been used to configure the password for the router and the next topology has been used for the simulation.

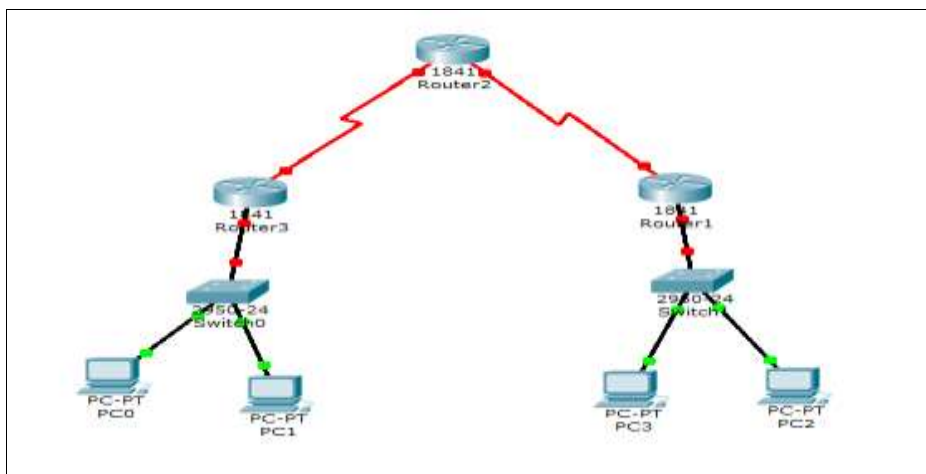


Figure 4: Topology

The passwords are set for console line and Virtual Terminal Line (VTY) for router 3 using the Command Line Interface (CLI) as shown in figure5.

The screenshot shows a terminal window titled 'Router3' with tabs for 'Physical', 'Config', and 'CLI'. The main area is titled 'IOS Command Line Interface'. The command history shows: Router>enable, Router#config t, Router(config)#host name Zliten (with an error message for an invalid character), Router(config)#hostname Zliten, Zliten(config)#line consol 0, Zliten(config-line)#password zliten, Zliten(config-line)#login, Zliten(config-line)#exit, Zliten(config)#line vty 0 4, Zliten(config-line)#password zliten, Zliten(config-line)#login, Zliten(config-line)#exit, Zliten(config)#exit, Zliten#, %SYS-5-CONFIG_I: Configured from console by console, Zliten#exit. There are 'Copy' and 'Paste' buttons at the bottom right.

```
Router3>enable
Router3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router3(config)#host name Zliten
^
% Invalid input detected at '^' marker.

Router3(config)#hostname Zliten
Zliten3(config)#line consol 0
Zliten3(config-line)#password zliten
Zliten3(config-line)#login
Zliten3(config-line)#exit
Zliten3(config)#line vty 0 4
Zliten3(config-line)#password zliten
Zliten3(config-line)#login
Zliten3(config-line)#exit
Zliten3(config)#exit
Zliten3#
%SYS-5-CONFIG_I: Configured from console by console
Zliten3#exit
```

Figure 5: Console and VTY password setting

By default, Cisco IOS program leaves passwords in plain text when they are entered on a router. As shown in the next figure the password was in plain text (password zliten).

The screenshot shows a terminal window titled 'Router3' with tabs for 'Physical', 'Config', and 'CLI'. The main area is titled 'IOS Command Line Interface'. The command history shows: interface FastEthernet0/1, no ip address, duplex auto, speed auto, shutdown, |, interface Serial0/0/0, no ip address, shutdown, |, interface Vlan1, no ip address, shutdown, |, ip classless, |, |, |, |, |, |, |, |, |, line con 0, password zliten, login, --More--. There are 'Copy' and 'Paste' buttons at the bottom right.

```
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
|
interface Serial0/0/0
no ip address
shutdown
|
interface Vlan1
no ip address
shutdown
|
ip classless
|
|
|
|
|
|
|
|
|
line con 0
password zliten
login
--More--
```

Figure 6: Password in Plain Text

That is why, all passwords should be encrypted in a configuration file. The following

instructions would be applied in configuration mode to encrypt the password as shown in figure 7.8. So here the previous password had been encrypted.

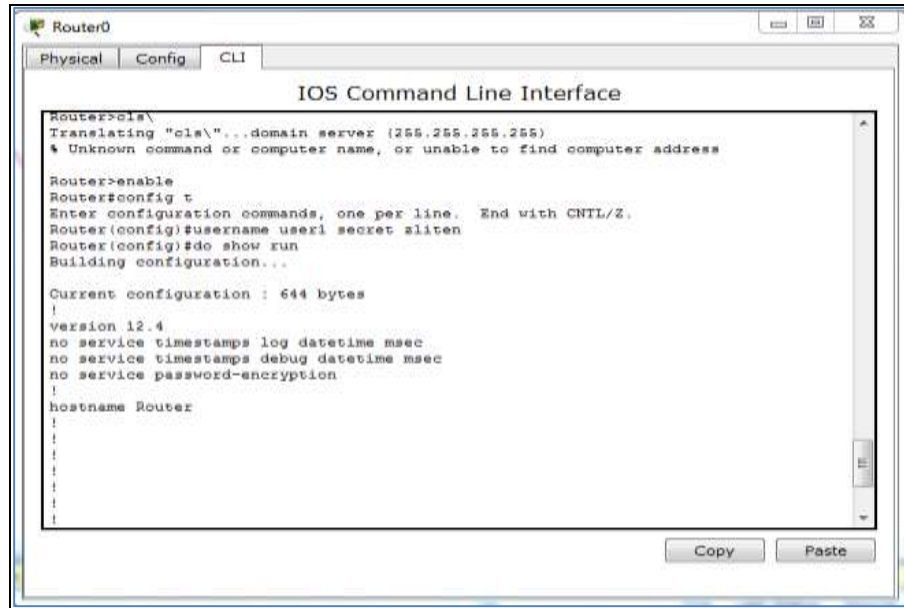


Figure 7: Setup the Encrypt Password

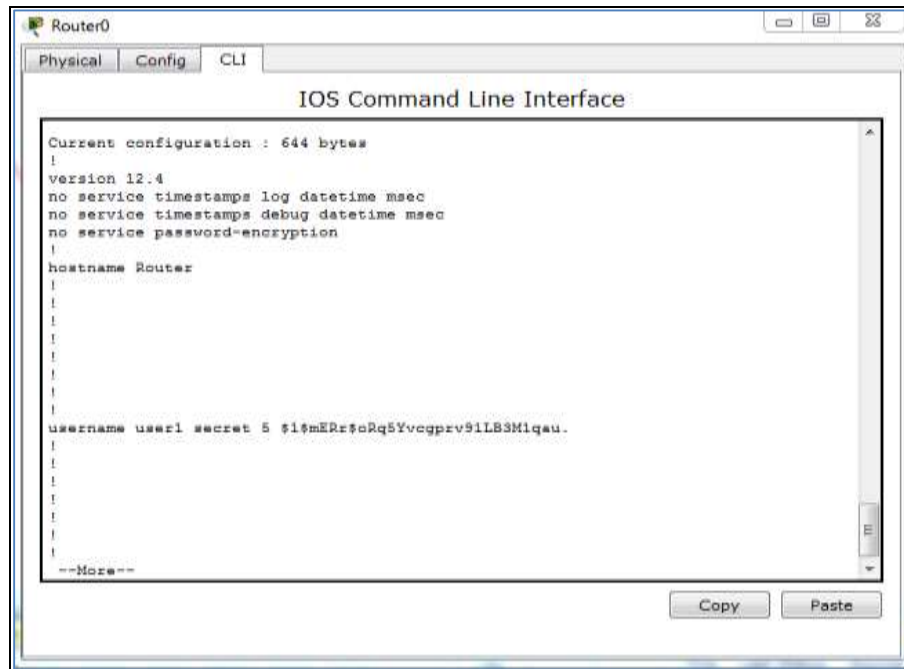


Figure 8: Encrypted Password

6.2 Securing Router Administrative Access

Administrators should ensure that logins on all lines, including devices that are supposed to be inaccessible from non-trusted networks, are managed using an



authentication mechanism. This is particularly important for VTY lines for remote access. Configuring the router by no password and no transport input commands with login will fully prevent logins on any side for VTYS.

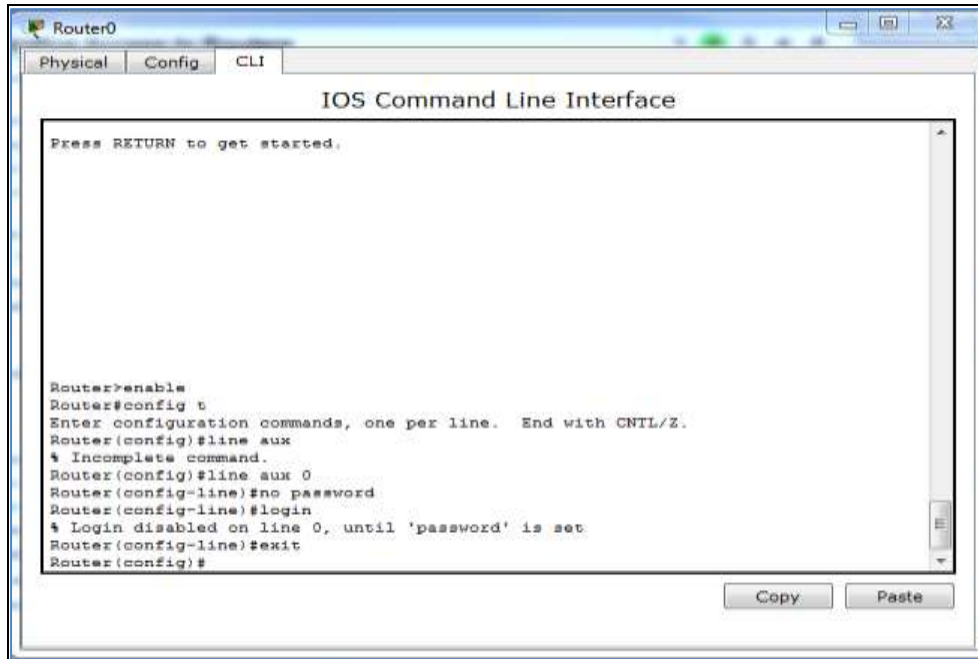


Figure 9: Configure the Ports idle

Usually in real world the routers are located in the server's room and for the configuration of the router that should be done in the server room. The laptop or a PC are used the proper cable which is the console cable and connect the cable to the serial port of the router . Using the following topology the Telnet and SSH were configured to secure a way to login to the router.

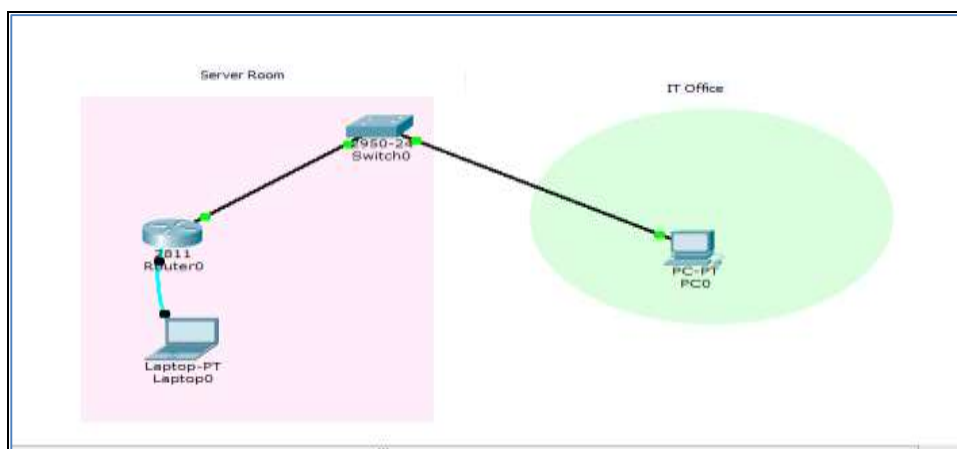
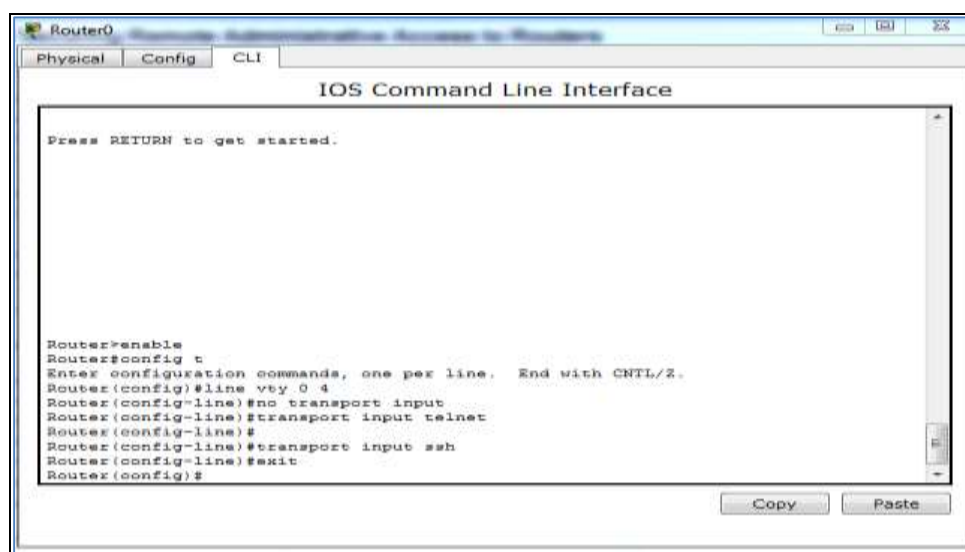


Figure 11: Topology

7. CONTROLLING VTYS

All VTY lines are configured by default to accept some form of remote link. VTY lines should be configured to allow connections only with the protocols currently required for security reasons. This is done with the input command for transportation, for example a VTY that only Telnet (port 23) sessions were supposed to receive would be configured with `transport input telnet`, and a VTY that would allow both Telnet and SSH (port 22) sessions would have configured `transport input telnet SSH` as shown in figure 12.

A screenshot of a Cisco Router0 CLI window showing the configuration of VTY lines. The window title is 'Router0' and it has tabs for 'Physical', 'Config', and 'CLI'. The main area is titled 'IOS Command Line Interface' and contains the following text:

```
Press RETURN to get started.  
  
Router#enable  
Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#line vty 0 4  
Router(config-line)#no transport input  
Router(config-line)#transport input telnet  
Router(config-line)#  
Router(config-line)#transport input ssh  
Router(config-line)#exit  
Router(config)#
```

At the bottom right of the window, there are 'Copy' and 'Paste' buttons.

Figure 12: Supports Incoming Telnet and SSH

Now the Router0 is able to accept the Telnet and SSH sessions from the PC0 which is located far away from the server room. The next configuration was done with the terminal configuration using `labtop0` by the way the same configuration could be done similar thing in the packet tracer directly click on the router and do the setting. Using the command prompt telnetting the router. PC0 which wants to connect with the router remotely would be asked for the two passwords as show in figure 13.

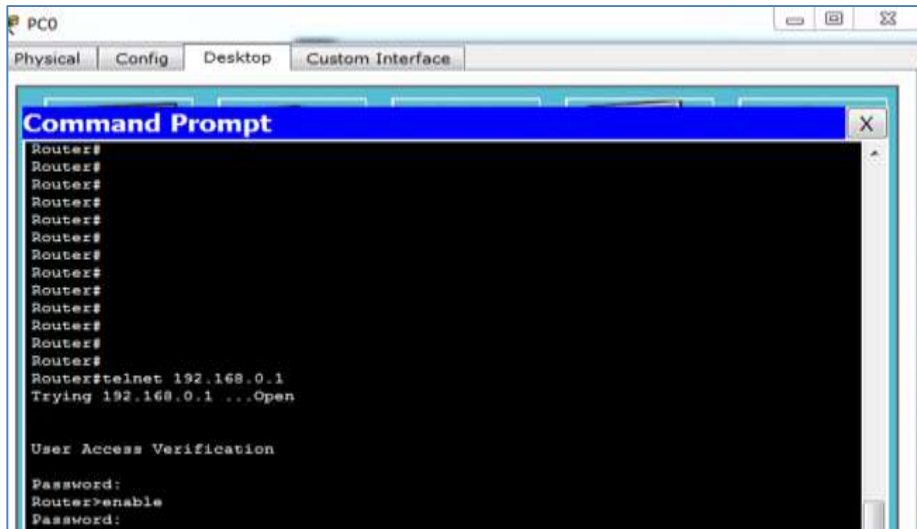


Figure 13: Telnet the Router

8. IMPLEMENTING SSH

As the best practice for providing remote router management with connections that respect good privacy and session integrity, SSH has replaced Telnet. The following steps showed setup SSH login:

- 1- **Set Parameters for Router** configure the hostname of the router from the configuration mode with the *hostname Libya* order.

- 2- **Set the name of the domain** to allow SSH, a domain name must exist. In this example, from the global configuration mode, enter the IP domain-name *zliten.net* command.

- 3- **Generate asymmetric keys** the key needs to be created that the router uses to encrypt its SSH management traffic with the *crypto key generate RSA* command from configuration mode. The router responds with a message showing the naming convention for the keys. Choose the size of the key modulus in the range of 360 to 2048 .and here the length of the key was 1024.

- 4- **Configure local authentication and VTY** Local user identified and assign the VTY lines to SSH communication.

The job is done in the router side. Now at PC0 in the IT office easily SSH in the secure way to the router. By typing SSH - L (for logging) ali (user name) 192.168.0.1(the target router) then the SSH connection is open. The password of the user has to be entered. SSH has used RSA public key cryptography to establish a secure connection between PC0 and



the router . Because connections are encrypted, passwords and other sensitive information are not exposed in clear text in the network. Finally the router under control remotely in secure way.

```
Router0
Physical Config CLI
IOS Command Line Interface
Router>en
Password:
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip domain-name zliten.net
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#hostname libya
libya(config)#crypto key generate rsa
The name for the keys will be: libya.zliten.net
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
libya(config)#username ali privilege 15 password ali
*???? 1 0:48:5.697: %SSH-5-ENABLED: SSH 1.99 has been enabled
libya(config)#line vty 0 4
libya(config-line)#login
libya(config-line)#login local
libya(config-line)#transport input ssh
libya(config-line)#exit
libya(config)#
```

Figure 15: Configure SSH on the Router



```
PCO
Physical Config Desktop Custom Interface
Command Prompt
User Access Verification
Password:
Router>enable
Password:
Router#do show run
^
% Invalid input detected at '^' marker.

Router#telnet 192.168.0.1
Trying 192.168.0.1 ...Open

User Access Verification
Password:
Router>en
Password:
Password:
libya#ssh -l ali 192.168.0.1
Open
Password:

libya#
```

Figure 16: SSH open Connection



9. CONCLUSION

Securing the routers is a critical role in securing a network. Routers are the network gateway and are obvious targets. Basic administrative discussions were started, including good physical protection, maintenance of modified IOS, and backup of configuration files. In order to harden routers and close doors opened by used ports and utilities, Cisco IOS software offers a variety of security features. It's important for the efficient management of a network to provide remote access to a network equipment. Remote administrative access is more convenient than local access for administrators who have multiple devices to deal. It can be very insecure to enforce remote administrative access using Telnet, as Telnet forwards all network traffic in plain text. Therefore, with additional security measures, remote administrative access needs to be configured with SSH. SSH makes it possible to communicate safely over an unreliable network. The Cisco packet tracer was used to use Telnet and SSH to remotely access the router. After seeing the simulations We conclude that SSH is more secure than Telnet in easy way.

10. REFERENCES

- [1] M. Ahmed, L. Sharif, A. Issa-Salwe, and A. Alharby, "Information security: securing a network device with passwords to protect information," *Trends Inf. Manag. TRIM*, vol. 6, no. 1, 2012.
- [2] F. M. Avolio, M. J. Ranum, and M. Glenwood, "A network perimeter with secure external access," 1994, pp. 109–119.
- [3] A. S. Tergeusizova and A. J. Toigojinova, "Router Security Issues," *Bull. Natl. Acad. Sci. Repub. KAZAKHSTAN*, no. 6, pp. 34–37, 2013.
- [4] F. Waheed and M. Ali, "Hardening CISCO Devices based on Cryptography and Security Protocols-Part II: Implementation and Evaluation," *Ann. Emerg. Technol. Comput. AETiC Print ISSN*, pp. 2516–0281, 2018.
- [5] C. Maurice *et al.*, "Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud.," in *NDSS*, 2017, vol. 17, pp. 8–11.
- [6] T. Ylonen, P. Turner, K. Scarfone, and M. Souppaya, "Security of interactive and automated access management using secure shell (ssh)," *NISTIR 7966 Natl. Inst. Stand. Technol.*, 2015.
- [7] D. Moore, G. M. Voelker, and S. Savage, "Proceedings of the 10th USENIX Security Symposium.," 2001.



- [8] Y. Fei, J. Jones, K. Lakkas, and Y. Zheng, "Measurement of the usage of several secure Internet protocols from Internet traces," *Stud. Proj. Dep. Comput. Sci. Eng. Univ. Calif. San Diego CA USA*, 2002.
- [9] P. McLaren, G. Russell, W. J. Buchanan, and Z. Tan, "Decrypting live SSH traffic in virtual environments," *Digit. Investig.*, vol. 29, pp. 109–117, 2019.
- [10] B. M. Onimode and K. J. Danjuma, "Issues And Challenges of Network Security In the Africa Environment," *Afr. J. Comput. ICT*, vol. 7, p. 5, 2014.
- [11] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era," *Int. J. Parallel Program.*, vol. 48, no. 2, pp. 280–295, 2020.
- [12] H. S. Hawedi, O. A. Bentaher, and K. E. Abodhir, "Using Access Control List against Denial of service attacks." *Journal of Economics and Political Science, Faculty of Economics and Commerce / Al-Asmariya Islamic University Issue 10: Dec.*, 2017.
- [13] V. Bontchev, D. Polimirova, V. Yosifova, and A. Inkov, "Results From Running An Ssh And Telnet Honeypot For A Year. СБОРНИК НАУЧНИ ТРУДОВЕ –ISBN 978-954-9681-89-5 ИС 2018.
- [14] Omran Ali Bentaher¹, Hadya S. Hawedi², Kaled E. I. Abodhir³, "Comparative Study of The Impact of Dos Attacks on Lans Using Vlans," vol. 5, no. Volume (5) Issue 1, pp. 88–105, Jun. 2020, [Online]. Available: http://www.asmarya.edu.ly/journal/wp-content/uploads/2020/12/JAU.BA_.June2020-6.pdf.
- [15] R. El Saadany, "Lock-and-key security: evaluation of Telnet as an authentication method usually associated with dynamic access control lists application," 2013.
- [16] Y.-N. Su, G.-H. Chung, and B. J. Wu, "Developing the upgrade detection and defense system of SSH dictionary-attack for multi-platform environment," *J IBusiness*, vol. 3, no. 1, pp. 65–70, 2011.
- [17] F. Bergsma, B. Dowling, F. Kohlar, J. Schwenk, and D. Stebila, "Multi-ciphersuite security of the Secure Shell (SSH) protocol," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 369–381.
- [18] M. Bala and H. Rohil, "Design And Implementation Of Mobile To Pc Ssh Protocol. IJREISS,2012.



الوصول عن بعد لجهاز التوجيه باستخدام SSH بأمان

هدية سليمان هويدي*

عمران علي بن طاهر**

خالد احمد ابو ظهير***

الملخص:

تعتبر أجهزة التوجيه في شبكة الكمبيوتر مسؤولة عن إدارة الكثير من تدفق البيانات. لذلك، من المهم تكوين أجهزة التوجيه بشكل صحيح، حيث سيساعد ذلك على مقاومة الهجمات والحفاظ على أمان وسرية حركة مرور الشبكة. استخدام Telnet للوصول إلى جهاز توجيه عن بُعد ليس آمنًا بدرجة كافية. الهدف من هذا البحث هو إثبات أن استخدام بروتوكول غلاف المقبس الآمن (SSH) لتسجيل الدخول عن بُعد إلى جهاز توجيه أكثر أمانًا. تم استخدام محاكاة تتبع حزم سيسكو لتكوين جهاز التوجيه. أظهرت المحاكاة أن SSH يوفر مصادقة قوية وتشفيرًا، ويحافظ على سرية وخصوصية الاتصالات.

الكلمات الرئيسية: جهاز التوجيه، الوصول عن بعد، Telnet، SSH، الأمان، VTY

*كلية تقنية المعلومات الجامعة الأسمرية الإسلامية زليتن hadia20008@asmarya.edu.ly

**المعهد العالي للعلوم والتقنية زليتن omalbeta@yahoo.com

***كلية العلوم الجامعة الأسمرية الإسلامية زليتن k.abodhir@asmarya.edu.ly