Redes y comunicación de Datos 2

Sesión 14

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Radius y Tacacs
- **Actividad:**
  - **Implementación del protocolo AAA Radius/Tacacs.**

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la unidad, el estudiante aprende a configurar el protocolo AAA, el protocolo Radius, el protocolo Tacacs y realiza las pruebas correspondientes, a través de ejemplos desarrollados en clase.

Buenas Prácticas

Buenas Prácticas

Con respecto a la Sesión 13

- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

Control de acceso

Autenticación con una contraseña local

Muchas formas de autenticación pueden ser llevadas a cabo en dispositivos de red, y cada método ofrece diferentes niveles de seguridad.

El simple método de autenticación por acceso remoto es para configurar un inicio de sesión y contraseña combinación en consola, lineas vty, y puertos auxiliares, como se muestra en las lineas vty en el siguiente ejemplo.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH es un tipo de acceso remoto más seguro:

- Requiere un nombre de usuario y una contraseña.
- El nombre de usuario y la contraseña se pueden autenticar localmente.

El método de base de datos local tiene algunas limitaciones:

- Las cuentas de usuario deben configurarse localmente en cada dispositivo que no sea escalable.
- El método no proporciona ningún método de autenticación alternativa.

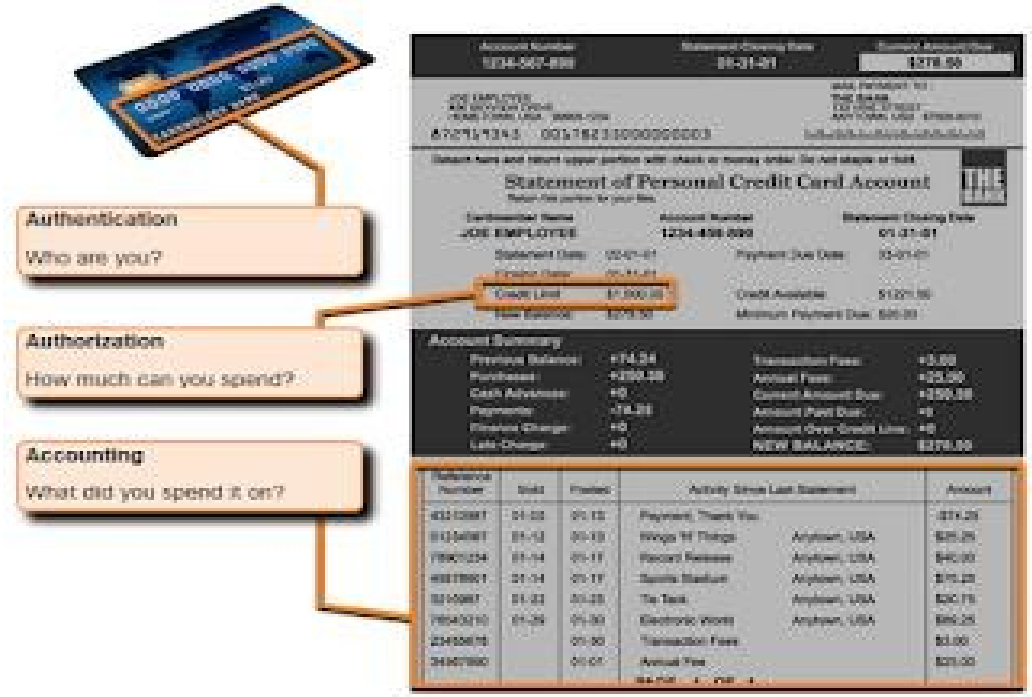
```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Control de acceso

Componentes AAA

AAA significa **Autenticación, Autorización y Contabilidad,** y proporciona el marco principal para configurar el control de acceso en un dispositivo de red.

AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).



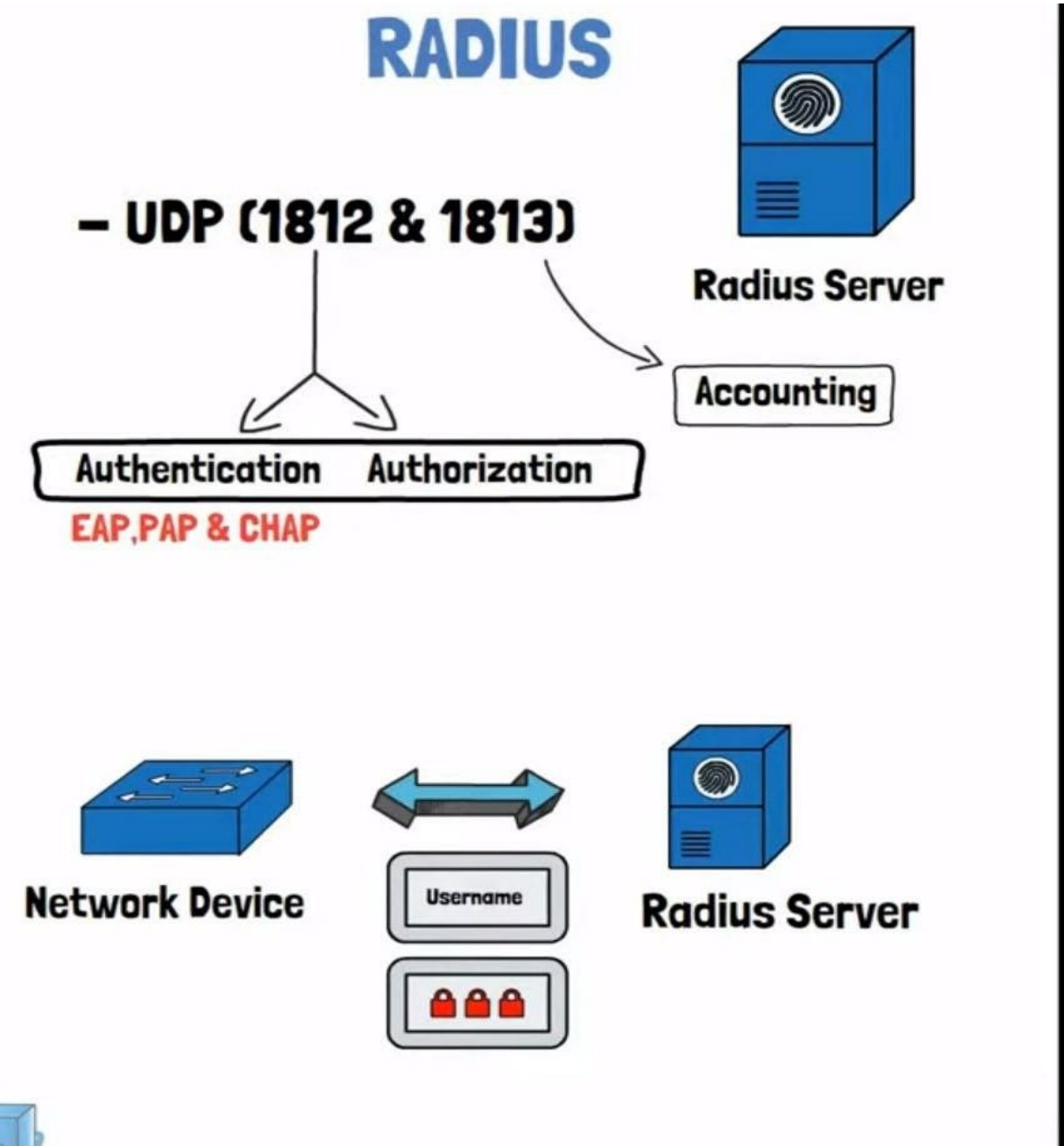
Buenas Prácticas

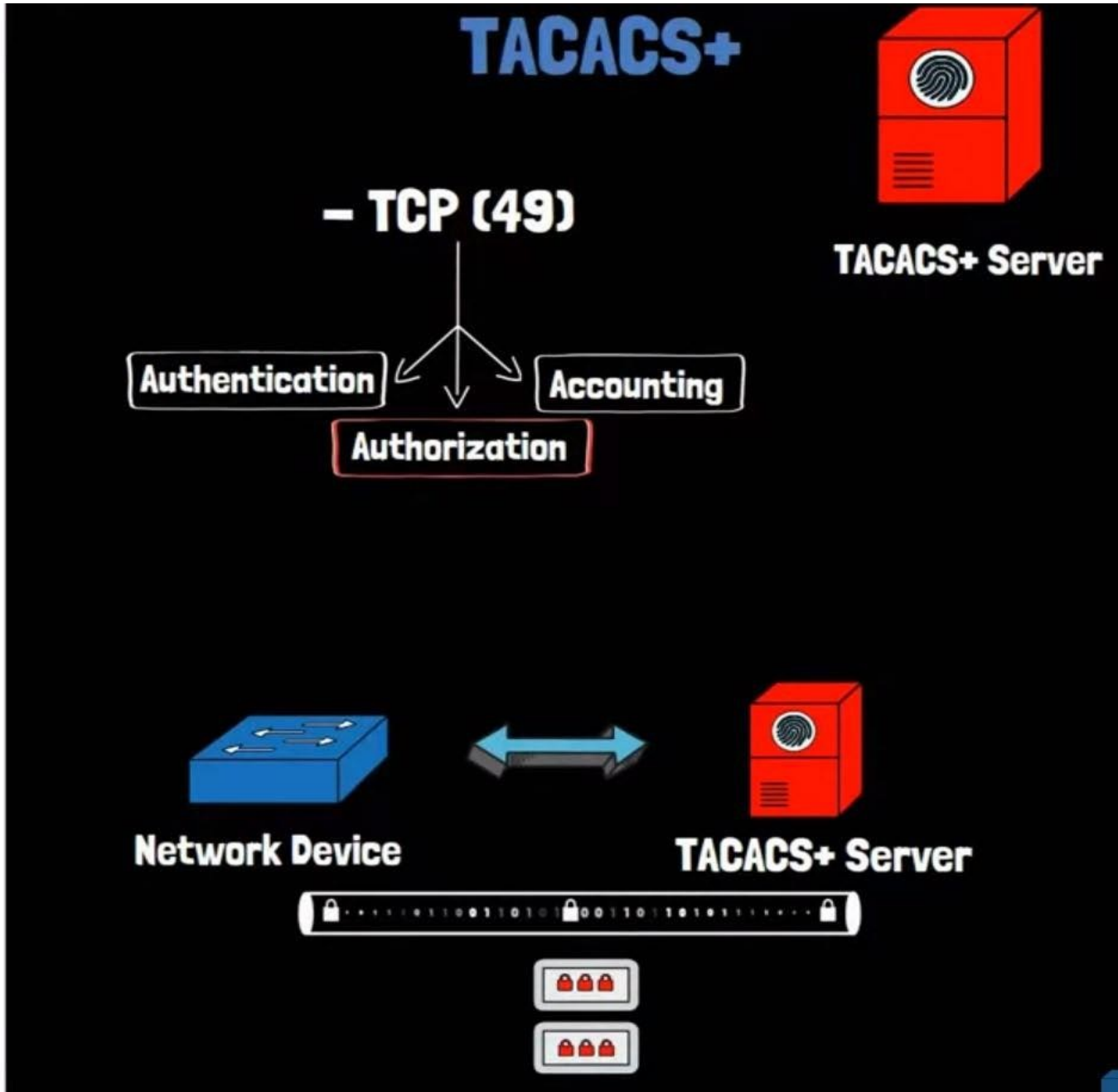
Sesión 14

Lluvia de ideas sobre los protocolos Tacacs/Radius

- ¿Qué son los protocolos Tacacs/Radius?
- ¿Para qué sirve los protocolos Tacacs/Radius?

Radius / Tacacs



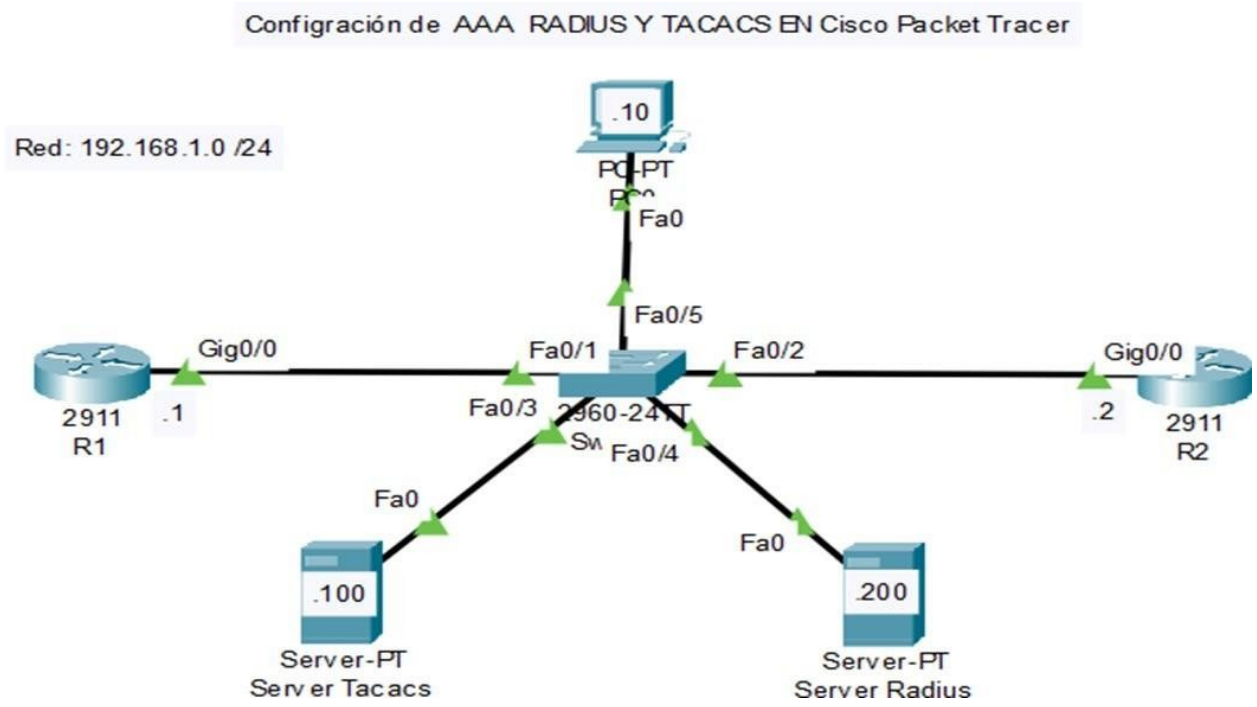


El protocolo AAA Radius/Tacacs

Información básica

- Los servidores AAA (Autorización, Autenticación y Accounting), se utilizan para una mayor seguridad en el acceso dentro de una red, centralizando y asegurando el acceso a dispositivos de red.

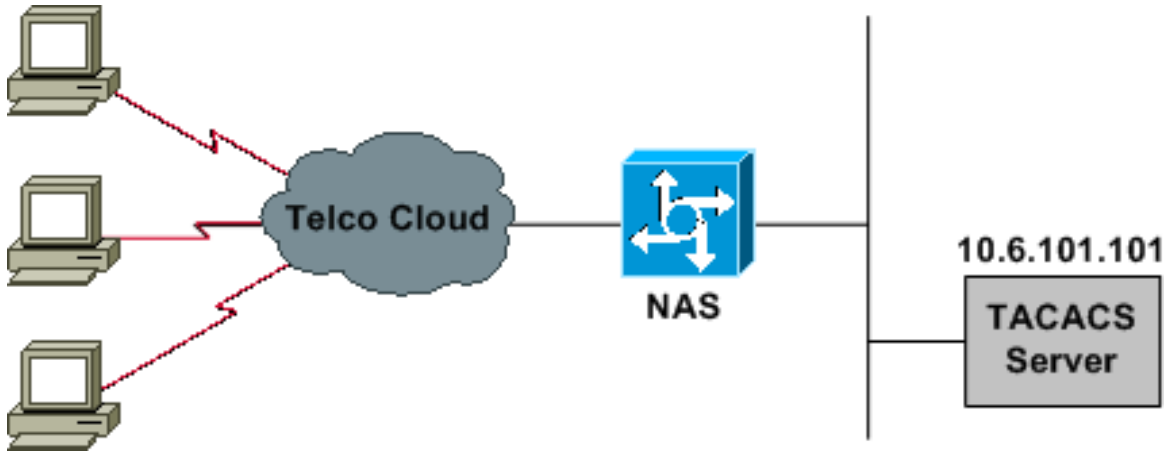
- Existen dos protocolos principales que son RADIUS y TACACS



Tacacs

Este protocolo utiliza una administración de redes simplificadas incrementando su seguridad al permitir centralizar la gestión de los usuarios en la red, a través de políticas de acceso de usuario, grupos, comandos, su ubicación, su red o tipo de dispositivo.

TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

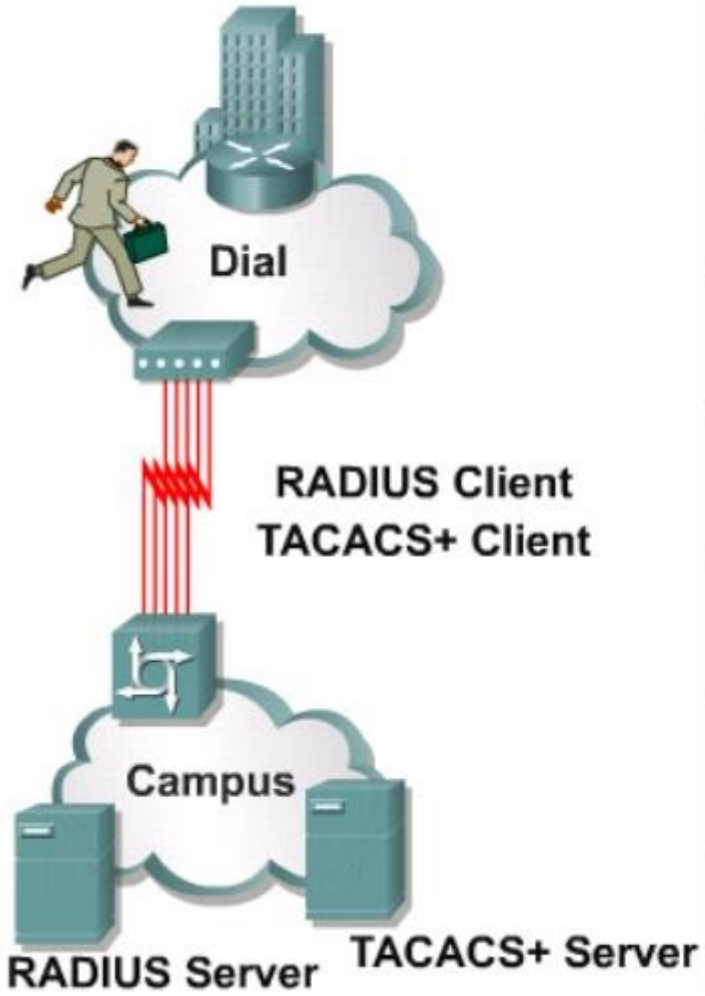


Radius

Este protocolo funciona sobre un equipo que hace las veces de servidor de acceso a través de AAA. Radius esta pensado para distribución de acceso remoto seguro a redes y a servicios que no poseen control de acceso a los usuarios.

Radius es un protocolo que ofrece un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red.

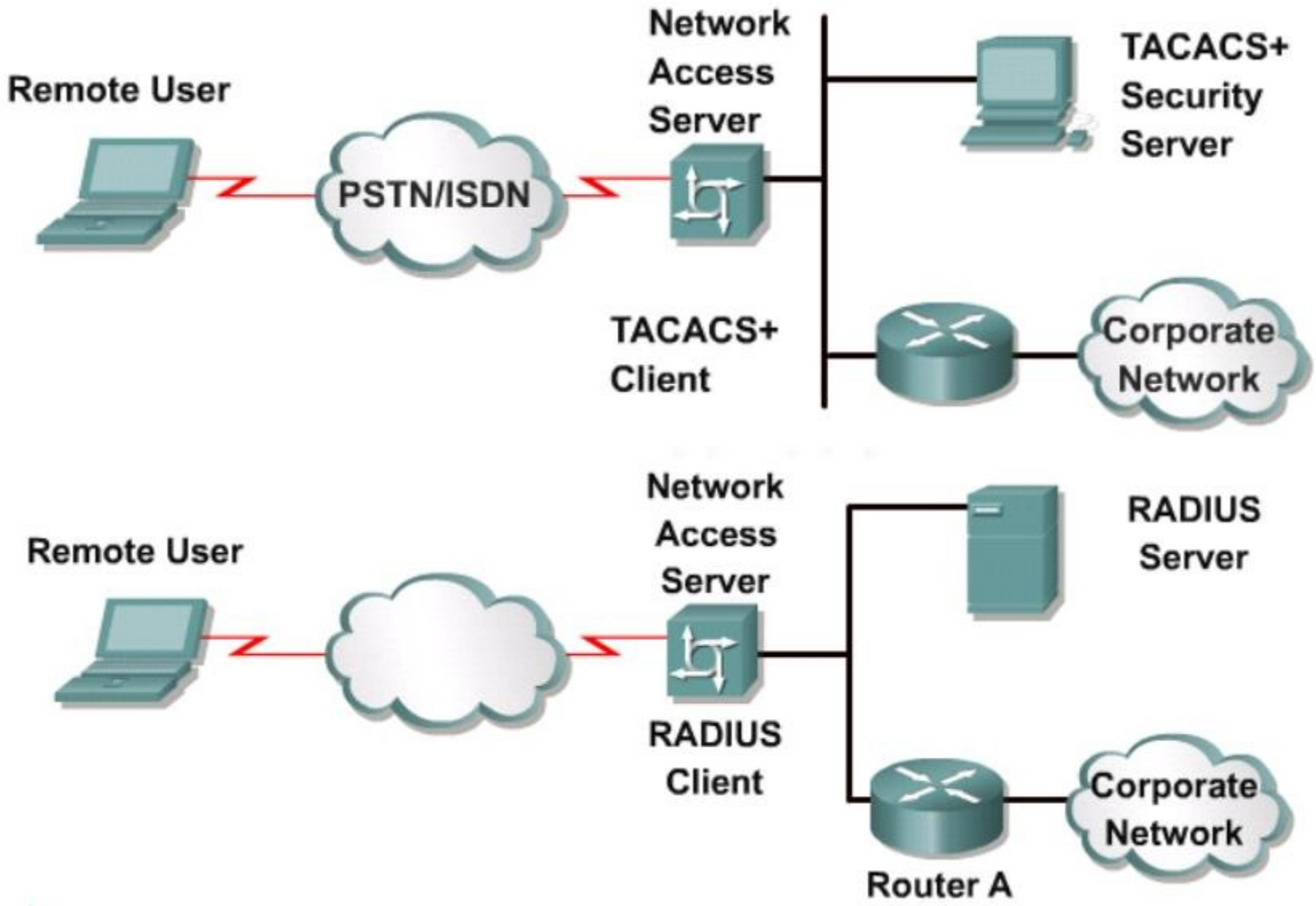
El protocolo AAA Radius/Tacacs



	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication/ Authorization
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
Protocol Support	Multi-protocol support	No ARA No NetBEUI
Confidentiality	Entire Packet-Encrypted	Password-Encrypted
Accounting	Limited	Extensive

https://www.youtube.com/watch?v=kiVg1q6Chvs

El protocolo AAA Radius/Tacacs



Implementar el protocolo AAA Radius/Tacacs

Objetivos de aprendizaje

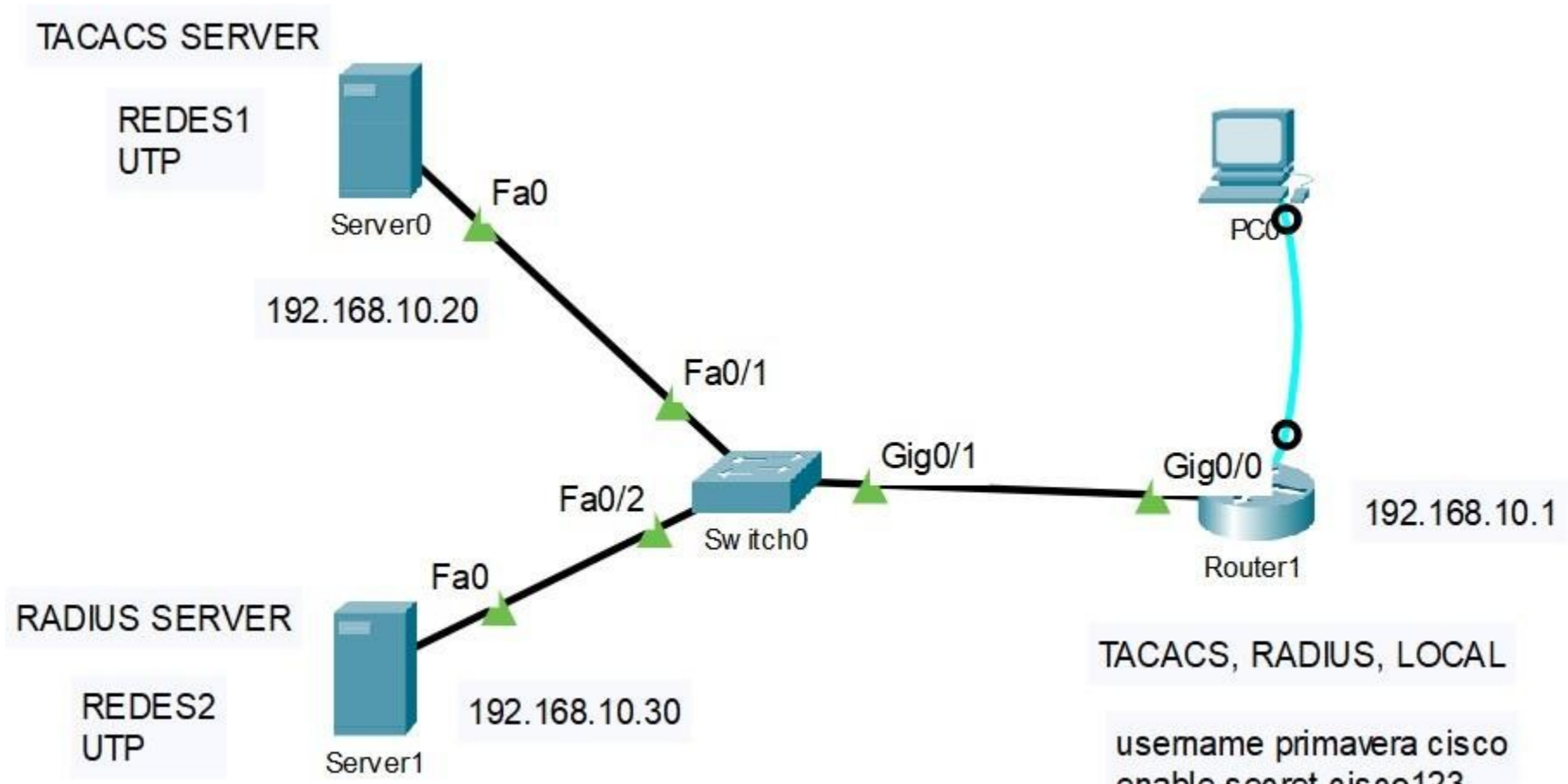
- Al completar esta actividad, usted podrá:
- Implementar una red de acuerdo con el diagrama de topología.
- Asignar un nombre a los routers (R1 y R2)
- Realizar tareas de configuración básicas del router.
- Configurar y activar interfaces.
- Asignar direcciones IP a las interfaces y los Hosts
- Configurar el protocoloAAA
- Configurar el protocolo Radius
- Configurar el protocolo TACACS +
- Realizar las pruebas respectivas

Actividad

Práctica de laboratorio

Packet Tracer - Implementar el protocolo AAA Radius/Tacacs

Actividad: Implementar el protocolo AAA Radius/Tacacs



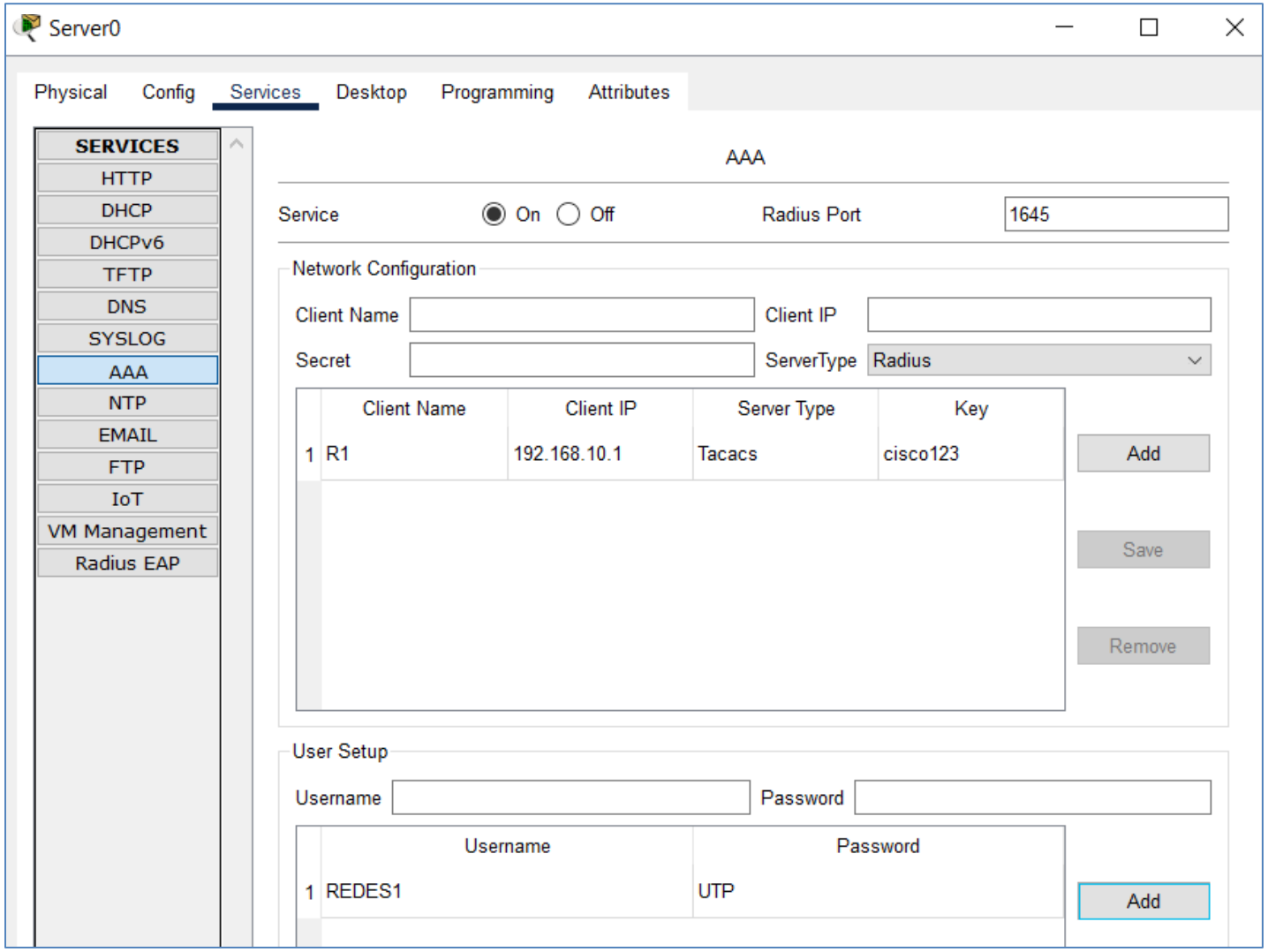
Actividad: Implementar el protocolo AAA Radius/Tacacs

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret cisco123
R1(config)#username primavera password cisco
R1(config)#exit
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config)#exit
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#tacacs-server host 192.168.10.20 key cisco123
R1(config)#radius-server host 192.168.10.30 key cisco123
R1(config)#
```

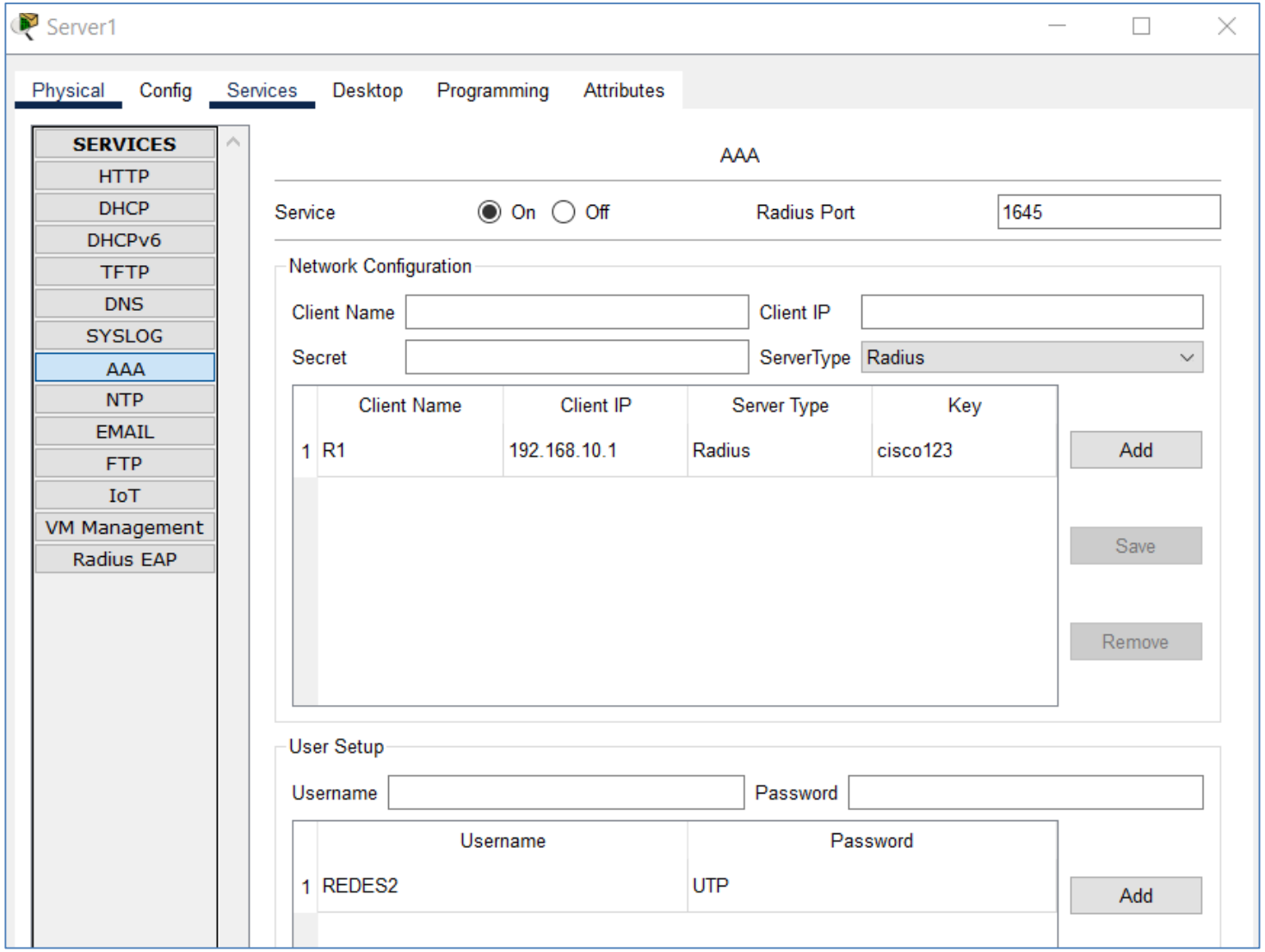
Actividad: Implementar el protocolo AAA Radius/Tacacs

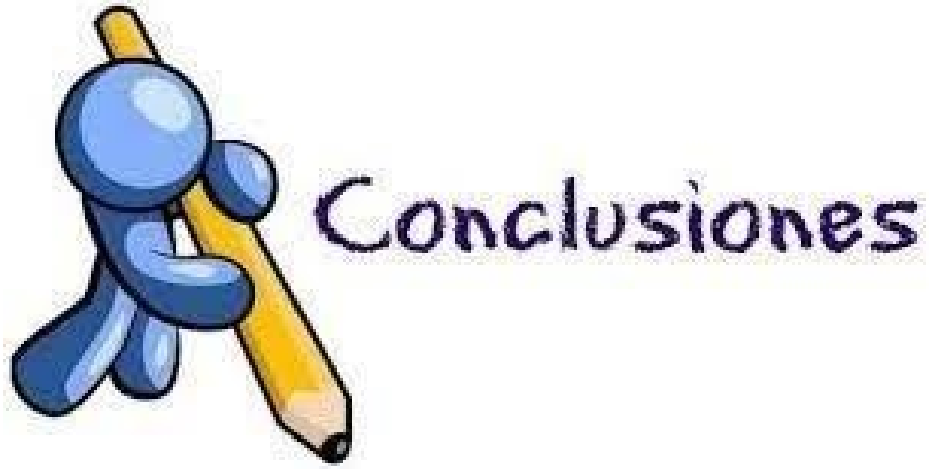
```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa authentication ?
        enable Set authentication lists for enable.
        login Set authentication lists for logins.
        ppp Set authentication lists for ppp.
R1(config)#aaa authentication login ?
        WORD Named authentication list.
        default The default authentication list.
R1(config)#aaa authentication login dedefault ?
        enable Use enable password for authentication.
        group Use Server-group.
        local Use local username authentication.
        local-case Use case-sensitive local username authentication.
        none NO authentication.
R1(config)#aaa authentication login default group tacacs+ group radius local-case
1(config)#exit
R1#
```

Actividad: Implementar el protocolo AAA Radius/Tacacs



Actividad: Implementar el protocolo AAA Radius/Tacacs



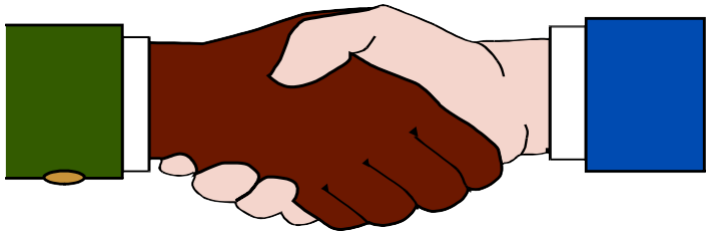


¿Qué aprendí en esta sesión?

¿Qué aprendí en este módulo?

- Configurar el protocolo AAA
- Configurar el protocolo Radius
- Configurar el protocolo TACACS +
- Realizar las pruebas respectivas

Gracias



Universidad
Tecnológica
del Perú