DATOS DE LA ACTIVIDAD							
No. de Práctica:	**2**	**Práctica:**	**Configurar en Routers con Autenticación AAA**				
Unidad:	1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**Seguridad en Infraestructura de TI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	05/03/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet. Profesional		CP1-1	

1. Objetivo(s) de la práctica

Conocer los protocolos de configuración remota, de sincronización de tiempo y administración de registros en una red.

- Configurar una cuenta de usuario local en R1 y autenticarse en las líneas de consola y VTY utilizando AAA local.
- Verifique la autenticación AAA local desde la línea de consola del Router y el cliente PC-A.
- Configurar una autenticación AAA basada en servidor utilizando TACACS +.
- Verifique la autenticación AAA basada en servidor desde el cliente PC-B
- Configurar una autenticación AAA basada en servidor utilizando RADIUS.
- Verifique la autenticación AAA basada en servidor desde el cliente PC-C.

2. Resumen

Protocolos Autenticación, autorización y registro (AAA): Son un conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información. Se sigue un protocolo para autenticar a un usuario basándose en la identidad verificable del usuario, autorizar a un usuario basándose en sus derechos de usuario y contabilizar el consumo de recursos de una red de un usuario.

- Autenticación: Se refiere a la confirmación de que, el usuario que solicita los servicios sea un usuario valido de los servicios de red solicitados.
- Autorización: Se refiere a otorgar tipos específicos de recursos y/o servicios a un usuario, basado en su autenticación, los servicios que solicitan, y el estado actual del sistema.
- Registro: La contabilidad se refiere al seguimiento del consumo de recursos de red por parte de los usuarios.

RADIUS: RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

RADIUS es un servidor de acceso que utiliza el protocolo AAA. Es un sistema de seguridad distribuida que protege el acceso remoto a las redes y a los servicios de red contra el acceso no autorizado. RADIUS comprende tres elementos:

- Un protocolo con un formato de trama que utiliza el User Datagram Protocol (UDP) /IP.
- Un servidor.
- Un cliente.

El servidor se ejecuta en un equipo central típicamente en el sitio de cliente, mientras que los clientes residen en los servidores de acceso por marcado y pueden ser distribuidos en la red.

TACACS: Terminal Access Controller Access-Control System (TACACS) se refiere a una familia de protocolos relacionados que manejan la autenticación remota y los servicios relacionados para el control de acceso en red a través de un servidor centralizado. El protocolo TACACS original, que se remonta a 1984, se utilizó para comunicarse con un servidor de autenticación, común en las redes UNIX más antiguas; generó protocolos relacionados como TACACS+

TACACS+ es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un Router o a un servidor de acceso a la red. El TACACS+ proporciona estos servicios del Authentication, Authorization, and Accounting (AAA)

- Autenticación de los usuarios que intentan iniciar sesión al equipo de red
- Autorización de determinar qué nivel de usuarios del acceso debe tener
- El considerar para no perder de vista todos los cambios el usuario hace

Referencia:

AAA - AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO. Recuperado el 05/03/2021 desde: https://www.ccncert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=5.html

Iván Darío. A. Q. (2013) ANALISIS COMPARATIVO DE DOS PROTOCOLOS PARA CONTROL DE ACCESO Y ADMINISTRACION DE EQUIPOS DE TELECOMUNICACIONES. Recuperado el 05/03/2021 desde: https://repository.ucatolica.edu.co/bitstream/10983/812/2/ANALISIS%20COMPARATIVO%20DE%20DOS%20PROTOCOLOS%20PARA%20CONTROL%20DE%20ACCESO%20Y%20ADMINISTRACION%20DE%20EQUIPOS%20DE%20TELECOMUNICACIONES%20Final.pdf

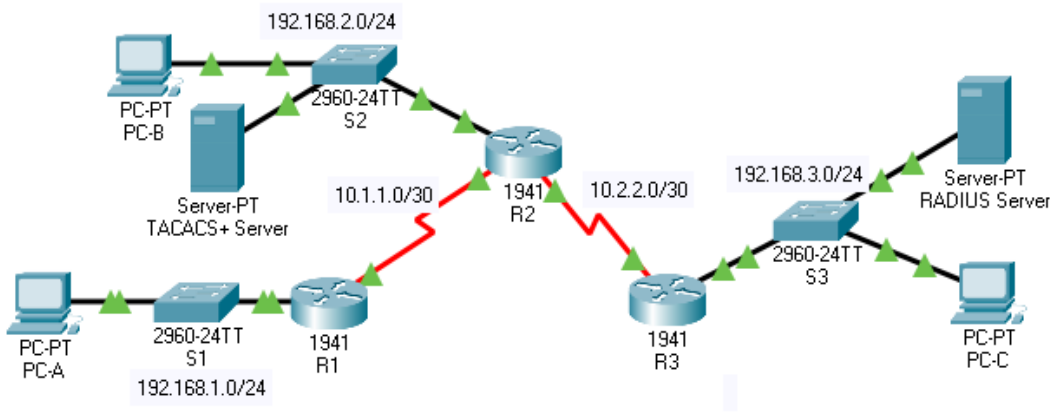
3. Material, equipo y/o herramienta necesaria

- Tres Routers cisco 1941

- Dos servidores PT
- Tres switches 1960-24TT
- Tres PC
- Cable recto
- Cable serial DTE
- Acceso a la línea de comandos de la PC

4. Desarrollo de la práctica (Procedimiento Teórico/Práctico en base al documento Cisco, diagramas, dibujos, tablas, codificación, impresiones de pantalla completa con nombre y fecha)

- **Topología**



- **Tabla de configuración básica.**

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

- **Tabla de comandos**

Sintaxis	Descripción
username Admin1 secret admin1pa55	Crear un usuario local con su respectivo nombre y contraseña
aaa new-model	Aplica inmediatamente la autenticación local a todas las líneas e interfaces (excepto la línea estafa 0 de la línea de la consola). Si se abre una sesión Telnet hacia el Router después de habilitar este comando (o si una conexión caduca y debe volver a conectarse), entonces el usuario debe autenticarse usando la base de datos local del Router.
aaa authentication login default local	Indica que la autenticación por default es la base de datos local
aaa authentication login default group radius local	La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del Router (el segundo método).
login authentication default	Configurar la consola para usarla como el método de listado por default.
ip domain-name ccnasecurity.com	Usar ccnasecurity como el dominio de R1
aaa authentication login SSH-LOGIN local	Configurar una lista llamada SSH-LOGIN para autenticar los inicios de sesión que usan el AAA local.
transport input shh	Únicamente acceso remoto a SSH
tacacs-server host 192.168.2.2	Configurar la ip del servidor Tatacs
tacacs-server key tacacspa55	Configurar la llave de acceso secreto en el servidor Tacacs

- **Procedimiento (del PDF) con Impresiones de pantalla de resultados en el simulador Packet Tracert 7.0 (SIN Preguntas) (Imágenes con nombre y número de Figura**

Parte 1: configurar la autenticación AAA local para el acceso a la consola en el R1

Paso 1: probar la conectividad.

- Haga ping de la PC-A a la PC-B.
- Haga ping de la PC-A a la PC-C.
- Haga ping de la PC-B a la PC-C.

Paso 2: configurar un nombre de usuario local en el R1.

- Configure un nombre de usuario de Admin1 con una contraseña secreta de admin1pa55.

Paso 3: configurar la autenticación AAA local para el acceso a la consola en el R1.

- Habilite AAA en R1 y configure la autenticación AAA para que el inicio de sesión de la consola utilice la base de datos local.

Paso 4: Configure la consola de línea para utilizar el método de autenticación AAA definido.

- Habilite AAA en R1 y configure la autenticación AAA para que el inicio de sesión de la consola utilice la lista de métodos predeterminada.

Packet Tracer: configure la autenticación AAA en los routers Cisco

Paso 5: Verifique el método de autenticación AAA.

- Verifique el inicio de sesión EXEC del usuario utilizando la base de datos local.

Parte 2: configurar la autenticación AAA local para las líneas vty en el R1

Paso 1: Configure el nombre de dominio y la clave criptográfica para usar con SSH.

- Utilice ccnasecurity.com como nombre de dominio en R1.
- Cree una clave criptográfica RSA con 1024 bits.

Paso 2: Configure un método de autenticación AAA de lista con nombre para las líneas vty en el R1.

- Configure una lista con nombre llamada SSH-LOGIN para autenticar los inicios de sesión mediante AAA local.

Paso 3: Configure las líneas vty para usar el método de autenticación AAA definido.

- Configure las líneas vty para usar el método AAA con nombre y solo permita SSH para acceso remoto.

Paso 4: Verifique el método de autenticación AAA.

- Verifique la configuración SSH SSH a R1 desde el símbolo del sistema de la PC-A.

Parte 3: configurar la autenticación AAA basada en servidor mediante TACACS + en R2

Paso 1: Configure una entrada de la base de datos local de respaldo llamada Admin.

- Para fines de respaldo, configure un nombre de usuario local de Admin2 y una contraseña secreta de admin2pa55.

Paso 2: Verifique la configuración del servidor TACACS+.

- Haga clic en TACACS + Server. En la pestaña Servicios, haga clic en AAA. Tenga en cuenta que hay una configuración de red.
- Entrada para R2 y una entrada de Configuración de usuario para Admin2.

Paso 3: Configure las especificaciones del servidor TACACS + en R2.

- Configure la dirección IP del servidor AAA TACACS y la clave secreta en R2.
- Nota: Los comandos tacacs-server host y tacacs-server key están obsoletos. Actualmente, Packet Tracer no admite el nuevo servidor de comando tacacs.
    - R2 (config) # tacacs-server host 192.168.2.2
    - R2 (config) # tacacs-clave de servidor tacacspa55

Paso 4: configurar la autenticación de inicio de sesión AAA para el acceso a la consola en R2.

- Habilite AAA en R2 y configure todos los inicios de sesión para autenticarse usando el servidor AAA TACACS +. Si no está disponible, utilice la base de datos local.

Paso 5: Configure la consola de línea para utilizar el método de autenticación AAA definido.

- Configure la autenticación AAA para que el inicio de sesión de la consola utilice el método de autenticación AAA predeterminado.

Paso 6: Verifique el método de autenticación AAA.

- Verifique el inicio de sesión EXEC del usuario mediante el servidor AAA TACACS+.

Parte 4: configurar la autenticación AAA basada en servidor mediante RADIUS en R3

Paso 1: Configure una entrada de la base de datos local de respaldo llamada Admin.

- Para fines de respaldo, configure un nombre de usuario local de Admin3 y una contraseña secreta de admin3pa55.

Paso 2: Verifique la configuración del servidor RADIUS.

- Haga clic en el servidor RADIUS. En la pestaña Servicios, haga clic en AAA. Observe que hay una entrada de configuración de red para R3 y una entrada de configuración de usuario para Admin3.

Paso 3: Configure las especificaciones del servidor RADIUS en R3.

- Configure la dirección IP y la clave secreta del servidor RADIUS AAA en el R3.
- Nota: Los comandos radius-server host y radius-server key están obsoletos. Actualmente, Packet Tracer no es compatible con el nuevo servidor de comandos radius.
    - R3 (config) # radius-server host 192.168.3.2
    - R3 (config) # radius-server key radiuspa55

Paso 4: Configure la autenticación de inicio de sesión AAA para el acceso a la consola en el R3.

- Habilite AAA en R3 y configure todos los inicios de sesión para autenticarse usando el servidor AAA RADIUS. Si no está disponible, utilice la base de datos local.

Paso 5: Configure la consola de línea para utilizar el método de autenticación AAA definido.

- Configure la autenticación AAA para que el inicio de sesión de la consola utilice el método de autenticación AAA predeterminado.

Paso 6: Verifique el método de autenticación AAA.

- Verifique el inicio de sesión EXEC del usuario mediante el servidor AAA RADIUS.

Paso 7: Verifique los resultados.

- Su porcentaje de finalización debe ser del 100%. Haga clic en Verificar resultados para ver comentarios y verificar qué componentes requeridos se han completado.

Figura 1: Método de autenticación AAA en R1

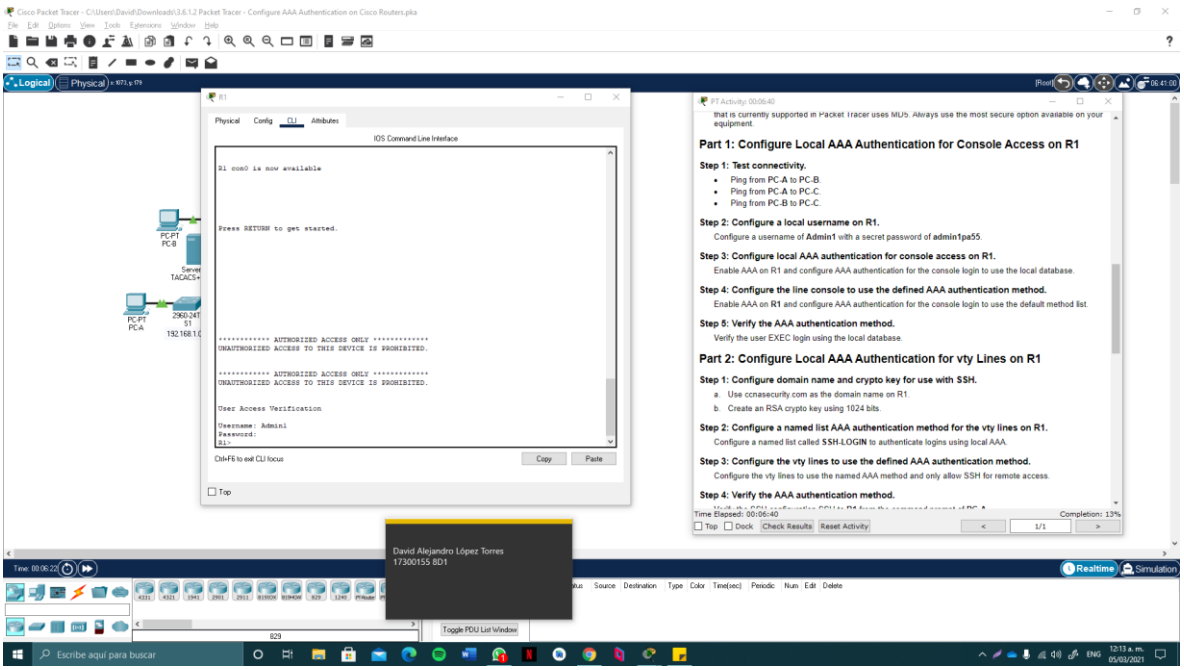


Figura 2: Verificación de la configuración SSH para R1 desde PCA

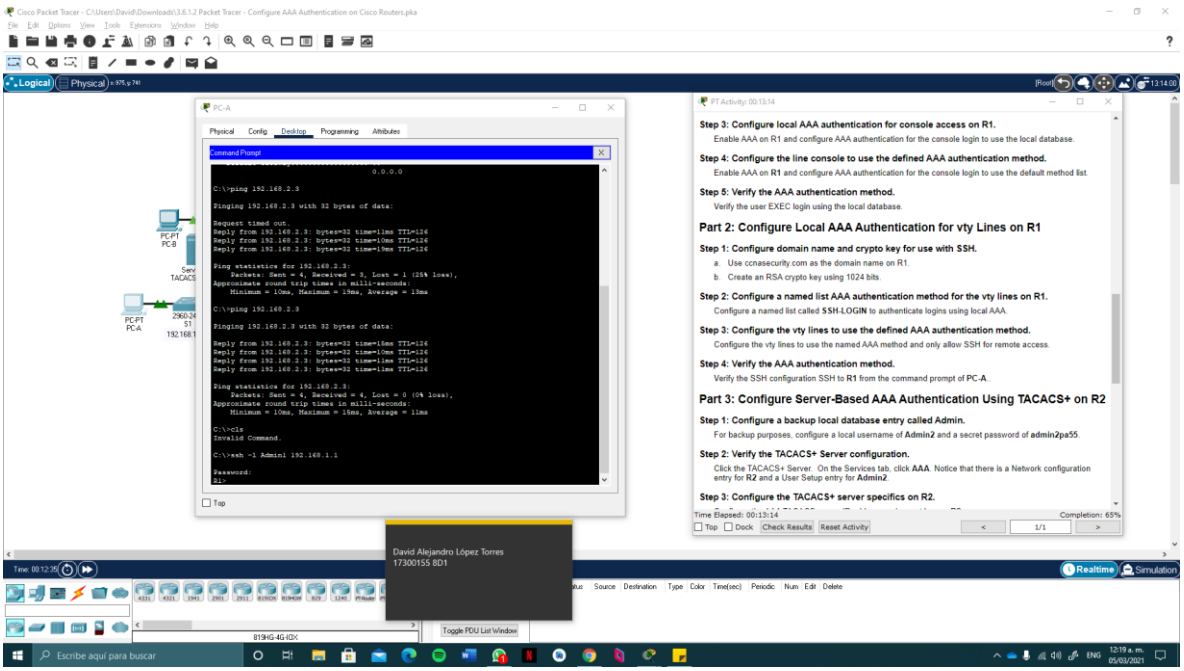


Figura 3: Verificación de la configuración del servidor TACACS+

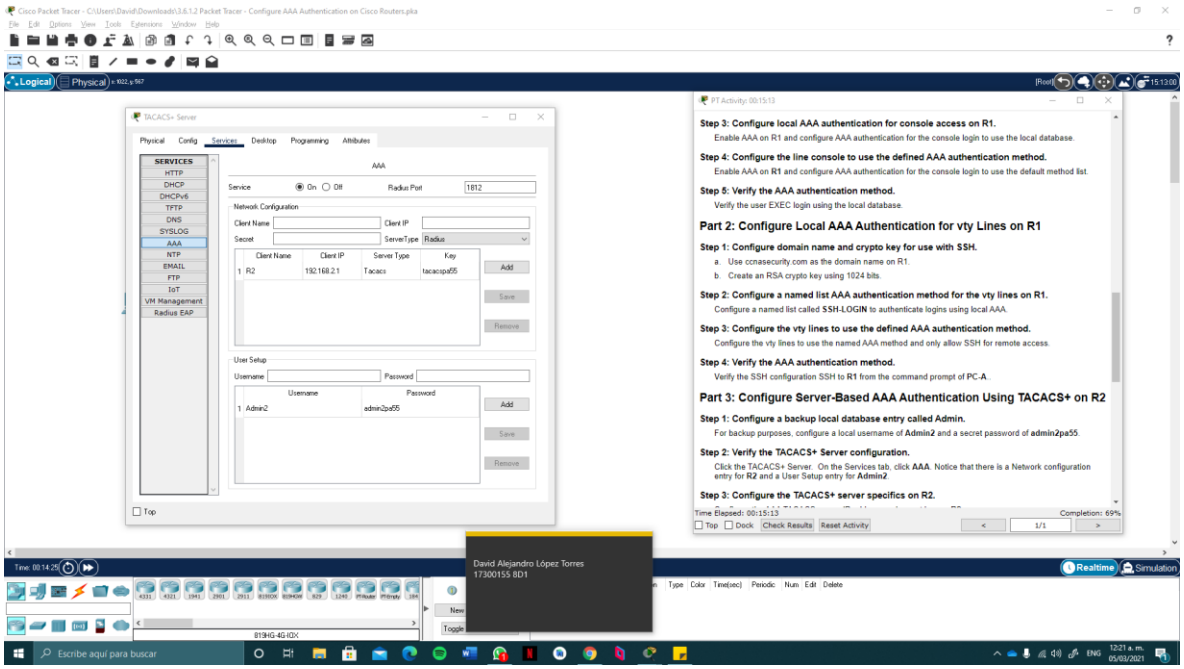


Figura 4: Método de autenticación AAA en R2

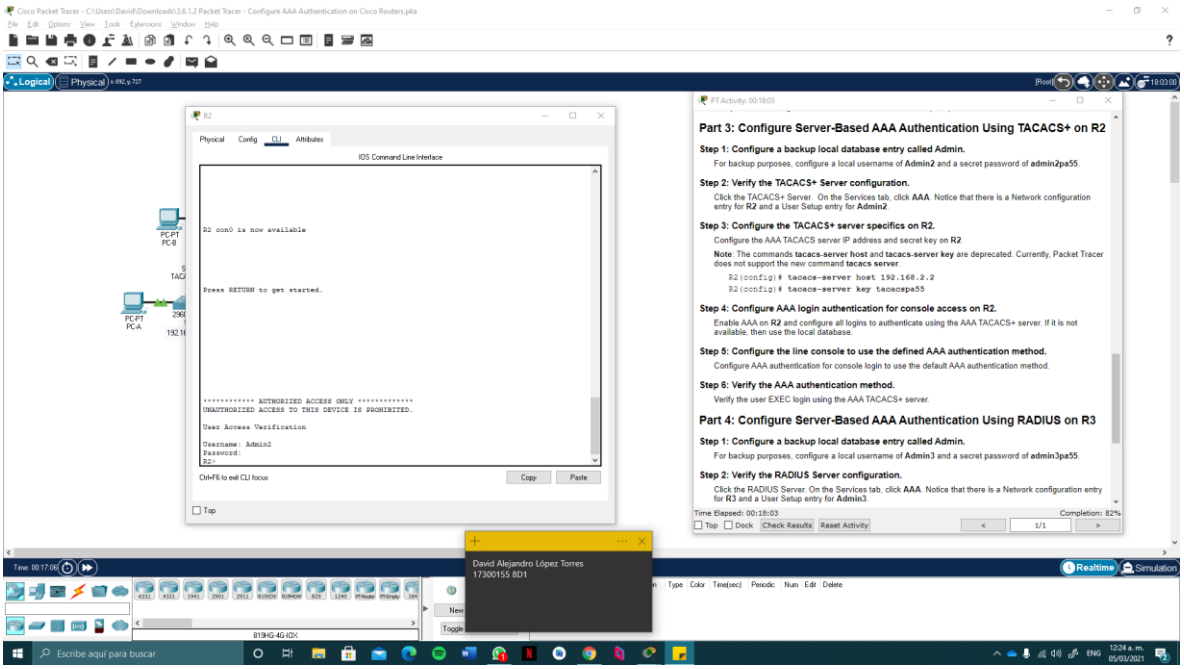


Figura 5: Verificación de la configuración del servidor RADIUS

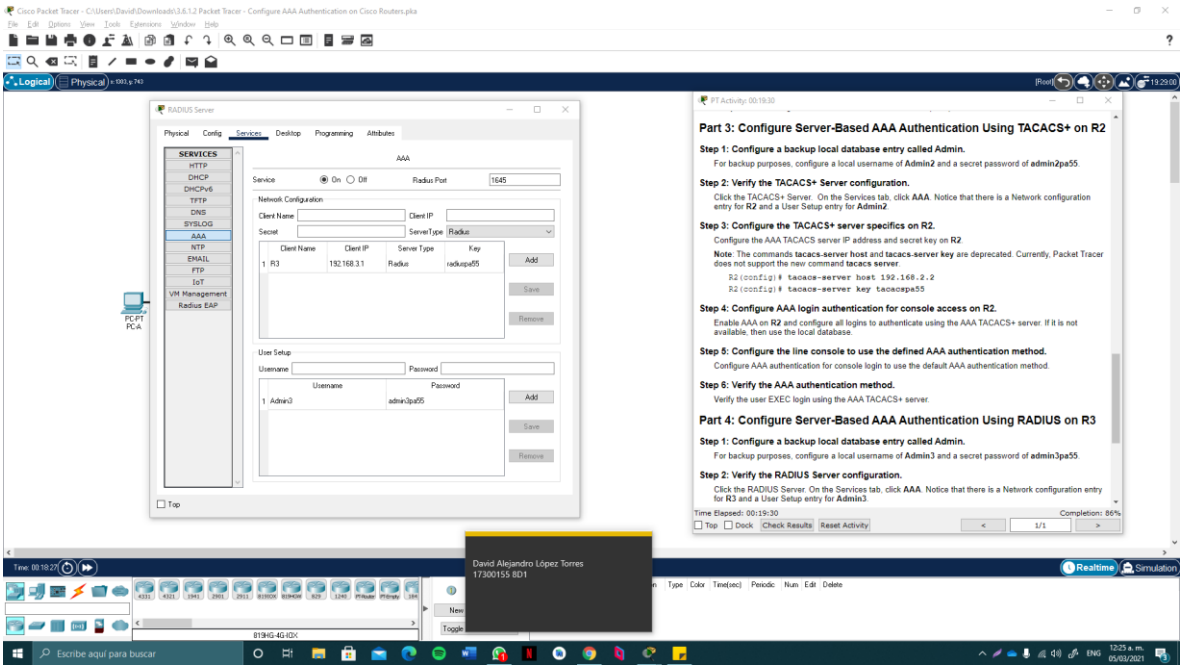


Figura 6: Método de autenticación AAA en R3

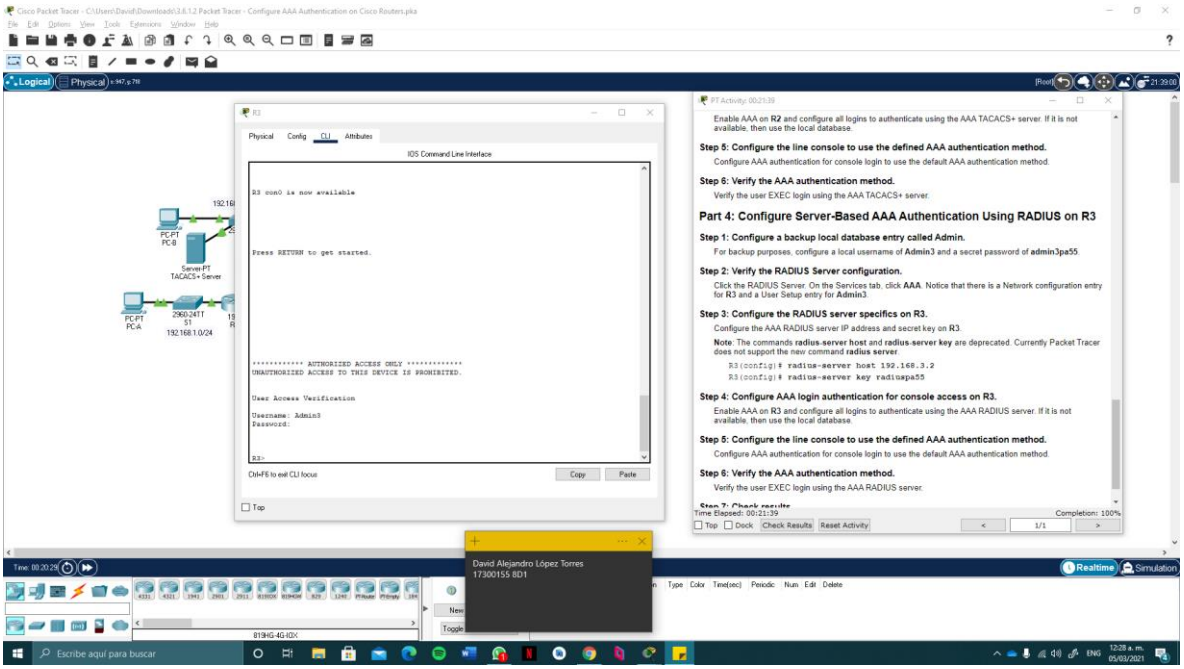
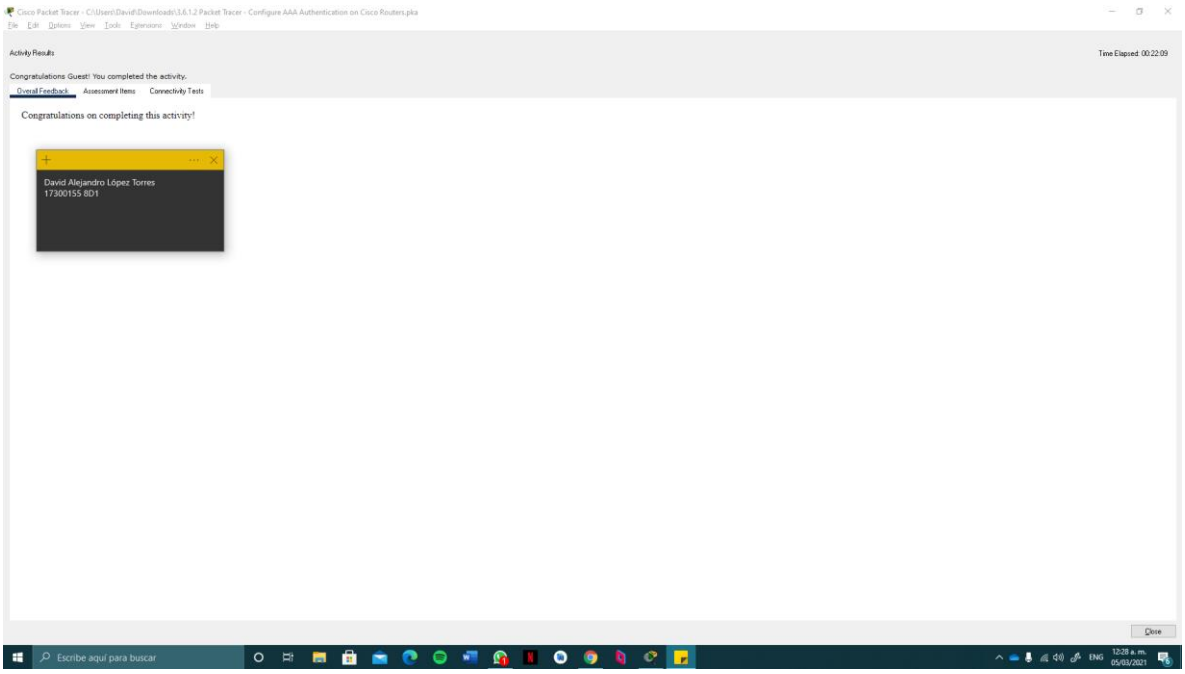


Figura 7: Actividad finalizada



5. Observaciones

El desarrollo de esta práctica fue una tarea simple gracias a la documentación brindada por el profesor para llevarlo a cabo. En general, los principales problemas que se enfrentaron tenían que ver con el flujo del tiempo en Packet Tracer (igual al de la vida real), así que solo era cuestión de esperar o acelerar el ritmo de la simulación para ver el efecto de algunas de las configuraciones de los servicios RADIUS y TACACS.

6. Conclusiones

Con el desarrollo de esta práctica hemos llevado a la práctica los conceptos estudiados acerca de la implementación de la seguridad AAA dentro de la infraestructura de una red por medio de la configuración de los enrutadores. Ambos servidores (RADIUS y TACACS) poseen una serie de características que los vuelven óptimos para una determinada topología y esquema de tráfico de la información. No obstante, ambos representan una gran alternativa para la implementación AAA dentro de una red. El resultado de configurar alguno de estos servidores representa una mejora considerable en la seguridad de la red, pues se brindan servicios de autenticación, autorización y registro integrados en un solo servidor.