

Prácticas de laboratorio: **Criptografía (SSH)**

Para la Unidad de Aprendizaje “Seguridad en redes”

Versión 1.0 (Septiembre 2016)

Datos de identificación

Programa educativo:	Licenciatura en Ingeniería en computación
Programa de estudios por competencias :	Seguridad en redes
Unidad de competencia 3:	Criptografía y autenticación
Subtemas	SSH
Créditos de la Unidad de Aprendizaje:	9
Espacio académico en que se imparte la UA:	CU UAEM Valle de Chalco

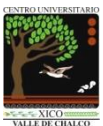
Elaborado por:

Autor: Maestro. Rodolfo Melgarejo Salgado
Coautor: Maestra. Marisol Hernández Hernández
Coautor: Maestro. Francisco Raúl Salvador Gínez

Fecha: Septiembre de 2016

INDICE

PRESENTACIÓN	3
PROPÓSITO DE LA UNIDAD DE APRENDIZAJE	4
ESTRUCTURA DE LA UNIDAD DE APRENDIZAJE	4
Práctica de laboratorio: 1 Configuración de SSH (Universidades)	5
Práctica de laboratorio: 2 SSH con Frame Relay Point-to-point	11
Práctica de laboratorio: 3 SSH en redes LAN y WAN	16
Práctica de laboratorio: 4 SSH en routers	20
Práctica de laboratorio: 5 SSH con VLAN	23
Referencias	26



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

PRESENTACIÓN

Tradicionalmente, el acceso remoto en los routers era mediante telnet. Sin embargo, telnet se desarrolló en los días en que la seguridad no era un problema. Por esta razón, todo el tráfico de telnet se envía en texto plano. Si el atacante captura el flujo de telnet, podrá conocer el nombre de usuario y la contraseña del administrador.

SSH ha sustituido a telnet con conexiones que soportan privacidad y la integridad de la sesión. SSH proporciona una funcionalidad similar a la de una conexión de telnet, excepto que la conexión está **encriptada**. Con la **autenticación** y el **cifrado**, SSH permite las comunicaciones seguras a través de una red insegura.

Este manual de prácticas de laboratorio fueron desarrolladas en estricto apego a la unidad de competencia 3, cabe mencionar que el tema de **Criptografía y autenticación** tiene un amplio espectro de protocolos y de algoritmos, de tal forma que en este documento se abordará el subtema de **SSH (Secure Shell)**, el cual es un protocolo de aplicación incluido en algunos programas tales como el PuTTY, OpenSSH, TeraTerm entre otros. Este protocolo **hace uso del algoritmo de encriptación y claves RSA** (Rivest, Shamir y Adleman). **Las próximas prácticas de laboratorio** serán sobre la **autenticación PAP** y **CHAP** con el protocolo PPP, así como la **autenticación local** y basada en servidores como es el caso de **RADIUS** y **TACACS+**

La estructura y secuencia de las 5 prácticas son coherentes con el programa de la Unidad de Aprendizaje “SEGURIDAD EN REDES”, aunado a lo mencionado anteriormente, la secuencia y complejidad de las practicas es congruente con la UA.

Finalmente, es importante mencionar, que estas prácticas se implementaron a los alumnos de noveno semestre del CU UAEM Valle de Chalco de la licenciatura de Ingeniería en Computación durante los periodos 2014B y 2015B.



Prácticas de laboratorio Criptografía “SSH”

El algoritmo **MD5** fue desarrollado por **Ron Rivest**

```
19811: 896ba_41d4c1ca_Abe11_2014
19811: 6e09f0ab69e768ea3c3e5f8f4f7bb6f9
19811: 4b4d2d1b9b819e353601e6af42616a7ab28cf80c
19824: 88679b2bb1883fc0ca025b4d368b9ecf81f331bc2251c1cb8e3d5acf632f0e67
```

El algoritmo encriptación asimétrico **RSA** fue desarrollado por **Rivest, Shamir y Adleman**

DH es un protocolo criptográfico asimétrico Publicado por Whitfield **Diffie** y Martin **Hellman** en 1976

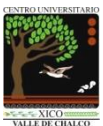


PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Que los alumnos sean capaces de realizar el diseño, implementación y el mantenimiento de la seguridad de distintas redes computacionales.

ESTRUCTURA DE LA UNIDAD DE APRENDIZAJE

1. Fundamentos de la seguridad en redes.
2. Arquitectura de seguridad del modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection).
3. **Criptografía** y autenticación.
4. Arquitecturas de componentes de seguridad (Firewalls, IDS, Analizadores de contenido).
5. Hardening a servidores y dispositivos de red.



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

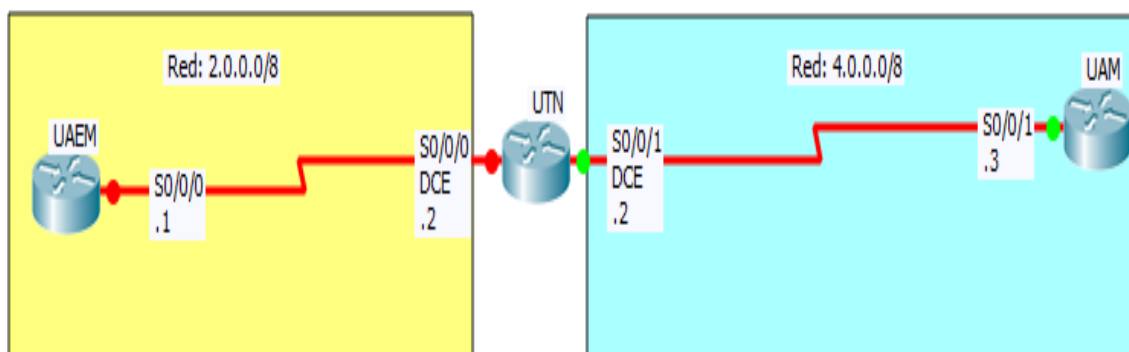
Página: <http://cux.uaemex.mx>

Academia de Redes



Práctica de laboratorio: 1 Configuración de SSH (Universidades)

Duración de la práctica: 50 minutos



Escenario a configurar

Procuren llegar al 100%
SUERTE!!!!

Objetivos de aprendizaje:

- Configurar el router UAEM
- Habilitar SSH en el router UAEM
- Accesar remotamente a los routers UAM y UTN vía SSH

Material y equipo a utilizar:

Para la realización de esta práctica son necesarios los siguientes componentes:

- Hojas
- Lápiz o Bolígrafo
- Packet Tracer versión 6.0.1.0011 o superior

Introducción

Telnet

Tradicionalmente, el acceso remoto en los routers era mediante Telnet.

Sin embargo, Telnet se desarrolló en los días en que la seguridad no era un problema. Por esta razón, todo **el tráfico de Telnet se envía en texto plano**.

Si el atacante captura el flujo de Telnet, podrá conocer el nombre de usuario y la contraseña del administrador.

SSH

SSH ha sustituido a Telnet con conexiones que soportan privacidad y la integridad de la sesión.

SSH Proporciona una funcionalidad similar a la de una conexión de Telnet, excepto que la conexión está **encriptada**.

Con la autenticación y el cifrado, SSH permite las comunicaciones seguras a través de una red insegura.

En resumen, SSH:

- Secure Shell (Interprete de ordenes)
- Es un protocolo de capa de aplicación
- Viene incluido en algunos programas (PuTTY, OpenSSH, TeraTerm...)
- Utiliza el puerto 22
- Sirve para acceder remotamente a equipos a través de la red. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.
- Utiliza claves RSA



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes



Requisitos previos antes de configurar SSH en routers Cisco.

Deben completarse cuatro pasos [antes de configurar un router para el protocolo SSH](#):

- Paso 1. Asegurarse de que los routers destino estén ejecutando una [imagen del IOS de Cisco release 12.1\(1\)T o posterior, para que soporten SSH](#).

Solo las [imágenes criptográficas del IOS de Cisco](#) que contienen el grupo de funciones IPsec soportan SSH.

Específicamente, las imágenes criptográficas del IOS de Cisco 12.1 o la posterior

[IPsec DES o el Triple Data Encryption Standard \(3DES\)](#) soportan SSH.

Estas imágenes generalmente tienen el **ID k8 o k9** en su nombre de imagen.

Por ejemplo, **c1841-advipservicesk9-mz.124-10b.bin** es una imagen que soporta SSH.

- Paso 2. Asegurarse de que cada uno de los routers destino tenga un [nombre de host único](#).
- Paso 3. Asegurarse de que cada router destino esté usando el [nombre de dominio correcto para la red](#).
- Paso 4. Asegurarse de que los routers destino estén configurados para [autenticación local o servicios AAA para autenticación de usuario y contraseña](#).

Versiones de SSH

SSHv1

* Creado por el finlandés Tatu Ylönen (UT de Helsinki)

* En 1995

* Hace uso de algoritmos de encriptación patentados

* Es vulnerable

SSHv2

* Creado en 1997

* Más segura que SSHv1.

* SSHv2 proporciona mejor seguridad usando el intercambio de claves Diffie-Hellman y el código de autenticación de mensajes (message authentication code - MAC) de fuerte revisión de integridad.

Los routers Cisco soportan dos versiones de SSH

El IOS de Cisco Release [12.1\(1\)T](#) y posteriores soportan SSHv1.

El IOS de Cisco Release [12.3\(4\)T](#) y posteriores operan en modo de compatibilidad y soportan tanto SSHv1 como SSHv2.

Comandos opcionales en SSH

Opcionalmente, pueden usarse comandos SSH para configurar lo siguiente:

Versión SSH: [ip ssh version {1 | 2}](#)

Período de vencimiento de sesión SSH (Tiempo de tolerancia de sesión desatendida): [ip ssh time-out 45](#)

Número de reintentos de autenticación: [ip ssh authentication-retries 2](#)

RSA

1. Rivest, Shamir y Adleman
2. Sistema criptográfico de clave pública
3. Desarrollado en 1977 y patentado por el MIT en 1983
4. Es utilizado para cifrar y firmar digitalmente.
5. Los mensajes enviados se representan mediante números elegidos al azar 10^{200}

A continuación se presenta un resumen de los algoritmos de encriptación

packetlife.net			
Encryption Algorithms			
	Type	Key Length (Bits)	Strength
DES	Symmetric	56	Weak
3DES	Symmetric	168	Medium
AES	Symmetric	128/192/256	Strong
RSA	Asymmetric	1024+	Strong



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes



Desarrollo

Indicaciones

En la barra de menu del Packet Tracert seleccionar **Options**

Elegir la opción de **Preferences... o Ctrl+R**

En la pestaña de **Interface**

Deshabilitar las opciones de:

Show Device Model Label

Show Device Name Model

En esta configuración, se tienen tres routers, los cuales tienen el protocolo de enrutamiento dinámico **RIP versión 1**.

La UAEM ha adquirido un router de la 1841 con el sistema operativo c1841-advipservicesk9-mz.124-15.T1.bin

Los routers UTN y UAM ya están configurados previamente

Tarea 1. Configurar el router UAEM

Paso 1. Para la configuración básica, digite los siguientes comandos:

enable

configure terminal

hostname UAEM

no ip domain-lookup

interface s0/0/0

no shutdown

ip address 2.0.0.1 255.0.0.0

exit

router rip

network 2.0.0.0

end

Paso 2. Para la configuración de TELNET, digite los siguientes comandos:

enable

configure terminal

hostname UAEM

enable **secret** UAEM

line vty 0 4

password UAEM

login

end

Paso 3. Verificar conectividad con los routers UTN y UAM

Desde el router UAEM digite los siguientes comandos

ping 4.0.0.3

ping 4.0.0.2

telnet 4.0.0.3

Password: **UAM**

telnet 4.0.0.2

Password: **UTN**

Paso 4. Verifique las tablas de enrutamiento.

Desde el modo EXEC privilegiado en los tres routers, ejecute el comando **show ip route** para verificar los todos los segmentos de la red se anuncian.



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes



Tarea 2: Configurar SSH en el router UAEM

Para habilitar SSH en el router, los siguientes parámetros deben ser configurados:

- Hostname
- Domain name
- Asymmetrical keys
- Local authentication
- ip domain-name

Paso 1. Escriba los siguientes comandos en el router UAEM.

```
enable
configure terminal
hostname UAEM
ip domain-name universidad.edu.mx ----- Nombre del dominio
crypto key generate rsa ----- Llave RSA Asimétrica
```

Cuando se pida un tamaño de módulo, especifique un módulo de 1024 bits.

El módulo determina el tamaño de la clave RSA y puede ser configurado de 360 bits a 2048 bits.

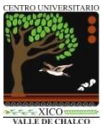
Cuanto más grande sea el módulo, más segura será la clave RSA.

Sin embargo, las claves con valores de módulo grandes toman más tiempo para ser generadas y para cifrarse y descifrarse.

La longitud mínima de clave módulo recomendada es de 1024 bits.

```
1024 ----- Longitud recomendada de la llave RSA Asimétrica
username admin password cisco ----- Autenticación local
ip ssh version 2 ----- Habilita SSHv2
ip ssh authentication-retries 2 ----- Intentos de autenticación 0--5
ip ssh time-out 45 ----- Tiempo de tolerancia de sesión desatendida 1--120
```

```
line vty 0 4
no transport input all ----- Deshabilita telnet
transport input ssh ----- Habilita ssh
login local ----- Autenticación local
end
```



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes



Tarea 3: Verificar conexiones seguras con SSH

Paso 1. Antes, se debe verificar si existe comunicación via TELNET entre los routers.

Desde el router UAEM, intente conectarse via Telnet al router UAM.

telnet 4.0.0.3

Trying 4.0.0.3 ...

[Connection to 4.0.0.3 closed by foreign host]

Desde el router UAEM, intente conectarse via Telnet al router UTN.

telnet 4.0.0.2

Trying 4.0.0.2 ...

[Connection to 4.0.0.2 closed by foreign host]

¿Se pudo establecer conexión remota por medio de Telnet? _____

Recordemos que fue desactivado Telnet utilizando la entrada de ningún medio de transporte.

Sólo SSH se puede utilizar para establecer una conexión remota.

Paso 2. Verificar que existe comunicación vía SSH entre los routers.

Digitar los siguientes comandos para conectarse al router UAM

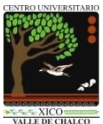
ssh -l admin 4.0.0.3

Password: **cisco**

Digitar los siguientes comandos para conectarse al router UTN

ssh -l admin 4.0.0.2

Password: **cisco**



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes



Conclusiones

Referencias

- Ariganello, Ernesto (2013).
Redes Cisco. Guía de estudio para la certificación CCNA Security.
Editorial Alfaomega. ISBN 978-607-707-654-4
- Barker, K y Morris, S. (2012).
CCNA Security 640-554 Official Cert Guide.
Editorial Cisco Press
- Cisco. (2005).
Fundamentos de seguridad de redes.
Editorial Cisco Press. ISBN: 84-205-4540-6
- Andrew G. Manson. (2002).
Redes privadas virtuales de Cisco Secure.
Editorial Cisco Press. ISBN: 84-205-3618-0
- Vachon, B., y **Graziani, R.** (2009).
Acceso a la WAN Guía de Estudio CCNA Exploration.
Editorial Cisco Press.
- **Graziani, R.** y Johnson, A (2008).
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
Cisco Press. ISBN 978-84-8322-472-4.
- IPSec. Recuperado el 28 de agosto del 2016 de:
<http://packetlife.net/library/cheat-sheets/>

Capturar la imagen donde se muestre su porcentaje de avance.

Recomiendo que dicha captura de imagen sea faltando 30 segundos antes de que expire su tiempo

**GRACIAS
TOTALES**

Criterios de evaluación

Activity Results Time Left: 00:49:25

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
DNS				
IP Domain-Lookup	Correct	0	Other	
Enable Secret	Correct	1	Other	
Host Name	Correct	1	Other	
IP Domain Name	Correct	1	Other	
Ports				
Serial0/0/0				
IP Address	Correct	1	Ip	
Subnet Mask	Correct	1	Ip	
RIP				
Networks	Correct	0	Routing	
Route0	Correct	1	Routing	
SSH Server				
SSH Authentication Retries	Correct	1	Other	
SSH Timeout	Correct	1	Other	
SSH Version	Correct	1	Other	
VTY Lines				
VTY Line 0				
Password	Correct	1	Other	
Transport Input	Correct	1	Physical	
VTY Line 1				
Password	Correct	1	Other	
Transport Input	Correct	1	Physical	
VTY Line 2				
Password	Correct	1	Other	
Transport Input	Correct	1	Physical	
VTY Line 3				
Password	Correct	1	Other	
Transport Input	Correct	1	Physical	
VTY Line 4				
Password	Correct	1	Other	
Transport Input	Correct	1	Physical	

Score : 20/20
Item Count : 20/20

Component	Items/Total	Score
Ip	2/2	2/2
Other	12/12	12/12
Physical	5/5	5/5
Routing	1/1	1/1



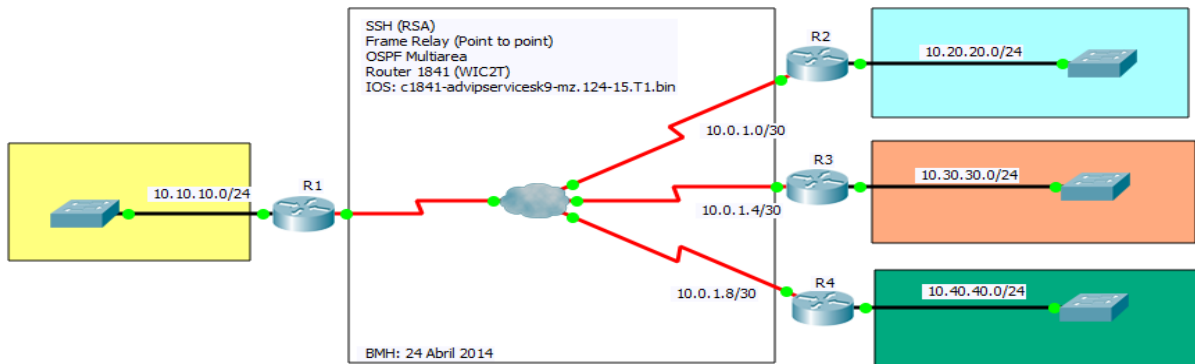
Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.
Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Práctica de laboratorio: 2 SSH con Frame Relay Point-to-point

Duración de la práctica: 50 minutos



Escenario a configurar

Procuren llegar al 100%
SUERTE!!!!

Objetivos de aprendizaje:

- Ver la configuración predeterminada
- Configurar SSH en R1
- Verificar conexiones seguras con SSH

Material y equipo a utilizar:

Para la realización de esta práctica son necesarios los siguientes componentes:

- Hojas
- Lápiz o Bolígrafo
- Packet Tracer versión 6.0.1.0011 o superior

Desarrollo

Indicaciones

En la barra de menú del Packet Tracer seleccionar **Options**

Elegir la opción de **Preferences...** o **Ctrl+R**

En la pestaña de **Interface**

Deshabilitar las opciones de:

Show Device Model Label

Show Device Name Model

En esta configuración, se tienen cuatro routers, los cuales están interconectados en una red de **Frame Relay**.

El router R1 es el centro, los routers R2, R3 y R4 son los radios.

El enrutamiento dinámico se ha configurado utilizando **OSPF multiárea**.



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Tarea 1. Ver la configuración predeterminada

Paso 1. Verifique la configuración de Frame Relay en los routers

- En los cuatro routers, entre al modo EXEC usuario con la contraseña **cisco**
- Entre en el modo EXEC privilegiado con la contraseña **cisco**
- Desde el modo EXEC privilegiado en los cuatro routers, ejecute el comando **show frame-relay map** para verificar la conectividad de Frame Relay.

Paso 2. Verifique las tablas de enrutamiento.

Desde el modo EXEC privilegiado en los cuatro routers, ejecute el comando **show ip route** para verificar los todos los segmentos de la red se anuncian.

Paso 3. Verificar la conectividad entre los routers.

- Desde R1, haga ping a todas las interfaces LAN para comprobar la conectividad.

```
ping 10.20.20.1
ping 10.30.30.1
ping 10.40.40.1
```

- Una vez más, desde el router R1, conectarse via Telnet a R2 y salir. Repita el paso para los routers R3 y R4.

```
telnet 10.20.20.1
Password: cisco
exit
```

```
telnet 10.30.30.1
Password: cisco
exit
```

```
telnet 10.40.40.1
Password: cisco
exit
```

Tarea 2: Configurar SSH en R1

Para habilitar SSH en el router, los siguientes parámetros deben ser configurados:

- Hostname
- Domain name
- Asymmetrical keys
- Local authentication

Paso 1. Escriba los siguientes comandos en R1.

```
enable
configure terminal
hostname R1
ip domain-name cisco.com ----- Nombre del dominio
crypto key generate rsa ----- Llave RSA Asimétrica
```

Cuando se pida un tamaño de módulo, especifique un módulo de 1024 bits.

El módulo determina el tamaño de la clave RSA y puede ser configurado de 360 bits a 2048 bits.

Cuanto más grande sea el módulo, más segura será la clave RSA.

Sin embargo, las claves con valores de módulo grandes toman más tiempo para ser generadas y para cifrarse y descifrarse.

La longitud mínima de clave módulo recomendada es de 1024 bits.

```
1024 ----- Longitud recomendada de la llave RSA Asimétrica
username admin password cisco ----- Autenticación local
ip ssh version 2 ----- Habilita SSHv2
line vty 0 4
no transport input all ----- Deshabilita telnet
transport input ssh ----- Habilita ssh
login local ----- Autenticación local
end
```

Paso 2. Repita los comandos del paso 1 en los routers R2, R3 y R4



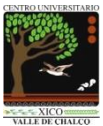
Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes





Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Tarea 3: Verificar conexiones seguras con SSH

Paso 1. Antes, se debe verificar que si existe comunicación via TELNET entre los routers.
Desde el router R1, conectarse via Telnet a R2. Repita el paso para los routers R3 y R4.

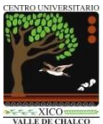
```
telnet 10.20.20.1
Trying 10.20.20.1 ...
[Connection to 10.20.20.1 closed by foreign host]
```

```
telnet 10.30.30.1
Trying 10.30.30.1 ...
[Connection to 10.30.30.1 closed by foreign host]
```

```
telnet 10.40.40.1
Trying 10.40.40.1 ...
[Connection to 10.40.40.1 closed by foreign host]
```

¿Se pudo establecer conexión remota por medio de Telnet ? _____
Recordemos que fue desactivado Telnet utilizando la entrada de ningún medio de transporte.
Sólo SSH se puede utilizar para establecer una conexión remota.

Paso 2. Verificar que existe comunicación via SSH entre los routers.
Usando R1 como el cliente SSH, digitar el siguiente comando para conectarse a R2
ssh -l admin 10.20.20.1
Password: **cisco**



Conclusiones

Referencias

- Ariganello, Ernesto (2013).
Redes Cisco. Guía de estudio para la certificación CCNA Security.
Editorial Alfaomega. ISBN 978-607-707-654-4
- Barker, K y Morris, S. (2012).
CCNA Security 640-554 Official Cert Guide.
Editorial Cisco Press
- Cisco. (2005).
Fundamentos de seguridad de redes.
Editorial Cisco Press. ISBN: 84-205-4540-6
- Andrew G. Manson. (2002).
Redes privadas virtuales de Cisco Secure.
Editorial Cisco Press. ISBN: 84-205-3618-0
- Vachon, B., y **Graziani, R.** (2009).
Acceso a la WAN Guía de Estudio CCNA Exploration.
Editorial Cisco Press.
- **Graziani, R.** y Johnson, A (2008).
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
Cisco Press. ISBN 978-84-8322-472-4.
- IPSec. Recuperado el 28 de agosto del 2016 de:
<http://packetlife.net/library/cheat-sheets/>

Capturar la imagen donde se muestre su porcentaje de avance.

Recomiendo que dicha captura de imagen sea faltando 30 segundos antes de que expire su tiempo

**GRACIAS
TOTALES**

Criterios de evaluación

Assessment Items	Status	Points	Component(s)	Feedback
R1				
IP Domain Name	Incorrect	1	Other	
SSH Server	Incorrect	0	Other	
SSH Version	Incorrect	1	Other	
VTY Lines				
VTY Line 0	Incorrect	0	Physical	
VTY Line 1	Incorrect	0	Physical	
VTY Line 2	Incorrect	0	Physical	
VTY Line 3	Incorrect	0	Physical	
VTY Line 4	Incorrect	0	Physical	
R2				
IP Domain Name	Incorrect	1	Other	
SSH Server	Incorrect	0	Other	
SSH Version	Incorrect	1	Other	
VTY Lines				
VTY Line 0	Incorrect	0	Physical	
VTY Line 1	Incorrect	0	Physical	
VTY Line 2	Incorrect	1	Physical	
VTY Line 3	Incorrect	0	Physical	
VTY Line 4	Incorrect	1	Physical	
R3				
IP Domain Name	Incorrect	1	Other	
SSH Server	Incorrect	0	Other	
SSH Version	Incorrect	1	Other	
VTY Lines				
VTY Line 0	Incorrect	0	Physical	
VTY Line 1	Incorrect	1	Physical	
VTY Line 2	Incorrect	0	Physical	
VTY Line 3	Incorrect	0	Physical	
VTY Line 4	Incorrect	1	Physical	
R4				
IP Domain Name	Incorrect	1	Other	
SSH Server	Incorrect	0	Other	
SSH Version	Incorrect	1	Other	
VTY Lines				
VTY Line 0	Incorrect	0	Physical	
VTY Line 1	Incorrect	1	Physical	
VTY Line 2	Incorrect	0	Physical	
VTY Line 3	Incorrect	1	Physical	
VTY Line 4	Incorrect	0	Physical	

Component	Items/Total	Score
Other	0/0	0/0
Physical	0/20	0/20



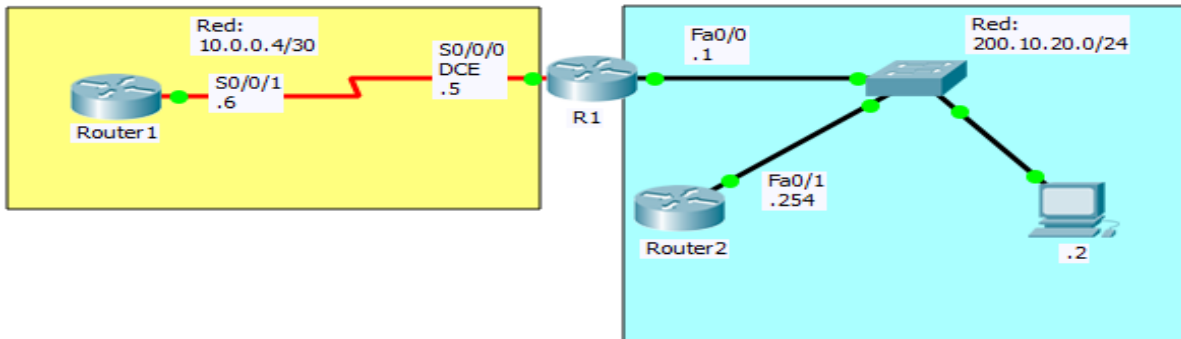
Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.
Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Práctica de laboratorio: 3 SSH en redes LAN y WAN

Duración de la práctica: 55 minutos



Escenario a configurar

Procuren llegar al 100%
SUERTE!!!!

Objetivos de aprendizaje:

- Configurar lo necesario para realizar un acceso de terminal virtual usando SSH (Secure Shell).
- Configurar adicionalmente diferentes puntos de entrada para probar el uso de SSH.

Material y equipo a utilizar:

Para la realización de esta práctica son necesarios los siguientes componentes:

- Hojas
- Lápiz o Bolígrafo
- Packet Tracer versión 6.0.1.0011 o superior

Desarrollo

Indicaciones

En la barra de menu del Packet Tracer seleccionar **Options**

Elegir la opción de **Preferences... o Ctrl+R**

En la pestaña de **Interface**

Deshabilitar las opciones de:

Show Device Model Label

Show Device Name Model

Configuración de interfaces en Router0 para luego realizar pruebas de entrada SSH por terminal virtual.

Interfaz FastEthernet 0/0:

Dirección IP: 200.10.20.1

Máscara de red: 255.255.255.0

Interfaz serial 0/0/0:

ip address 10.0.0.5 255.255.255.252

clock rate 64000

no shutdown

exit



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Direccionamiento IP en otros equipos de red de la topología:

Equipo	Interfaz	Dirección IP	Máscara de red	Puerta de enlace (Default Gateway)
Router1	Serial 0/0/1	10.0.0.6	255.255.255.252	N/A
Router2	FastEthernet 0/1	200.10.20.254	255.255.255.0	N/A
PC0	FastEthernet	200.10.20.2	255.255.255.0	200.10.20.1

Realizar las conexiones de red de acuerdo a la siguiente tabla:

Equipo	Interfaz	Conectado con:
Router0	S0/0/0 (DCE)	s0/0/1 de Router1
Router2	Fa0/1	cualquier puerto de Switch0
PC0	Fa	cualquier puerto de Switch0

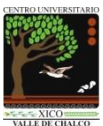
Configuración SSH en Router0.

```
hostname R1
ip domain-name utn.edu
crypto key generate rsa
(en este punto se te preguntará el tamaño de la clave la cual definirás a 1024)

username control secret admssh
line vty 0 4
login local
transport input ssh
exit
```

Desde Router1, Router2 y PC0 ejecuta el comando: `ssh -l control direccion_ip`
 Donde direccion_ip será la dirección ip más cercana de Router0 según el equipo donde realices la prueba.

Desde Router1 ssh -l control 10.0.0.5 password: admssh	Desde Router2 ssh -l control 200.10.20.1 password: admssh	Desde PC0 ssh -l control 200.10.20.1 password: admssh	Desde R1 sh ssh
--	---	---	--------------------



```

ena
conf t
hostname R1
int fa 0/0
ip add 200.10.20.1 255.255.255.0
no shut
exit

interface serial 0/0/0
ip address 10.0.0.5 255.255.255.252
clock rate 64000
no shutdown
exit

```

ip domain-name utn.edu

crypto key generate rsa

! (en este punto se te preguntará el tamaño de la clave la cual definirás a **1024**)

username control secret admssh

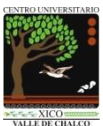
line vty 0 4

login local

transport input ssh

end

<pre> ena conf t hostname Router1 int s0/0/1 ip add 10.0.0.6 255.255.255.252 no shut exit !Para que haya conectividad TOTAL ip route 0.0.0.0 0.0.0.0 s0/0/1 end </pre>	<pre> ena conf t hostname Router2 int fa0/1 ip add 200.10.20.254 255.255.255.0 no shut !Para que haya conectividad TOTAL ip route 0.0.0.0 0.0.0.0 fa0/1 end </pre>
---	---



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Conclusiones

Referencias

- Ariganello, Ernesto (2013).
Redes Cisco. Guía de estudio para la certificación CCNA Security.
Editorial Alfaomega. ISBN 978-607-707-654-4
- Barker, K y Morris, S. (2012).
CCNA Security 640-554 Official Cert Guide.
Editorial Cisco Press
- Cisco. (2005).
Fundamentos de seguridad de redes.
Editorial Cisco Press. ISBN: 84-205-4540-6
- Andrew G. Manson. (2002).
Redes privadas virtuales de Cisco Secure.
Editorial Cisco Press. ISBN: 84-205-3618-0
- Vachon, B., y **Graziani, R.** (2009).
Acceso a la WAN Guía de Estudio CCNA Exploration.
Editorial Cisco Press.
- **Graziani, R.** y Johnson, A (2008).
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
Cisco Press. ISBN 978-84-8322-472-4.
- IPSec. Recuperado el 28 de agosto del 2016 de:
<http://packetlife.net/library/cheat-sheets/>

Capturar la imagen donde se muestre su porcentaje de avance.
Recomiendo que dicha captura de imagen sea faltando 30 segundos antes de que expire su tiempo

**GRACIAS
TOTALES**

Criterios de evaluación

Activity Results Time Elapsed: 00:00:26

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
Router				
SSH Server				
SSH Authentication Retries	Correct	1	Other	
SSH Timeout	Correct	1	Other	
SSH Version	Correct	1	Other	

Score : 3/3
Item Count : 3/3

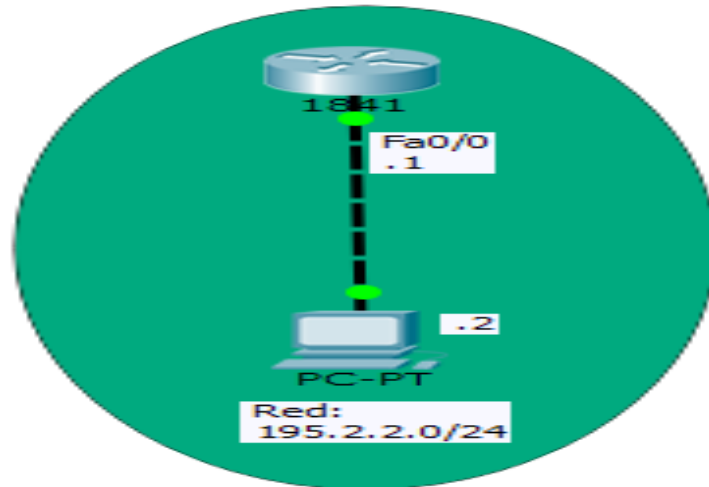
Component	Items/Total	Score
Other	3/3	3/3



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.
Tel: (55) 59714940, 59787577 y 30921763
Página: <http://cux.uaemex.mx>
Academia de Redes

Práctica de laboratorio: 4 SSH en routers

Duración de la práctica: 30 minutos



Escenario a configurar

Procuren llegar al 100%
SUERTE!!!!

Objetivos de aprendizaje:

- Configurar en forma básica y adicional la entrada por SSH (Secure Shell).
- Realizar prueba de entrada vía red local.

Material y equipo a utilizar:

Para la realización de esta práctica son necesarios los siguientes componentes:

- Hojas
- Lápiz o Bolígrafo
- Packet Tracert versión 6.0.1.0011 o superior

Desarrollo

Indicaciones

En la barra de menú del Packet Tracert seleccionar **Options**

Elegir la opción de **Preferences...** o **Ctrl+R**

En la pestaña de **Interface**

Deshabilitar las opciones de:

Show Device Model Label

Show Device Name Model

Ubica un router en el área de trabajo modelo 1841 y verifica que tenga como nombre de etiqueta Router0.



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Realiza en él una configuración SSH de acuerdo a las siguientes especificaciones:

Parámetro	Descripción
Nombre de router	ssh hostname ssh
Nombre de dominio	empresa.com ip domain-name empresa.com
Versión de SSH	2 ip ssh version 2
Intentos de autenticación	2 ip ssh authentication-retries 2
Tiempo de tolerancia de sesión desatendida de SSH	45 segundos ip ssh time-out 45
Cuenta de acceso para SSH	Usuario: admssh, Contraseña: admin username admssh secret admin
Vía de entrada	Terminal virtual en Fa0/0 line vty 0 4 login local transport input ssh
Red IP a usar en la red local	195.2.2.0/24

Realiza la prueba de conexión vía una computadora, verifica que tenga como nombre de etiqueta **PC0**

<pre> ena conf t hostname ssh int fa 0/0 ip add 195.2.2.1 255.255.255.0 no shut exit </pre>	<pre> ip domain-name empresa.com crypto key generate rsa ! (en este punto se te preguntará el tamaño de la clave la cual definirás a 1024) username admssh secret admin line vty 0 4 login local transport input ssh exit ip ssh version 2 ip ssh authentication-retries 2 ip ssh time-out 45 end </pre>
---	---

<pre> Desde PC0 ssh -l admssh 195.2.2.1 password: admin </pre>	<pre> Desde R1 sh ssh </pre>
--	------------------------------



Conclusiones

Referencias

- Ariganello, Ernesto (2013).
Redes Cisco. Guía de estudio para la certificación CCNA Security.
Editorial Alfaomega. ISBN 978-607-707-654-4
- Barker, K y Morris, S. (2012).
CCNA Security 640-554 Official Cert Guide.
Editorial Cisco Press
- Cisco. (2005).
Fundamentos de seguridad de redes.
Editorial Cisco Press. ISBN: 84-205-4540-6
- Andrew G. Manson. (2002).
Redes privadas virtuales de Cisco Secure.
Editorial Cisco Press. ISBN: 84-205-3618-0
- Vachon, B., y **Graziani, R.** (2009).
Acceso a la WAN Guía de Estudio CCNA Exploration.
Editorial Cisco Press.
- **Graziani, R.** y Johnson, A (2008).
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
Cisco Press. ISBN 978-84-8322-472-4.
- IPSec. Recuperado el 28 de agosto del 2016 de:
<http://packetlife.net/library/cheat-sheets/>

Capturar la imagen donde se muestre su porcentaje de avance.

Recomiendo que dicha captura de imagen sea faltando 30 segundos antes de que expire su tiempo

**GRACIAS
TOTALES**

Criterios de evaluación

Activity Results Time Elapsed: 00:00:19

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PCO				
Default Gateway	Correct	1	Ip	
Ports				
FastEthernet0/0				
IP Address	Correct	1	Ip	
Subnet Mask	Correct	1	Ip	
Router				
Host Name	Correct	1	Other	
IP Domain Name	Correct	1	Other	
Ports				
FastEthernet0/0				
IP Address	Correct	1	Ip	
Port Status	Correct	1	Physical	
Subnet Mask	Correct	1	Ip	
SSH Server				
SSH Authentication Re.	Correct	1	Other	
SSH Timeout	Correct	1	Other	
SSH Version	Correct	1	Other	
User Names		0	Other	
Username	Correct	1	Other	
VTY Lines				
VTY Line 0				
Login	Correct	1	Physical	
Transport Input	Correct	1	Physical	

Score : 14/14

Item Count : 14/14

Component	Items/Total	Score
Ip	5/5	5/5
Other	6/6	6/6
Physical	3/3	3/3



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

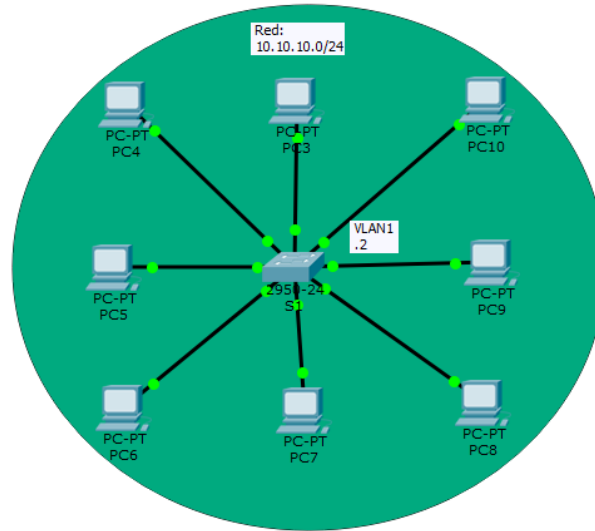
Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Práctica de laboratorio: 5 SSH con VLAN

Duración de la práctica: 20 minutos



Escenario a configurar

Procuren llegar al 100%
SUERTE!!!!

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC3	NIC	10.10.10.3	255.255.255.0
PC4	NIC	10.10.10.4	255.255.255.0
PC5	NIC	10.10.10.5	255.255.255.0
PC6	NIC	10.10.10.6	255.255.255.0
PC7	NIC	10.10.10.7	255.255.255.0
PC8	NIC	10.10.10.8	255.255.255.0
PC9	NIC	10.10.10.9	255.255.255.0
PC10	NIC	10.10.10.10	255.255.255.0

Objetivos de aprendizaje:

- Proteger las contraseñas
- Cifrar las comunicaciones
- Verificar la implementación de SSH

Material y equipo a utilizar:

Para la realización de esta práctica son necesarios los siguientes componentes:

- Hojas
- Lápiz o Bolígrafo
- Packet Tracer versión 6.0.1.0011 o superior



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Desarrollo

Indicaciones

En la barra de menu del Packet Tracert seleccionar **Options**

Elegir la opción de **Preferences... o Ctrl+R**

En la pestaña de **Interface**

Deshabilitar las opciones de:

Show Device Model Label

Show Device Name Model

Información básica

SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos. En esta actividad, protegerá un switch remoto con el cifrado de contraseñas y SSH.

Tarea 1: Contraseñas seguras

a. Desde el símbolo del sistema en la PC10, acceda al S1 mediante Telnet. La contraseña de los modos EXEC del usuario y EXEC privilegiado es cisco.

PC>**telnet 10.10.10.2**

b. Guarde la configuración actual, de manera que pueda revertir cualquier error que cometa reiniciando el S1.

wr o **copy run star**

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado. Introduzca el comando para cifrar las contraseñas de texto no cifrado:

sh run

enable password **UNI**

line vty 0 4

password **UNI**

login

line vty 5 15

password **UNI**

login

S1(config)# **service password-encryption**

d. Verifique que las contraseñas estén cifradas.

sh run

enable password 7 **0822455D0A16**

line vty 0 4

password 7 **0822455D0A16**

login

line vty 5 15

password 7 **0822455D0A16**

login



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Tarea 2: Cifrar las comunicaciones

Paso 1: Establecer el nombre de dominio IP y generar claves seguras.

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio netacad.pka.

```
S1(config)# ip domain-name UNI.EDU
```

b. Se necesitan claves seguras para cifrar los datos. Genere las claves RSA con la longitud de clave 1024.

```
S1(config)# crypto key generate rsa
```

The name for the keys will be: S1.UNI.EDU

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]
```

Paso 2: Crear un usuario de SSH y reconfigurar las líneas VTY para que solo admitan acceso por SSH.

a. Cree un usuario llamado administrator con la contraseña cisco.

```
S1(config)# username administrator password cisco
```

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

```
S1(config-line)# login local
```

```
S1(config-line)# transport input ssh
```

```
S1(config-line)# no password cisco
```

Tarea 3: Verificar la implementación de SSH

a. Cierre la sesión de Telnet e intente volver a iniciar sesión mediante Telnet. El intento debería fallar.

```
S1#exit
```

```
[Connection to 10.10.10.2 closed by foreign host]
```

```
PC>telnet 10.10.10.2
```

```
[Connection to 10.10.10.2 closed by foreign host]
```

b. Intente iniciar sesión mediante SSH. Escriba ssh y presione la tecla Enter, sin incluir ningún parámetro que revele las instrucciones de uso de comandos. Sugerencia: la opción -l representa la letra "L", no el número 1.

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC privilegiado y guarde la configuración. Si no pudo acceder de forma correcta al S1, reinicie y comience de nuevo en la parte 1.

```
PC>ssh -l administrator 10.10.10.2
```

```
Open
```

```
Password: cisco
```

```
S1>
```



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.

Tel: (55) 59714940, 59787577 y 30921763

Página: <http://cux.uaemex.mx>

Academia de Redes

Conclusiones

Referencias

- Ariganello, Ernesto (2013).
Redes Cisco. Guía de estudio para la certificación CCNA Security.
Editorial Alfaomega. ISBN 978-607-707-654-4
- Barker, K y Morris, S. (2012).
CCNA Security 640-554 Official Cert Guide.
Editorial Cisco Press
- Cisco. (2005).
Fundamentos de seguridad de redes.
Editorial Cisco Press. ISBN: 84-205-4540-6
- Andrew G. Manson. (2002).
Redes privadas virtuales de Cisco Secure.
Editorial Cisco Press. ISBN: 84-205-3618-0
- Vachon, B., y **Graziani, R.** (2009).
Acceso a la WAN Guía de Estudio CCNA Exploration.
Editorial Cisco Press.
- **Graziani, R.** y Johnson, A (2008).
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
Cisco Press. ISBN 978-84-8322-472-4.
- IPSec. Recuperado el 28 de agosto del 2016 de:
<http://packetlife.net/library/cheat-sheets/>

Capturar la imagen donde se muestre su porcentaje de avance.
Recomiendo que dicha captura de imagen sea faltando 30 segundos antes de que expire su tiempo

**GRACIAS
TOTALES**

Criterios de evaluación

Activity Results Time Elapsed: 00:18:02

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
DNS				
IP Domain Name	Correct	20	Other Device Harden...	
Security				
Modulus Bits	Correct	20	Device Harden...	
Service Password Encryption	Correct	20	Device Harden...	
User Names				
Username	Correct	20	Other Device Harden...	
VTY Lines				
VTY Line 0				
Login	Correct	7	Device Harden...	
Password	Correct	6	Device Harden...	
Transport Input	Correct	7	Device Harden...	

Score : 100/100
Item Count : 7/7

Component	Items/Total	Score
Device Hardening Configuration	7/7	100/100



Av. Hermenegildo Galeana No.3, Col. Ma. Isabel, Valle de Chalco, C.P. 56615, Edo. De México.
Tel: (55) 59714940, 59787577 y 30921763
Página: <http://cux.uaemex.mx>
Academia de Redes