UNIVERSIDAD DE LAS FUERZAS ARMADAS - “ESPE”

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

“EVALUACIÓN DEL DESEMPEÑO DE LOS SISTEMAS DE AUTENTICACIÓN DEL ESTÁNDAR DE SEGURIDAD IEEE 802.1X PARA LA INTEGRACIÓN DE UN PORTAL CAUTIVO BAJO EL PROTOCOLO DE RADIUS”

AUTOR: ÁLVAREZ MISE LUIS FERNANDO

DIRECTOR: ING. ROMERO GALLARDO CARLOS GABRIEL

QUITO-ECUADOR
2022

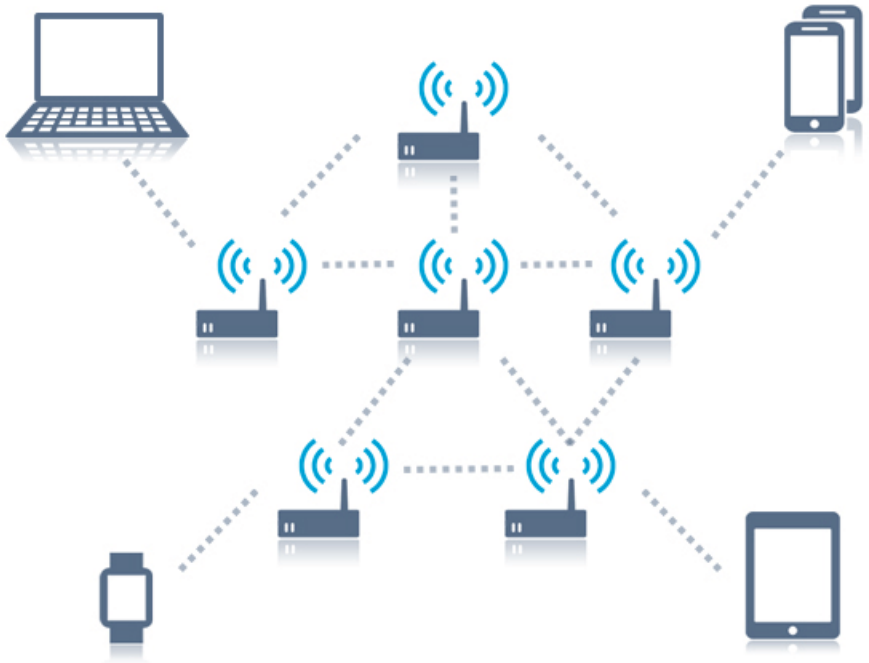
VERSIÓN: 1.1

AGENDA

1. Introducción
2. Análisis y Diseño
3. Implementación
4. Pruebas y Resultados
5. Conclusiones
6. Recomendaciones y Trabajos Futuros

INTRODUCCIÓN

Antecedentes



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

INTRODUCCIÓN

Trabajos relacionados

“Estudio comparativo de métodos de autenticación para redes Wi-Fi”

- EAP admite una variedad de protocolos en la capa de autenticación, cada uno con ventajas y desventajas.
- Detalla una tabla comparativa usando diferentes técnicas de los métodos de autenticación EAP.
- (Ali & Al-Khlifa, 2011)

“Análisis y mejoras del protocolo PEAP en WLAN”

- En los últimos años se ha desarrollado un gran número de aplicaciones WLAN, pero surgieron diferentes tipos de problemas en seguridad.
- Detalla sobre el PEAP, como se lleva a cabo su proceso de autenticación, cuales son los defectos y como podemos mejorar para que pueda superarlos.
- (Sang & Zhou, 2012)

“Estudio sobre los protocolos de autenticación WPA y 802.11i RSN”

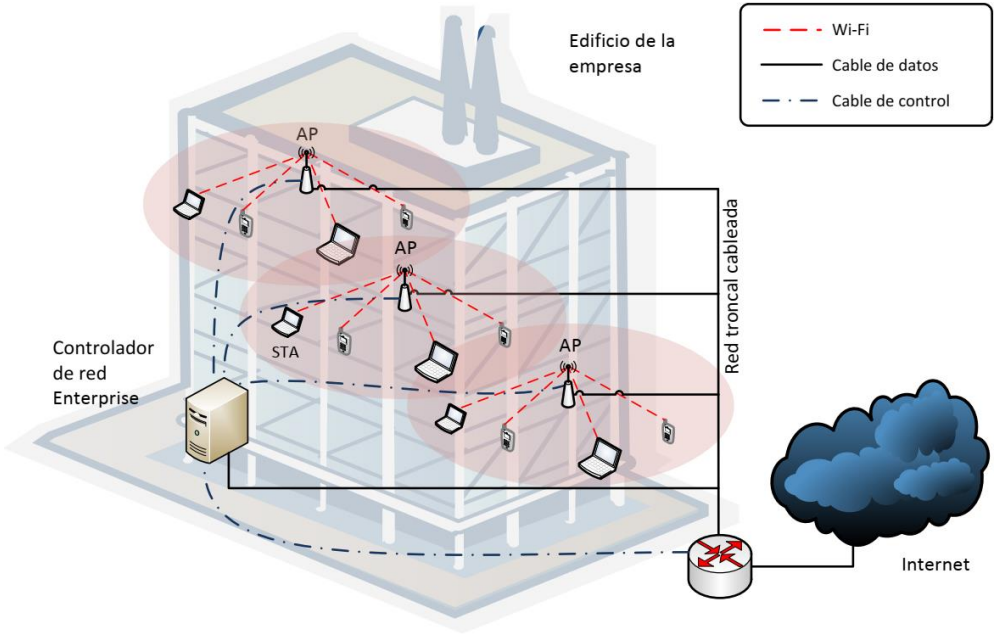
- Describe ocho propiedades deseadas para los protocolos de autenticación WLAN.
- Realiza un estudio sobre los diferentes tipos de protocolos de autenticación EAP y explica los protocolos con un diagrama de flujo entre el cliente y el servidor.
- (Baek, Smith, & Kotz, 2013)

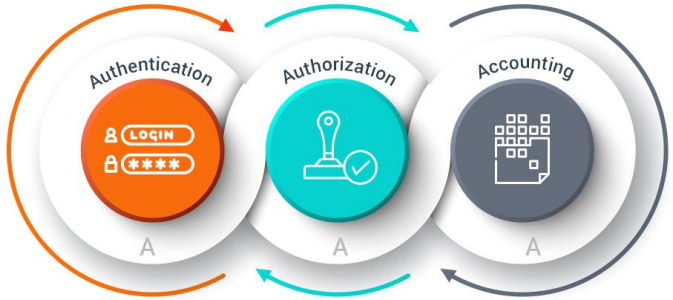
“Protocolos de seguridad de redes inalámbricas: un estudio comparativo”

- Explica la evolución de la seguridad para las redes inalámbricas mediante un estudio comparativo entre tres protocolos de seguridad: WEP, WPA y WPA2.
- Analiza el proceso de cifrado/descifrado, las limitaciones y la vulnerabilidad de cada protocolo a varios ataques.
- (Sukhija & Gupta, 2014)

INTRODUCCIÓN

Justificación





Seguridad en la red inalámbrica + Control sobre la red inalámbrica = Sistema RADIUS con: autenticación, autorización y contabilidad

OBJETIVOS

Objetivo General

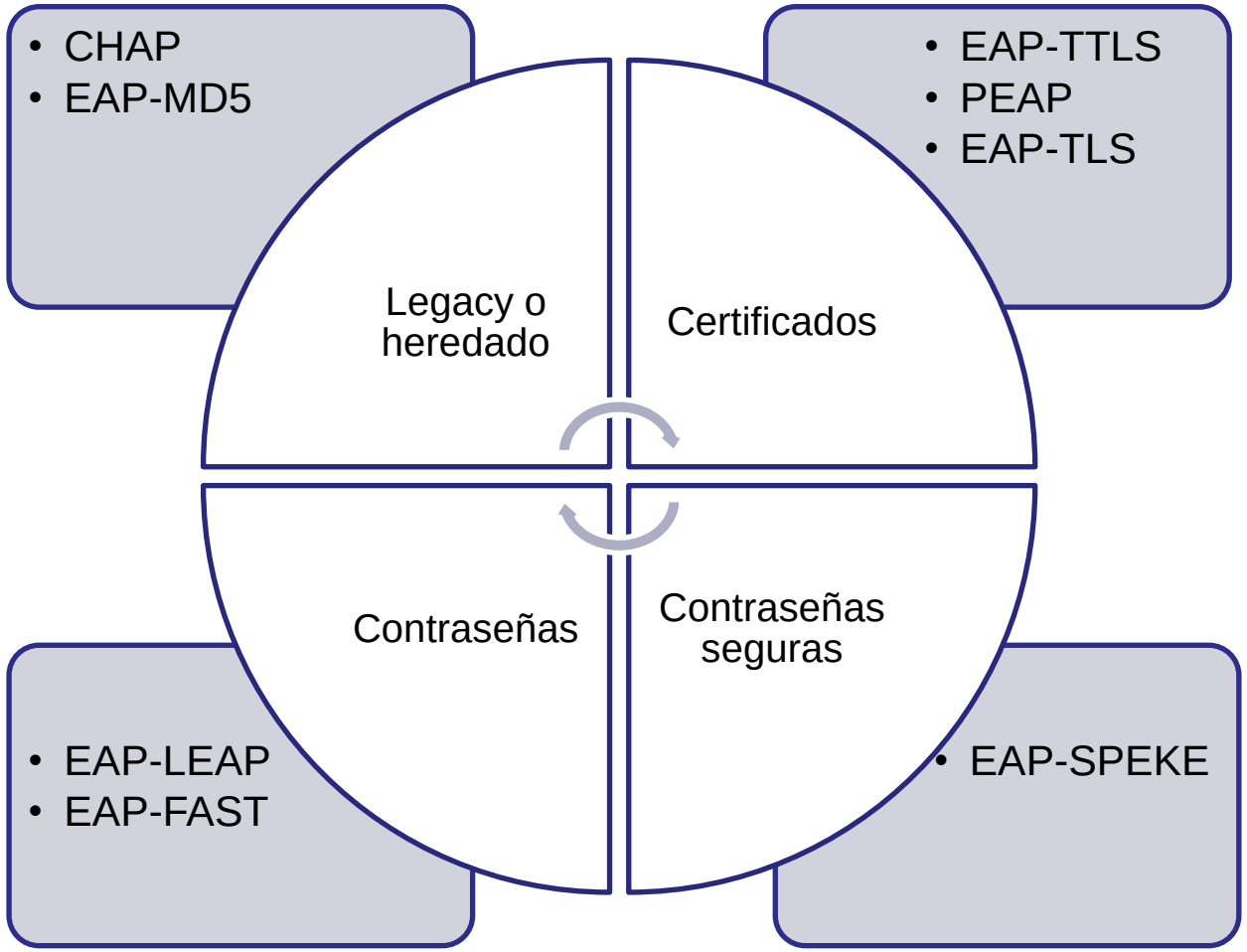
Evaluar el desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS y así brindar los servicios de red en la empresa Compu Seguridad.

Objetivos Específicos

- Desarrollar el estado del arte del estándar de seguridad IEEE 802.1X, el protocolo RADIUS y su integración en portales cautivos.
- Realizar un análisis comparativo de la autenticación del estándar de seguridad IEEE 802.1X.
- Realizar un análisis de la situación actual de la red inalámbrica de la empresa Compu Seguridad.
- Desarrollar un portal cautivo que permita iniciar sesión y conectarse a internet a los empleados de la empresa Compu Seguridad.
- Configurar los equipos de red inalámbrica de la empresa Compu Seguridad bajo el estándar de seguridad IEEE 802.1X.
- Evaluar los resultados obtenidos en la implementación de los sistemas de autenticación.

- IEEE 802.1X
- Métodos EAP
- RADIUS
- Protocolo AAA
- Portal Cautivo

Métodos EAP


• CHAP
• EAP-MD5
• EAP-TTLS
• PEAP
• EAP-TLS
Legacy o heredado
Certificados
Contraseñas
Contraseñas seguras
• EAP-LEAP
• EAP-FAST
• EAP-SPEKE

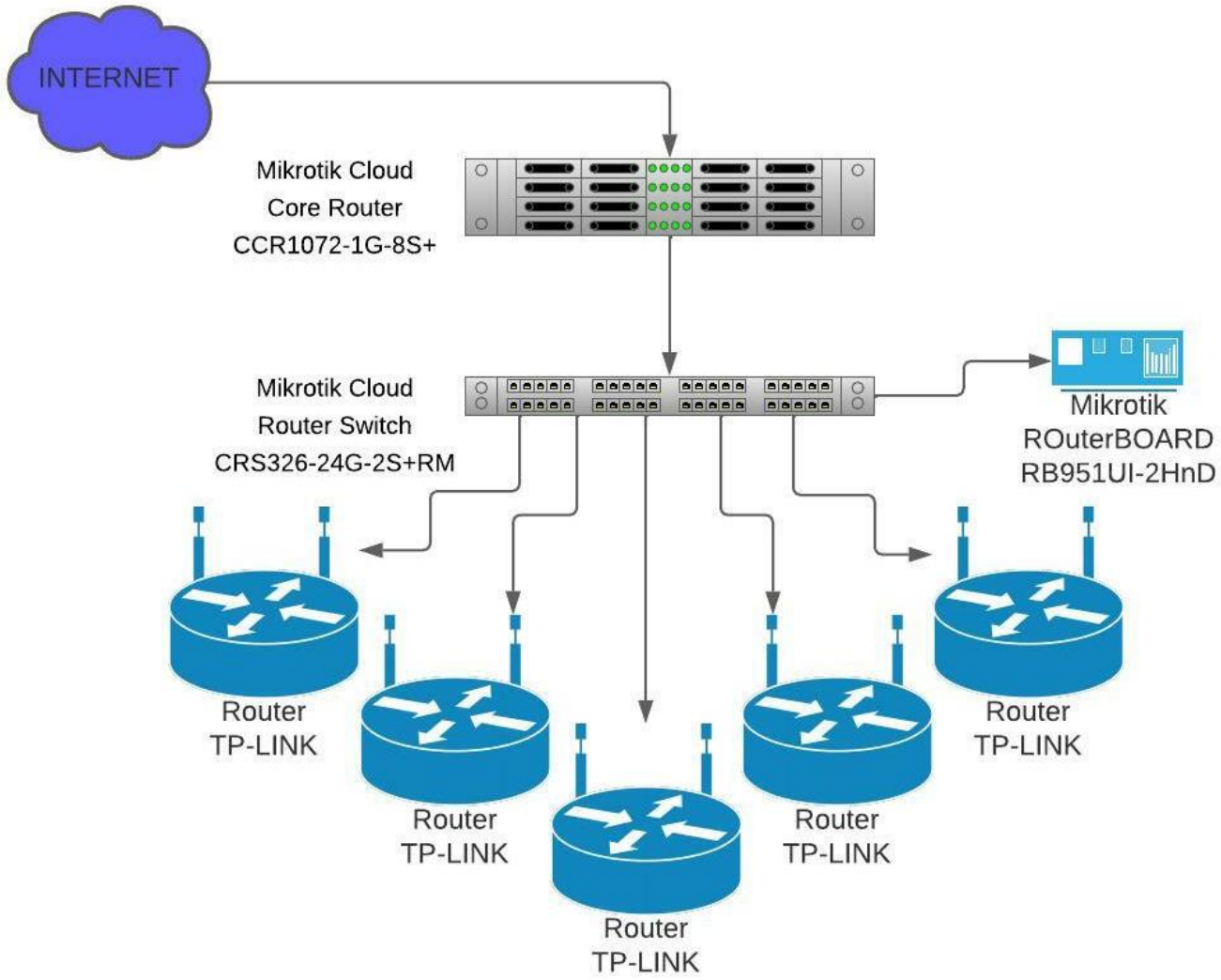
Métodos EAP – Comparación

	Legacy	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-LEAP	EAP-FAST	EAP-SPEKE
Autenticación mutua	No	Sí	Sí	Sí	Sí	Sí	Sí
Entrega de clave dinámica	No	Sí	Sí	Sí	Sí	Sí	Sí
Inmunidad en ataque de diccionario	No	Sí	Sí	Sí	No	Sí	Sí
Inmunidad en ataque MitD	No	Sí	Sí	Sí	No	Sí	Sí
Reautenticación rápida	No	Sí	Sí	Sí	No	Sí	No
Autenticación del servidor	No	Certificado	Certificado	Certificado	Claves de cifrado	PAC	Claves de cifrado
Autenticación del suplicante	Sí	No si el certificado está en el disco	No si el certificado está en el disco	No si el certificado está en el disco	Sí	No si el certificado está en el disco	Sí
Certificado de servidor	No	Requerido	Requerido	Requerido	No	Requerido	Requerido
Certificado de cliente	No	Requerido	Opcional	Opcional	No	Opcional	Requerido
Eficiente	Sí	No	No	No	Sí	No	Sí
Bajo costo	Sí	No	No	No	Sí	Sí	Sí
Amplio soporte de puntos de acceso	Sí	Sí	Sí	Sí	No	No	Sí
Fortaleza general de la seguridad	Mala	Fuerte	Buena	Buena	Buena	Buena	Fuerte

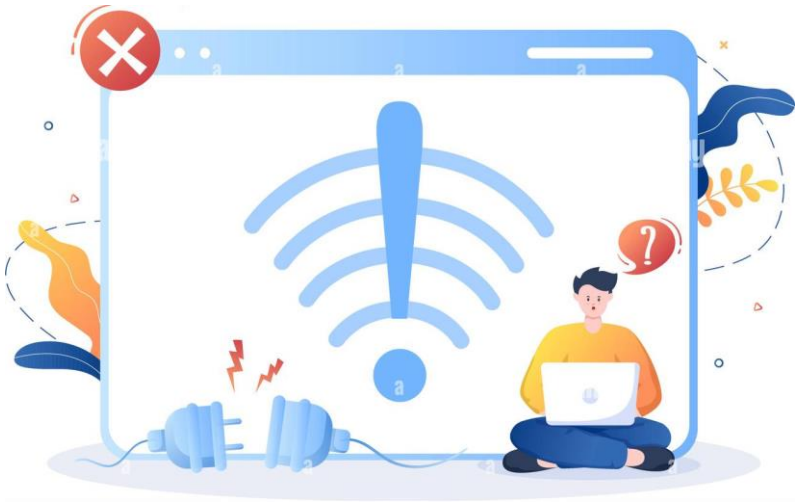
RFC 4017

Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs

Situación actual de Compu Seguridad



La población de la empresa es:
20 empleados
Más de 1500 clientes

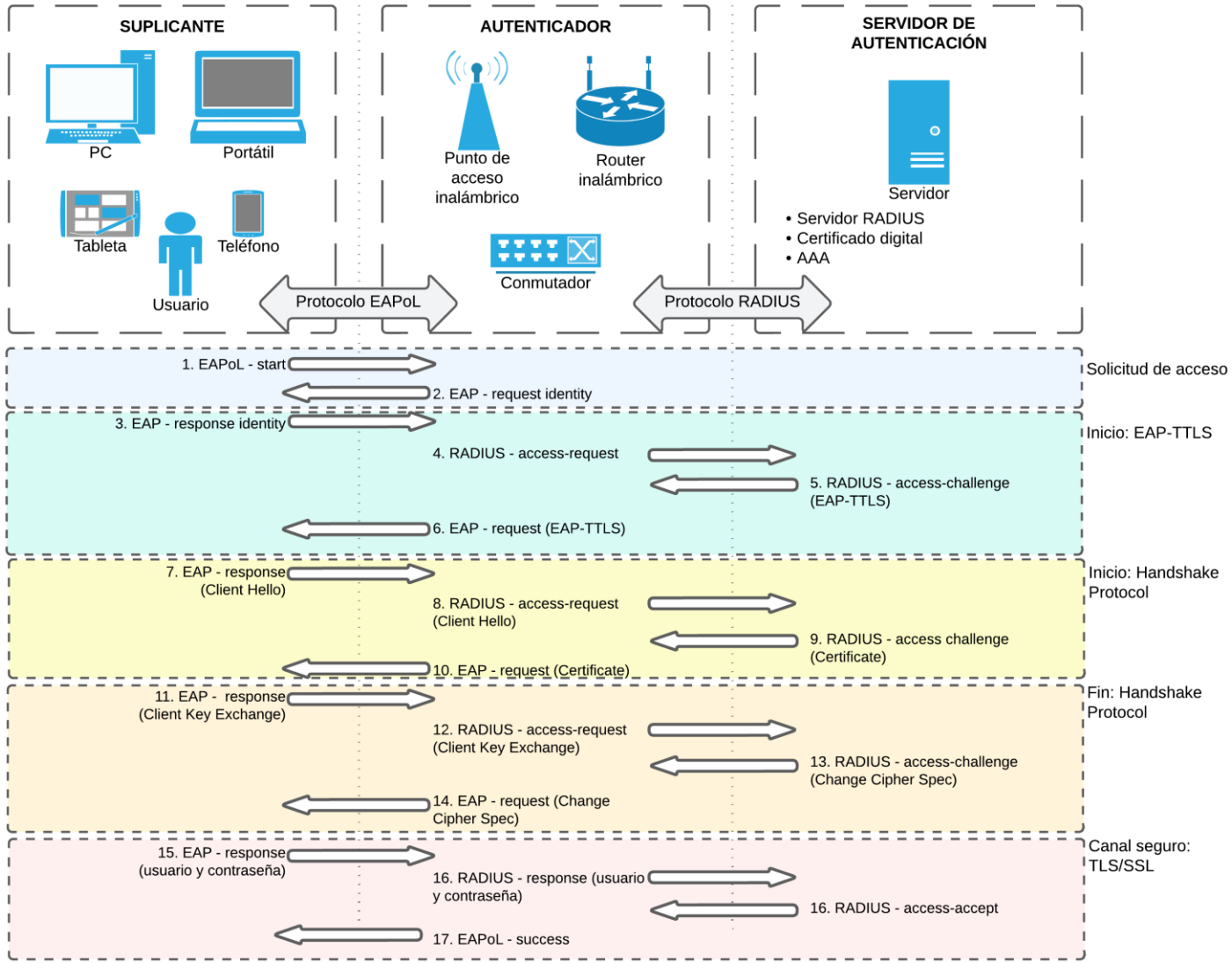


Establecimiento de políticas de seguridad

#	Requerimiento	Prioridad		
		Alta	Media	Baja
1	No exponer al sistema a altas temperaturas ni a humedad.	X		
2	Poseer una conexión estable a internet para el buen funcionamiento del servicio.	X		
3	Se deberá ingresar a la plataforma vía web o WinBox para poder configurar y gestionar el servicio.	X		
4	El sistema depurará a los usuarios que ya no pertenezcan a la empresa legalmente, así como también a los nuevos.	X		
5	La ubicación del sistema deberá encontrarse con los servidores de la empresa.	X		
6	Se requiere un software con soporte AAA (authentication, authorization, accounting).	X		
7	Se requiere compatibilidad entre la infraestructura con la que cuenta la empresa.	X		
8	Se requiere que el sistema siempre este activo.	X		
9	Los empleados tendrán de un ancho de banda de 5M y 10M para subida y descarga de datos, respectivamente.	X		
10	Los clientes dispondrán de un ancho de banda simétrico de 25M, 35M y 60M, por 24 horas. Dependiendo del plan de internet que deseen contratar.	X		
11	Internet inalámbrico gratuito por 30 minutos al día con un ancho de banda de 2M y 5M de subida y descarga de datos, respectivamente.	X		
12	Solo el administrador del servicio podrá modificar, leer o eliminar datos de la base de datos.	X		
13	Solo se permitirá utilizar 1 dispositivo por usuario.	X		
14	Cada usuario dispondrá de un usuario y contraseña única.	X		
15	El tiempo de conexión al recurso estará asignado por el administrador de toda la red según sea necesario.	X		
16	Se requiere de un Hotspot amigable con el usuario	X		

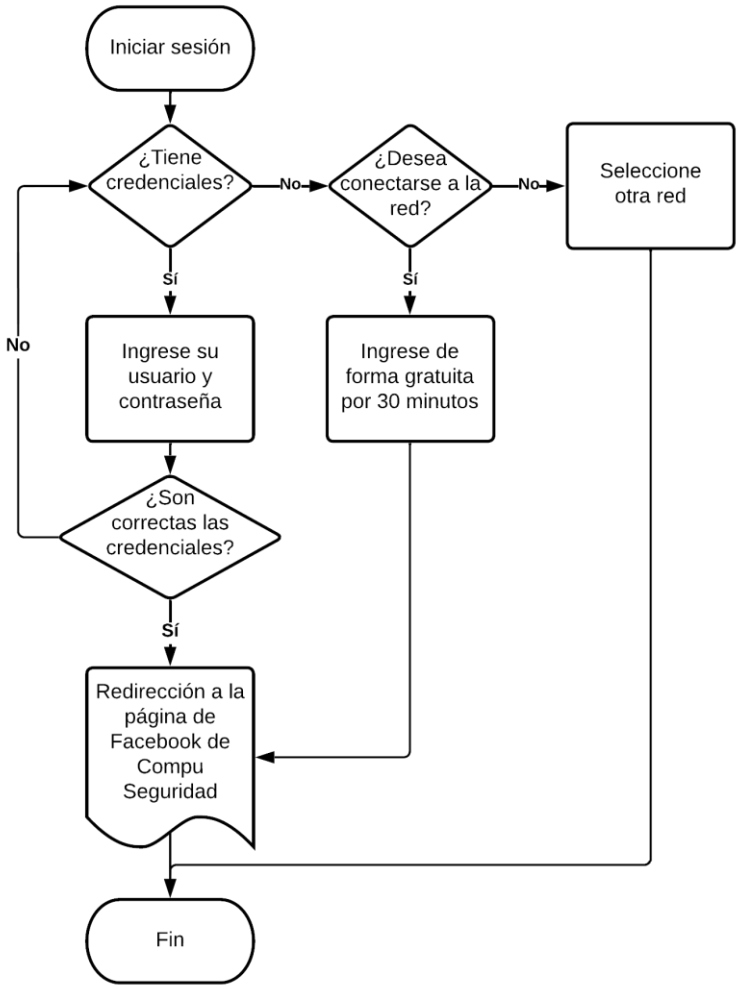
ANÁLISIS Y DISEÑO

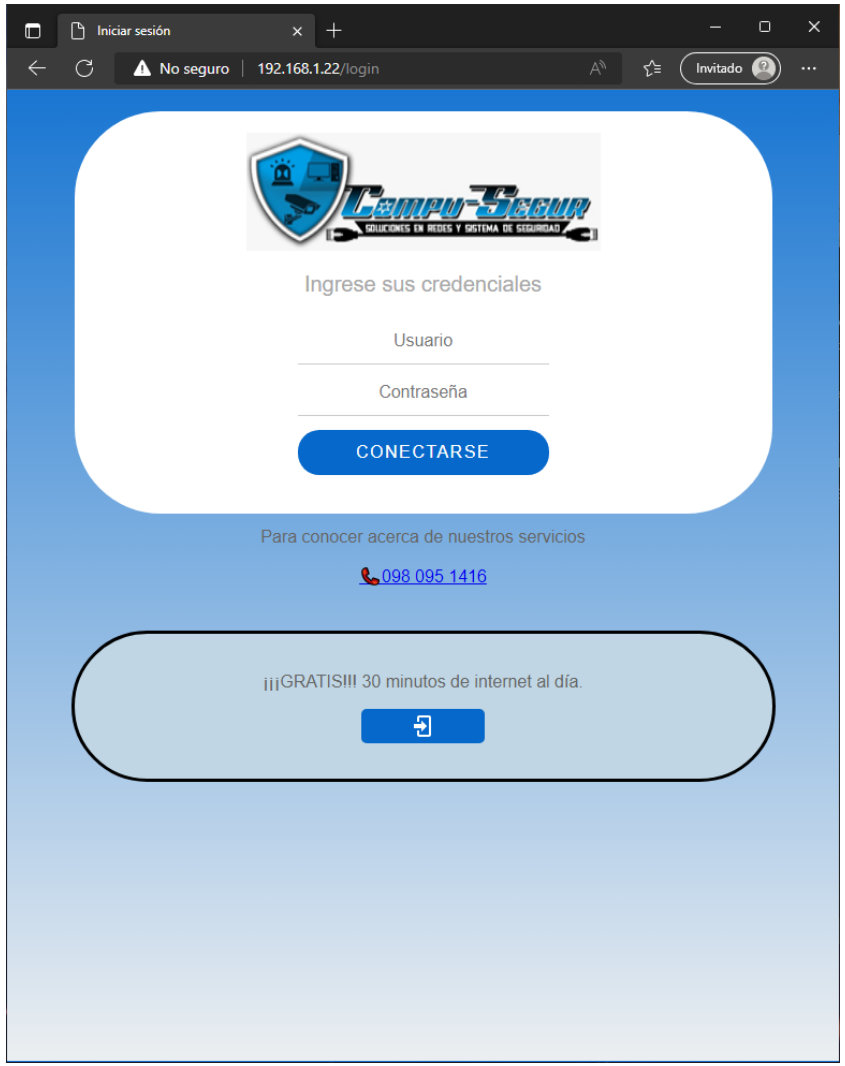
Diseño de la red inalámbrica



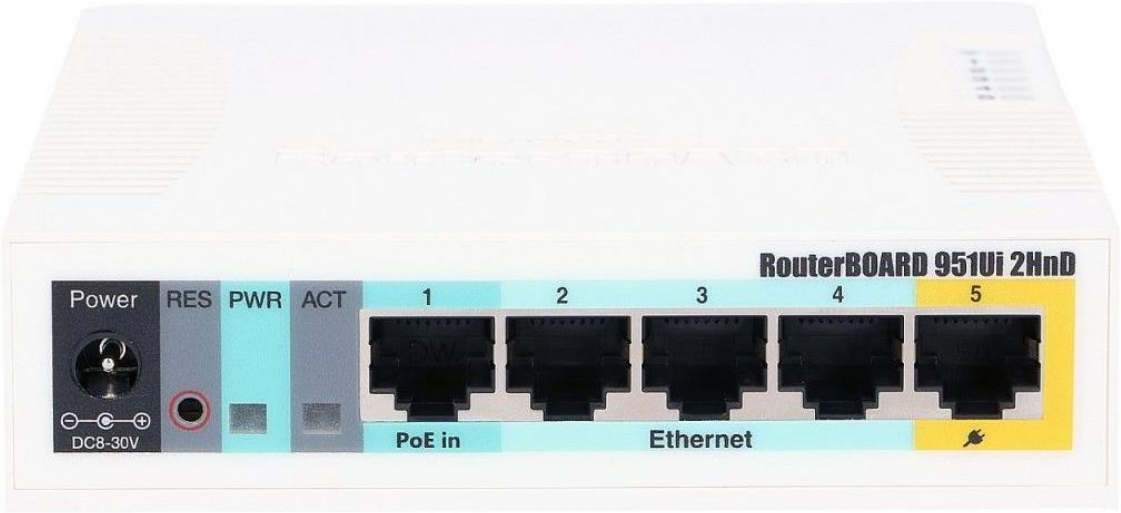
ANÁLISIS Y DISEÑO

Diseño del portal cautivo



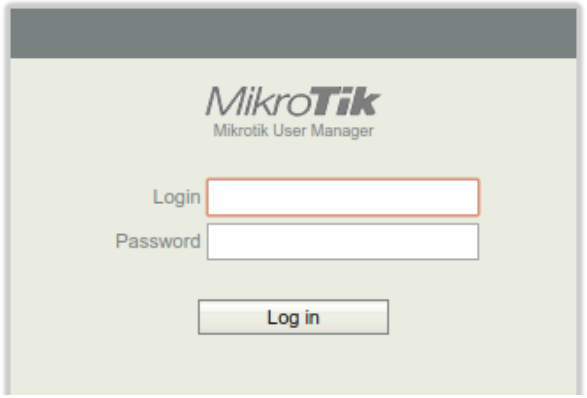


MikroTik RouterBOARD RB951Ui-2HnD

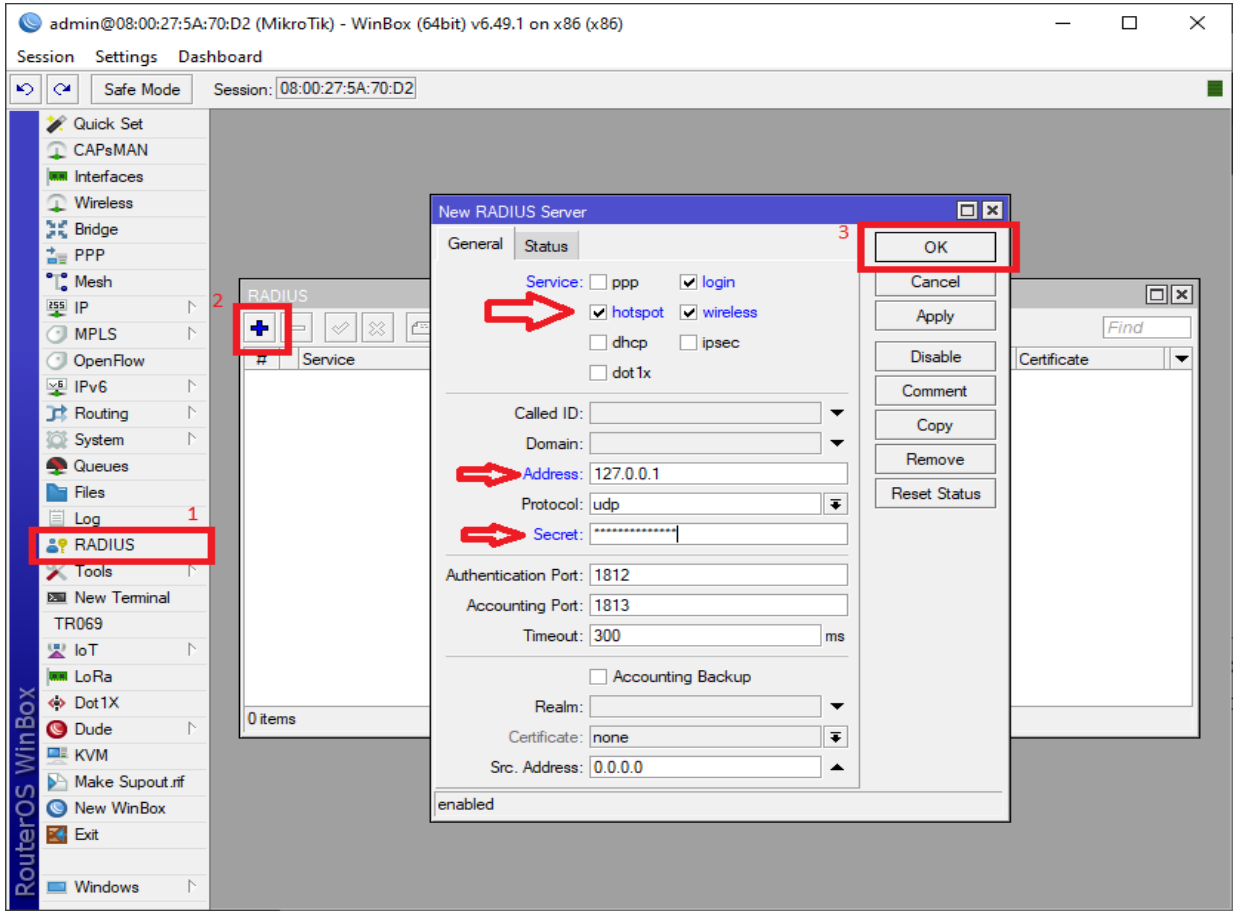


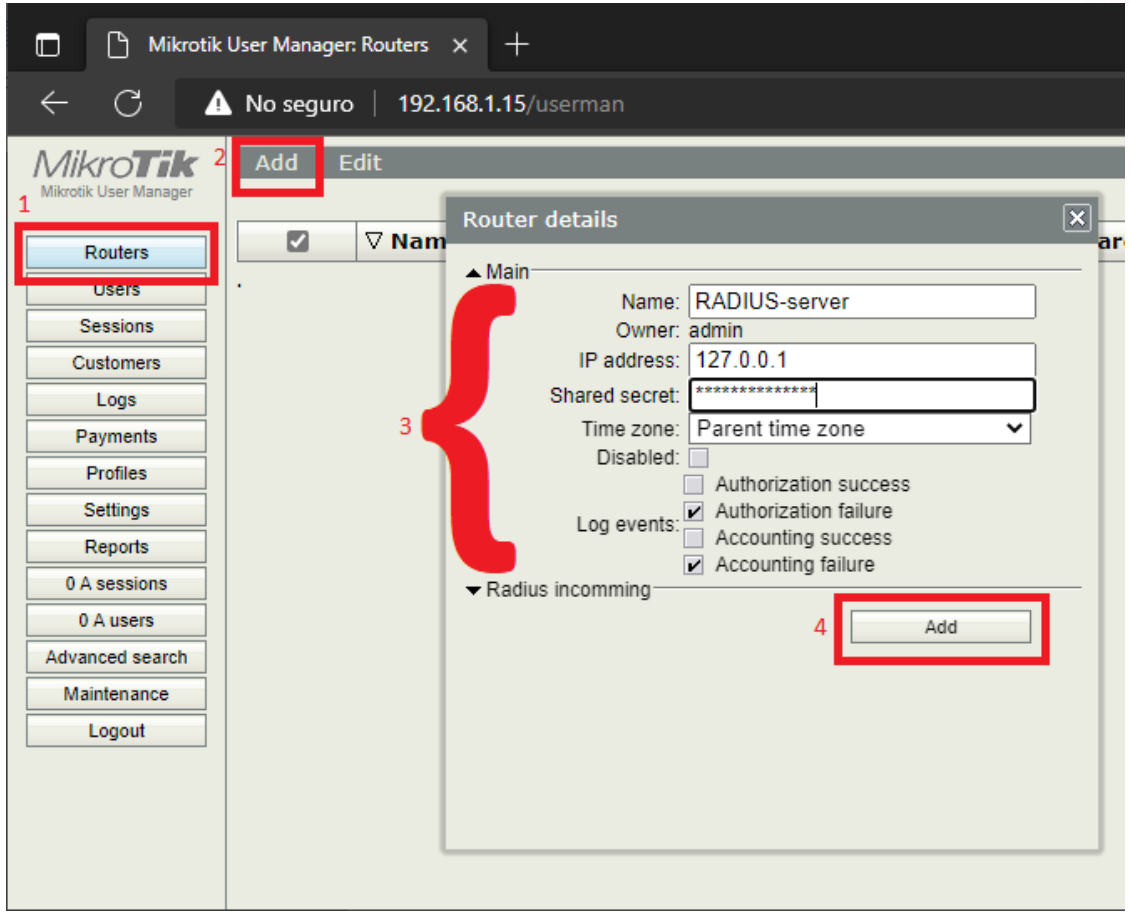
Detalle	Descripción
Código de producto	RB951Ui-2HnD
CPU	AR9344
Núcleos CPU	1
Frecuencia del CPU	600 MHz
Dimensiones	113 x 138 x 29 mm
SO	RouterOS
Licencia	Nivel 4
RAM	128 MB
Almacenamiento interno	128 MB
Tipo de almacenamiento	NAND
Estándares	802.11/b/g/n
Máx tasa de transmisión	300 Mbps
Temperatura de funcionamiento	-20°C a 60°C

Winbox



IMPLEMENTACIÓN RADIUS

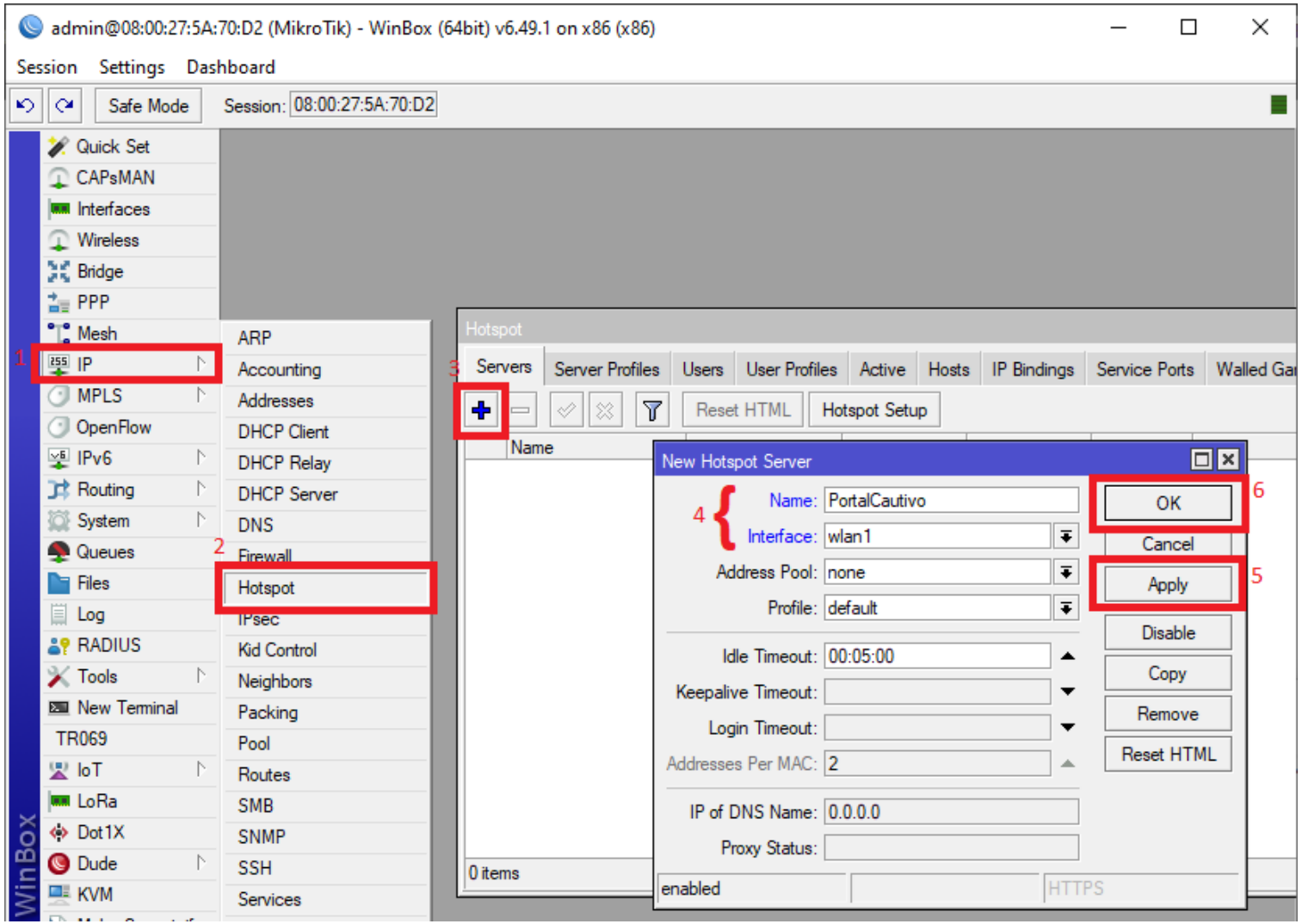




UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

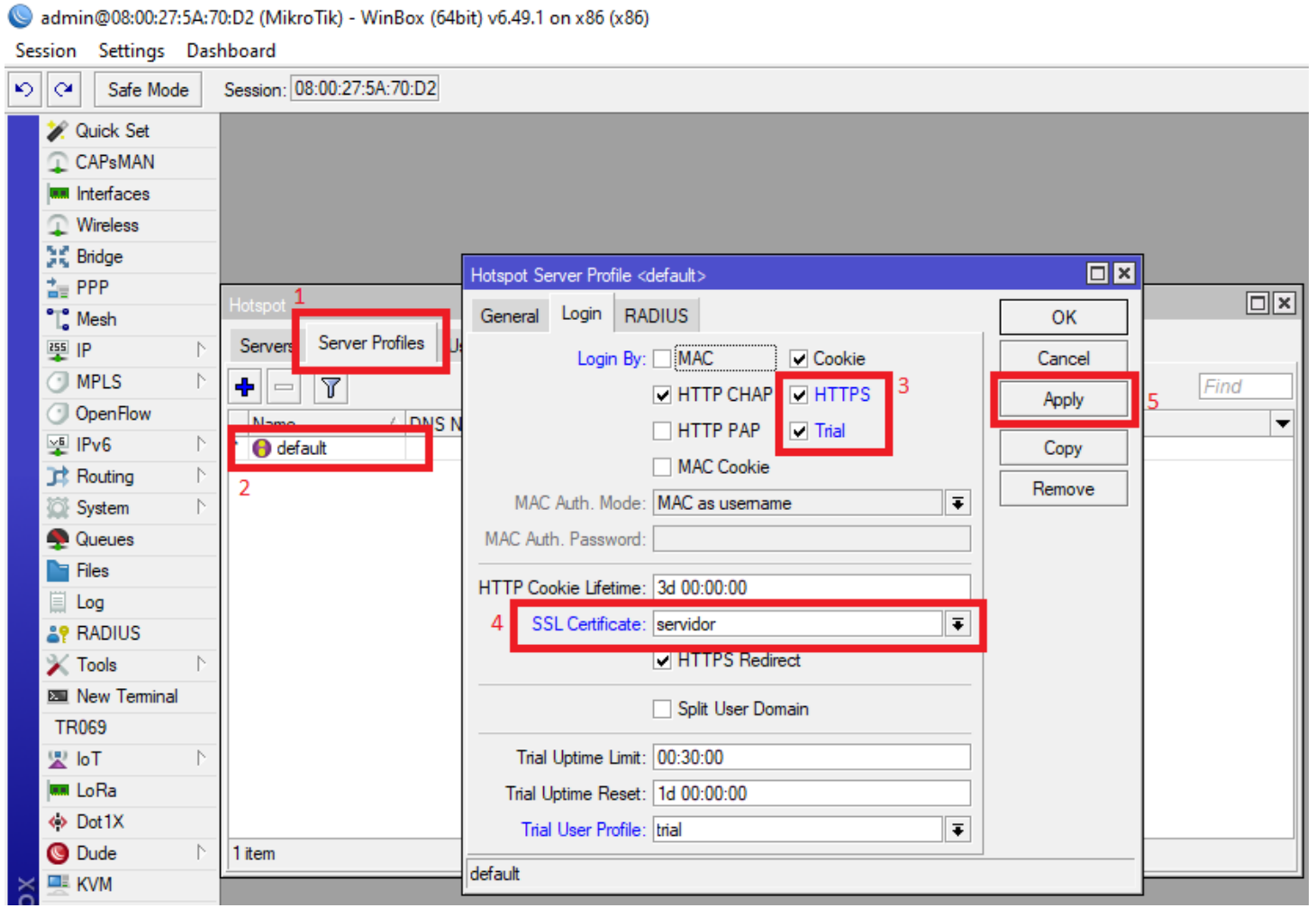
IMPLEMENTACIÓN

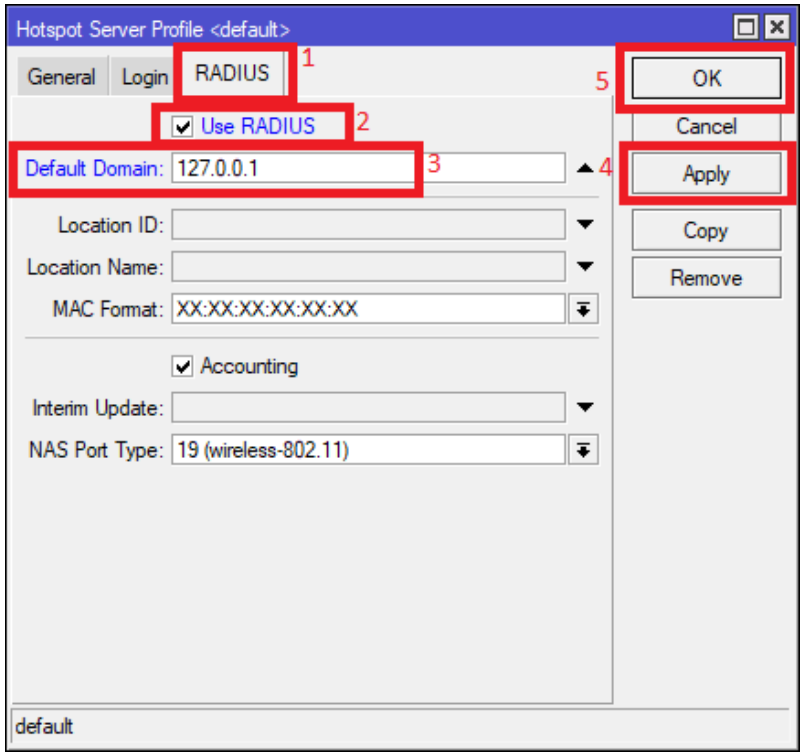
Portal cautivo



IMPLEMENTACIÓN

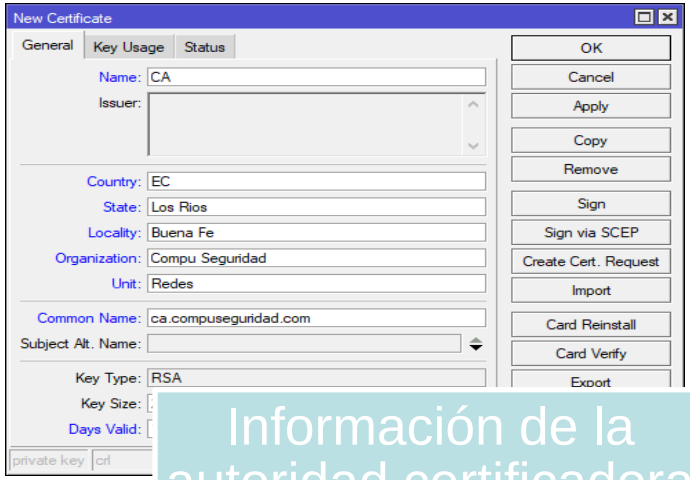
EAP-TTLS



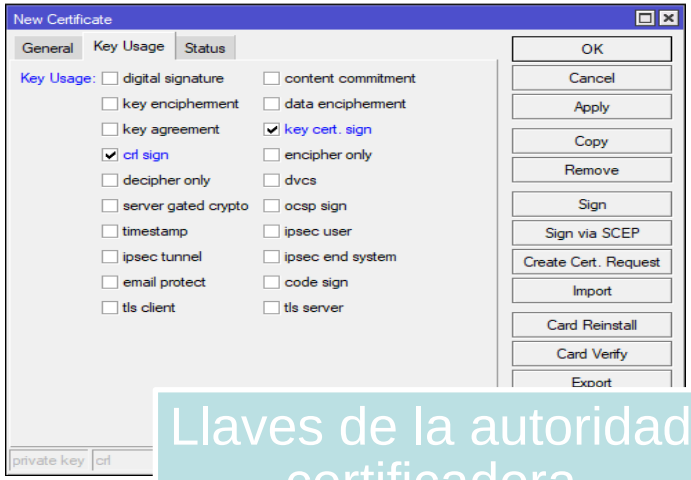


IMPLEMENTACIÓN

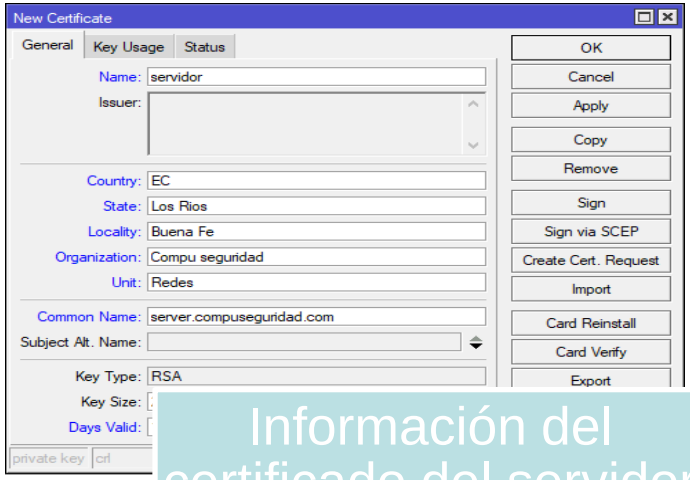
Certificados digitales



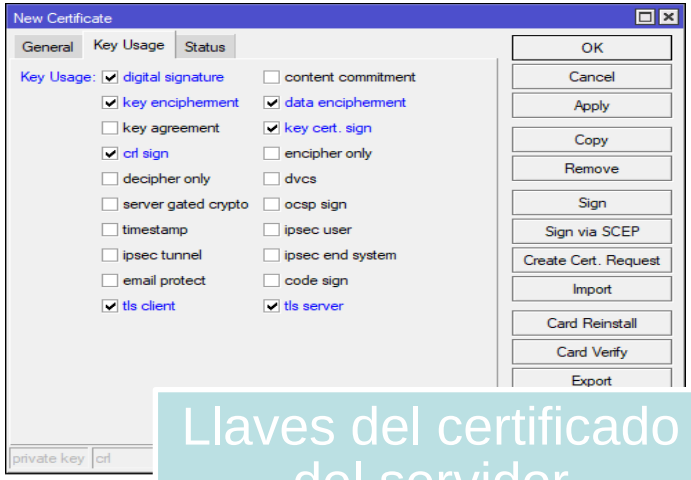
Información de la autoridad certificadora



Llaves de la autoridad certificadora



Información del certificado del servidor

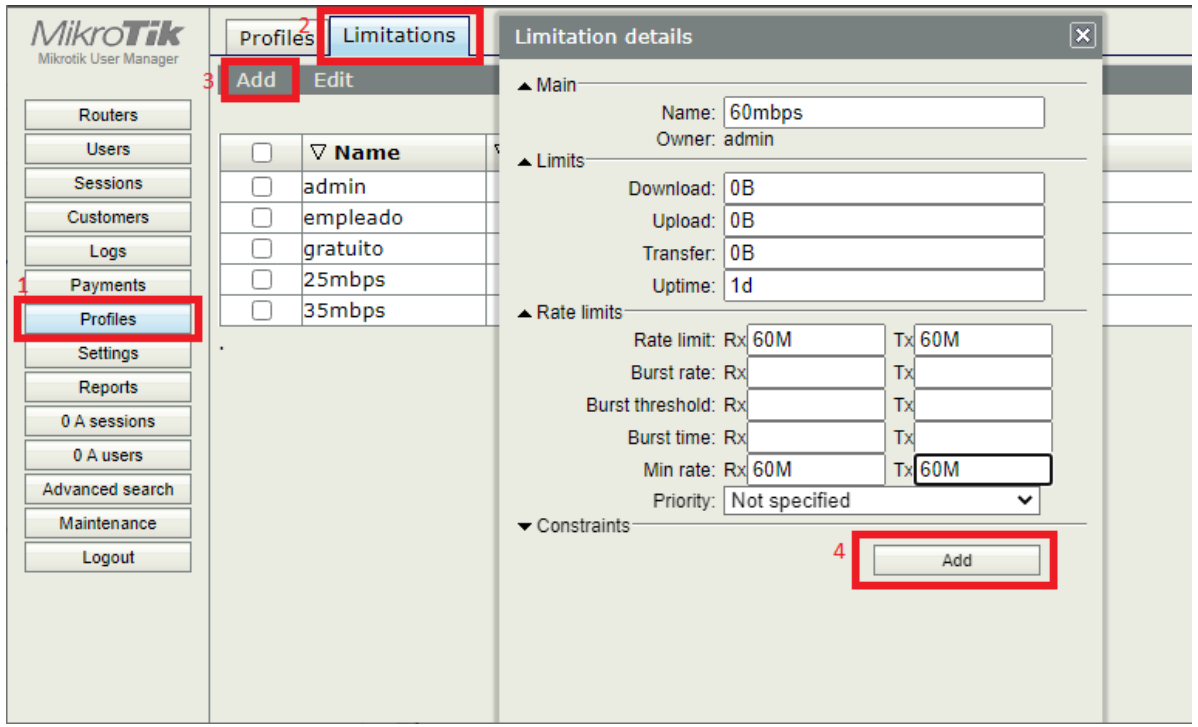


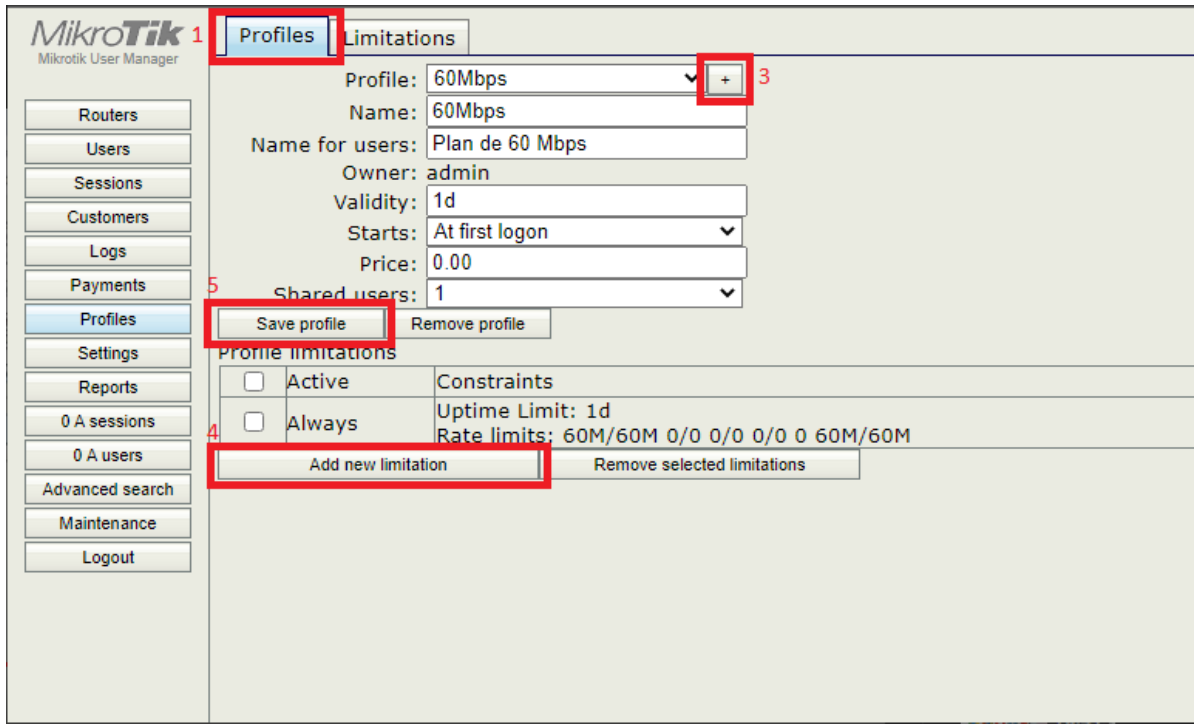
Llaves del certificado del servidor

IMPLEMENTACIÓN

Creación de usuarios

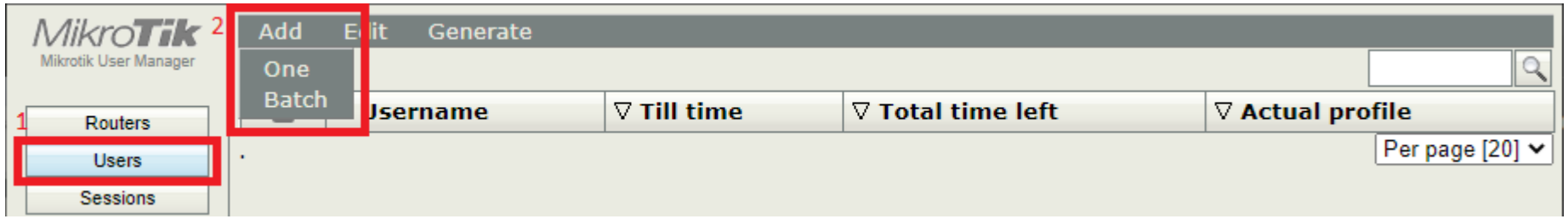
Tipo de usuario	Tiempo de uso	Tasa de transmisión Rx/Tx
Administrador	Ilimitado	50 Mbps / 100 Mbps
Empleado	Ilimitado	5 Mbps / 10 Mbps
Gratuito	30 minutos	2 Mbps / 5 Mbps
Plan 25 Mbps	24 horas	25 Mbps / 25 Mbps
Plan 35 Mbps	24 horas	35 Mbps / 35Mbps
Plan 60 Mbps	24 horas	60 Mbps / 60Mbps



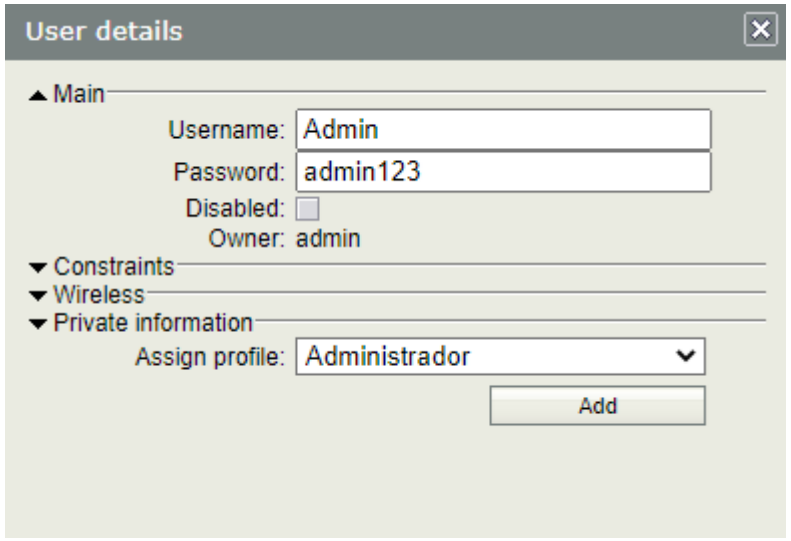


IMPLEMENTACIÓN

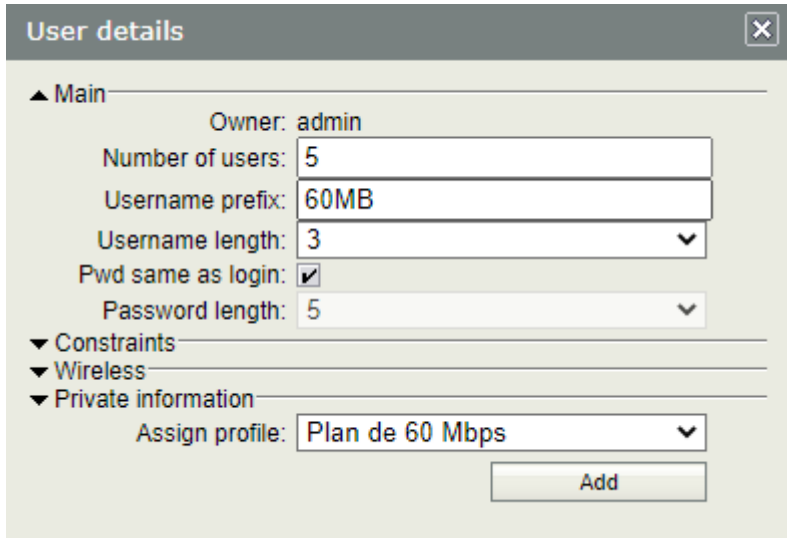
Creación de usuarios



Generación de un usuario

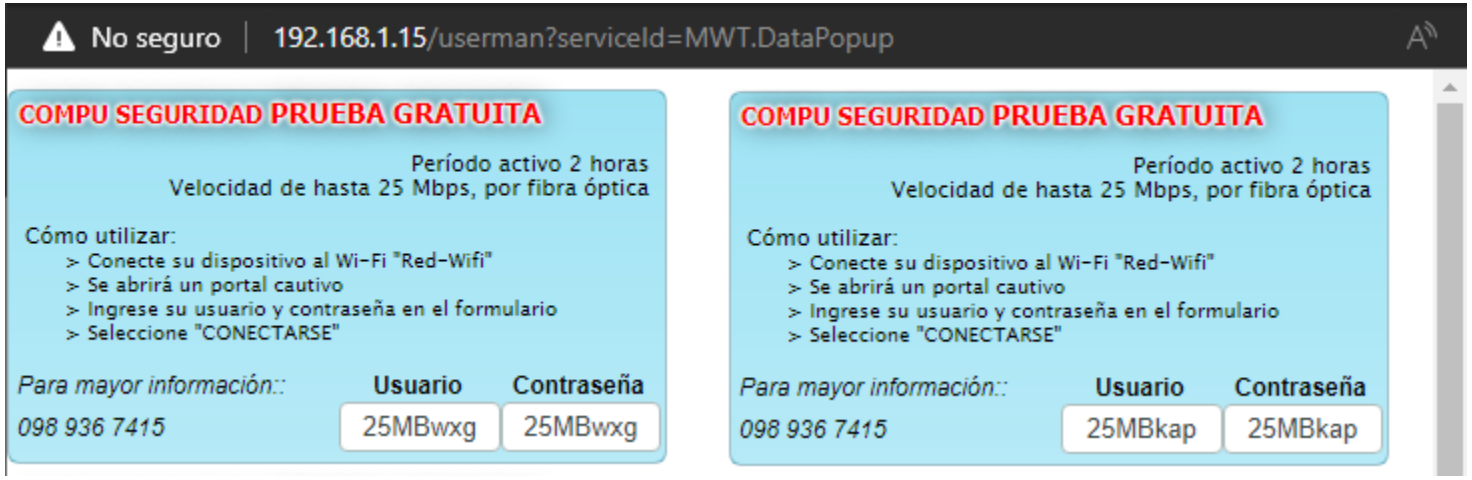


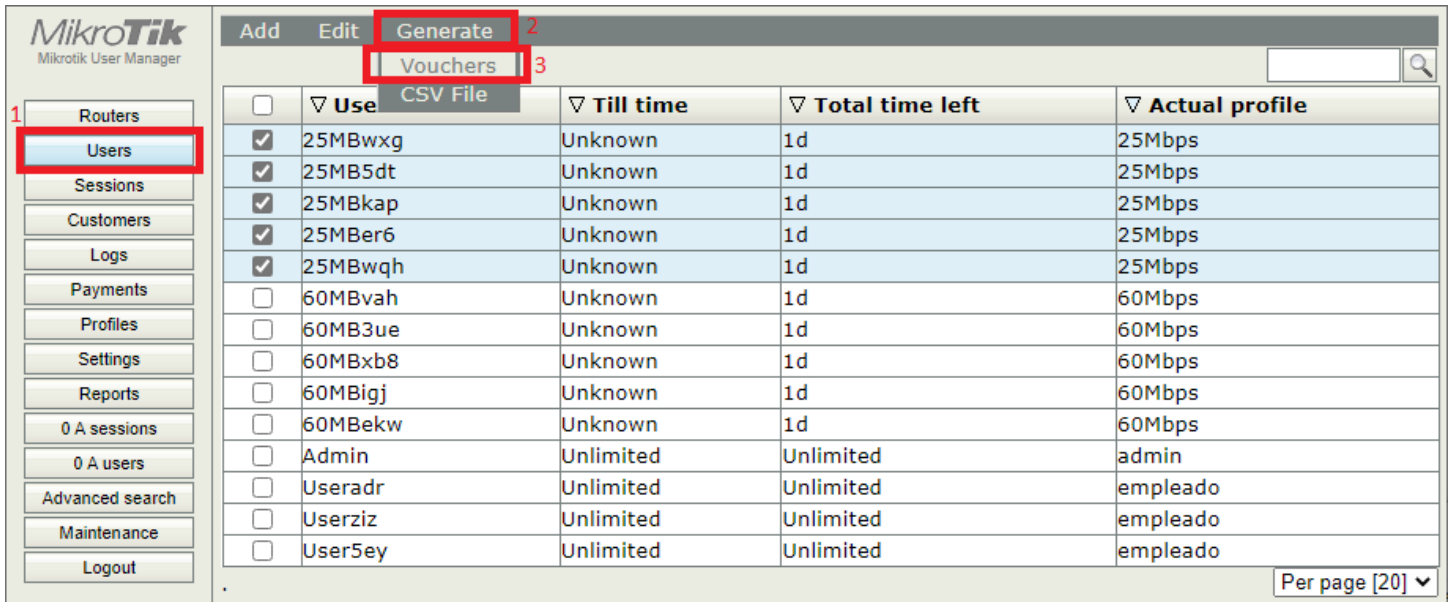
Generación de un grupo de usuarios



IMPLEMENTACIÓN

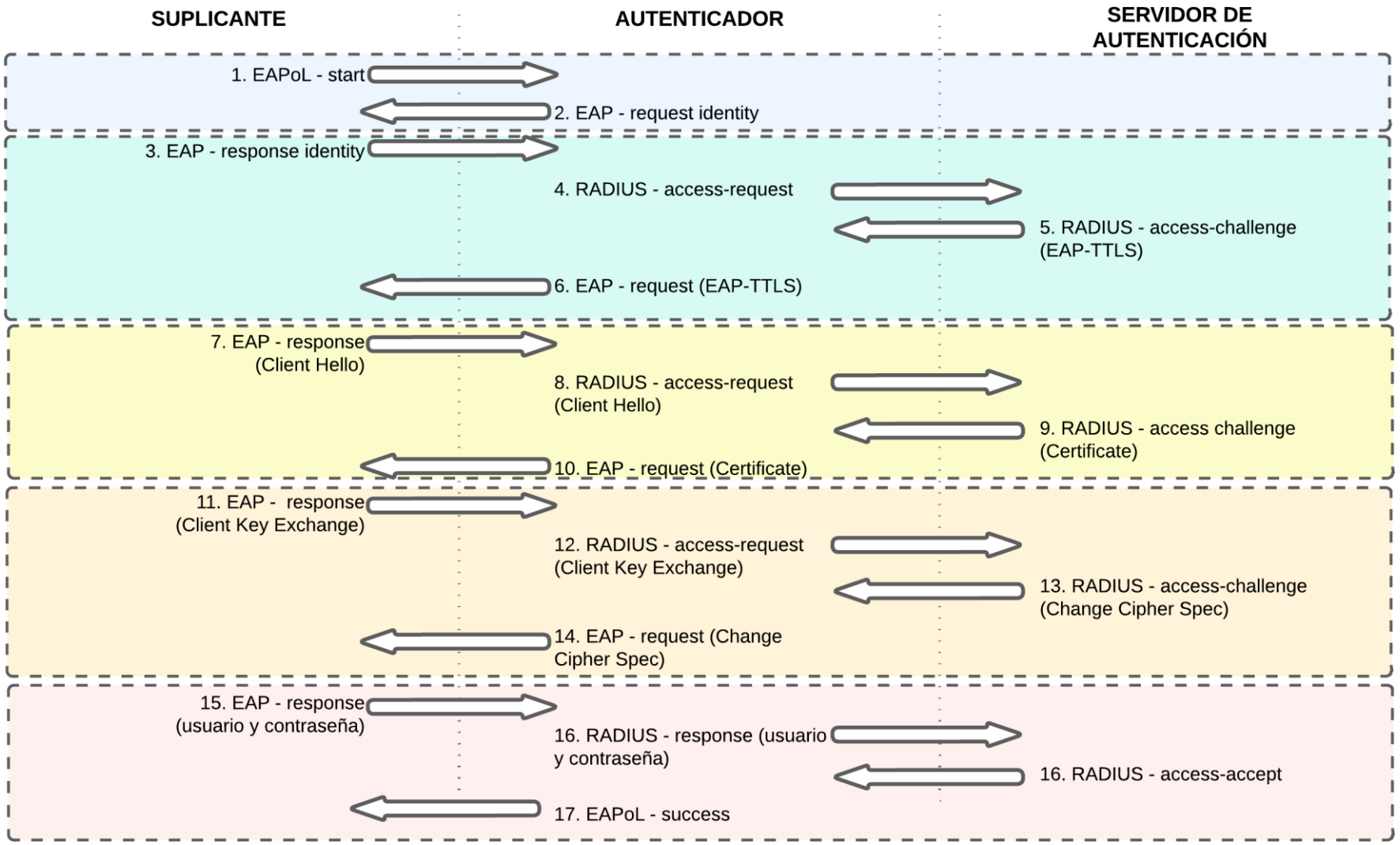
Vouchers





PRUEBAS Y RESULTADOS

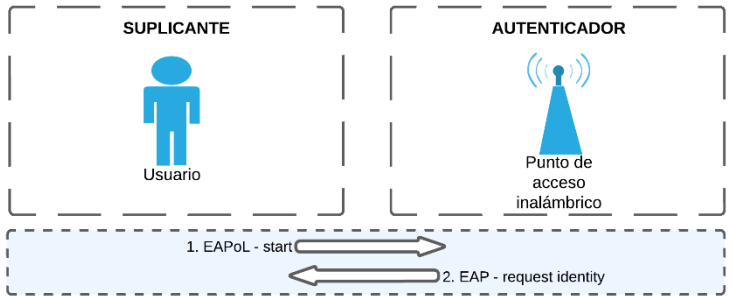
Autenticación EAP-TTLS



PRUEBAS Y RESULTADOS

Autenticación EAP-TTLS

Fase 1. Solicitud de acceso



EAPoL - start

```
No.     Source              Destination         Protocol  Length  Info
      1 00:16:76:d7:47:3f   01:80:c2:00:00:03   EAPOL         19  Start

⊞ Frame 1: 19 bytes on wire (152 bits), 19 bytes captured (152 bits) on interface
⊞ Ethernet II, Src: 00:16:76:d7:47:3f (00:16:76:d7:47:3f), Dst: 01:80:c2:00:00:03
⊟ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Start (1)
    Length: 0
```

EAP – request identity

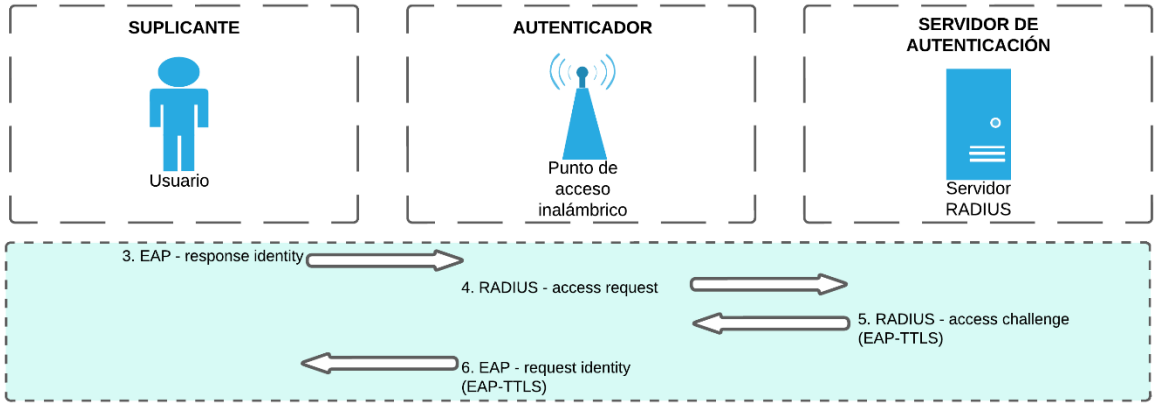
```
No.     Source              Destination         Protocol  Length  Info
      2 10:bd:18:82:11:91   00:16:76:d7:47:3f   EAP           60  Request, Identity

⊞ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on int
⊞ Ethernet II, Src: 10:bd:18:82:11:91 (10:bd:18:82:11:91), Dst: 00:16:76:d7
⊟ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 5
  ⊟ Extensible Authentication Protocol
      Code: Request (1)
      Id: 1
      Length: 5
      Type: Identity (1)
      Identity:
```

PRUEBAS Y RESULTADOS

Autenticación EAP-TTLS

Fase 2. Inicio EAP-TTLS



EAP – response identity

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 14
Extensible Authentication Protocol
    Code: Response (2)
    Id: 1
    Length: 14
    Type: Identity (1)
    Identity: anonymous
```

RADIUS – access-request

```
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 112
    Authenticator: d0580000c31500004044000045320000
    [The response to this request is in frame 114]
Attribute Value Pairs
    AVP: l=6  t=NAS-IP-Address(4): 172.25.1.254
    AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
    AVP: l=6  t=NAS-Port(5): 2
    AVP: l=11  t=User-Name(1): anonymous
    AVP: l=10  t=Acct-Session-Id(44): 05000018
    AVP: l=19  t=Calling-Station-Id(31): 00-16-76-D7-47-3F
    AVP: l=16  t=EAP-Message(79) Last Segment[1]
        EAP fragment
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 2
        Length: 14
        Type: Identity (1)
```

RADIUS – access-challenge (EAP-TTLS)

```
Radius Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x0 (0)
    Length: 64
    Authenticator: 7a01321ed440dd659b73b4646c4096c3
    [This is a response to a request in frame 106]
    [Time from request: 0.112706000 seconds]
Attribute Value Pairs
    AVP: l=8  t=EAP-Message(79) Last Segment[1]
        EAP fragment
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 3
        Length: 6
        Type: Tunneled TLS EAP (EAP-TTLS) (21)
        EAP-TLS Flags: 0x20
```

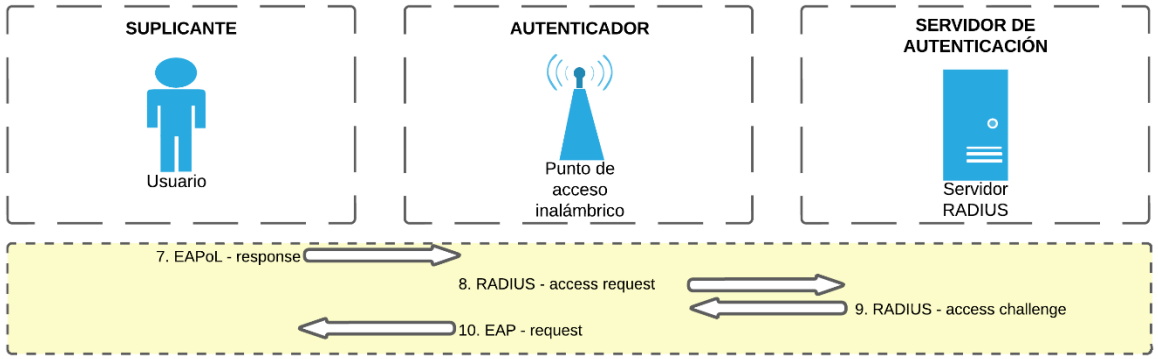
EAP – request idendity (EAP-TTLS)

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 6
Extensible Authentication Protocol
    Code: Request (1)
    Id: 2
    Length: 6
    Type: Tunneled TLS EAP (EAP-TTLS) (21)
```

PRUEBAS Y RESULTADOS

Autenticación EAP-TTLS

Fase 3. Inicio del protocolo Handshake



EAP – response (Client Hello)

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 56
  Extensible Authentication Protocol
    Code: Response (2)
    Id: 2
    Length: 56
    Type: Tunneled TLS EAP (EAP-TTLS) (21)
    EAP-TLS Flags: 0x00
    Secure Sockets Layer
      TLSv1 Record Layer: Handshake Protocol: Client Hello
          Content Type: Handshake (22)
          Version: TLS 1.0 (0x0301)
          Length: 45
        Handshake Protocol: Client Hello
```

RADIUS – access-request

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 1024
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 3
    Length: 1024
    Type: Tunneled TLS EAP (EAP-TTLS) (21)
    EAP-TLS Flags: 0xC0
    EAP-TLS Length: 2106
    [3 EAP-TLS Fragments (2106 bytes): #11(1014), #13(1014), #15(78)]
    Secure Sockets Layer
      TLSv1 Record Layer: Handshake Protocol: Server Hello
      TLSv1 Record Layer: Handshake Protocol: Certificate
      TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

RADIUS – access-request

```
Radius Protocol
  Code: Access-Request (1)
  Packet identifier: 0x0 (0)
  Length: 172
  Authenticator: 84350000597300000b3420000e8530000
  [Duplicate Request: 0]
  [The response to this request is in frame 114]
  Attribute Value Pairs
    AVP: l=6  t=NAS-IP-Address(4): 172.25.1.254
    AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
    AVP: l=6  t=NAS-Port(5): 2
    AVP: l=11  t=User-Name(1): anonymous
    AVP: l=10  t=Acct-Session-Id(44): 05000018
    AVP: l=18  t=State(24): 5bf765115bf4702f187ad3910299607d
    AVP: l=19  t=Calling-Station-Id(31): 00-16-76-D7-47-3F
    AVP: l=58  t=EAP-Message(79) Last Segment[1]
      EAP fragment
      Extensible Authentication Protocol
        Code: Response (2)
        Id: 3
        Length: 56
        Type: Tunneled TLS EAP (EAP-TTLS) (21)
        EAP-TLS Flags: 0x00
        Secure Sockets Layer
          TLSv1 Record Layer: Handshake Protocol: Client Hello
              Content Type: Handshake (22)
              Version: TLS 1.0 (0x0301)
              Length: 45
            Handshake Protocol: Client Hello
```

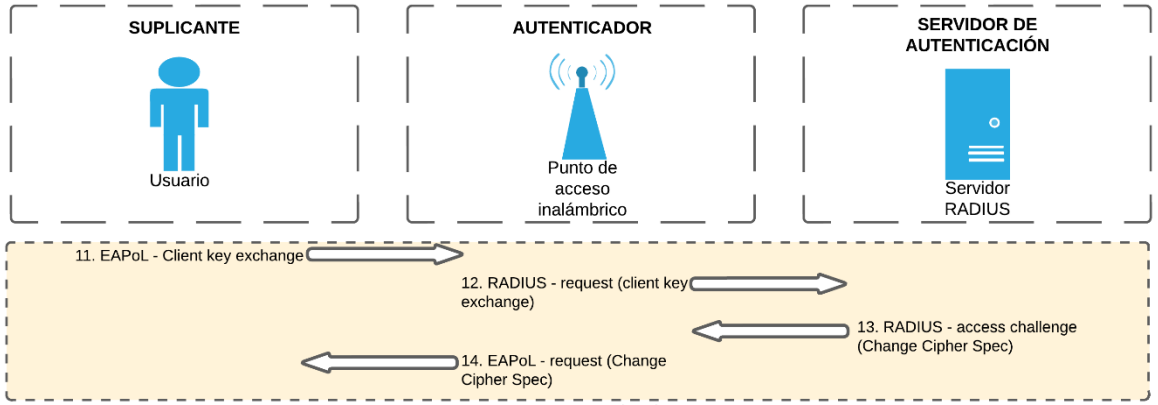
RADIUS – access-challenge (Server Hello, Certificate, etc)

```
Radius Protocol
  Code: Access-Challenge (11)
  Packet identifier: 0x0 (0)
  Length: 1090
  Authenticator: f03bb59749f99401f0cf58963e664fc2
  [This is a response to a request in frame 106]
  [Time from request: 0.156620000 seconds]
  [Duplicate Response: 0]
  Attribute Value Pairs
    AVP: l=255  t=EAP-Message(79) Segment[1]
    AVP: l=255  t=EAP-Message(79) Segment[2]
    AVP: l=255  t=EAP-Message(79) Segment[3]
    AVP: l=255  t=EAP-Message(79) Segment[4]
    AVP: l=14  t=EAP-Message(79) Last Segment[5]
      EAP fragment
      Extensible Authentication Protocol
        Code: Request (1)
        Id: 4
        Length: 1024
        Type: Tunneled TLS EAP (EAP-TTLS) (21)
        EAP-TLS Flags: 0xC0
        EAP-TLS Length: 2106
        [3 EAP-TLS Fragments (2106 bytes): #117(1014), #119(1014), #121(78)]
        Secure Sockets Layer
          TLSv1 Record Layer: Handshake Protocol: Server Hello
          TLSv1 Record Layer: Handshake Protocol: Certificate
          TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

PRUEBAS Y RESULTADOS

Autenticación EAP-TTLS

Fase 4. Fin del protocolo Handshake



EAP – response (Client Key Exchange)

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 196
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 5
        Length: 196
        Type: Tunneled TLS EAP (EAP-TTLS) (21)
        EAP-TLS Flags: 0x00
        Secure Sockets Layer
            TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
            TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
                Content Type: Change Cipher Spec (20)
                Version: TLS 1.0 (0x0301)
                Length: 1
                Change Cipher Spec Message
            TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
                Content Type: Handshake (22)
                Version: TLS 1.0 (0x0301)
                Length: 40
                Handshake Protocol: Encrypted Handshake Message
```

RADIUS – access-request

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 61
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 6
        Length: 61
        Type: Tunneled TLS EAP (EAP-TTLS) (21)
        EAP-TLS Flags: 0x80
        EAP-TLS Length: 51
        Secure Sockets Layer
            TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
```

RADIUS – access-request

```
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 312
    Authenticator: 7f43000082340000c16400009f720000
    [Duplicate Request: 0]
    [The response to this request is in frame 114]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 172.25.1.254
        AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
        AVP: l=6  t=NAS-Port(5): 2
        AVP: l=11  t=User-Name(1): anonymous
        AVP: l=10  t=Acct-Session-Id(44): 05000018
        AVP: l=18  t=State(24): 5bf7651158f1702f187ad3910299607d
        AVP: l=19  t=Calling-Station-Id(31): 00-16-76-D7-47-3F
        AVP: l=198  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Response (2)
                Id: 6
                Length: 196
                Type: Tunneled TLS EAP (EAP-TTLS) (21)
                EAP-TLS Flags: 0x00
                Secure Sockets Layer
                    TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
                    TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
                    TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

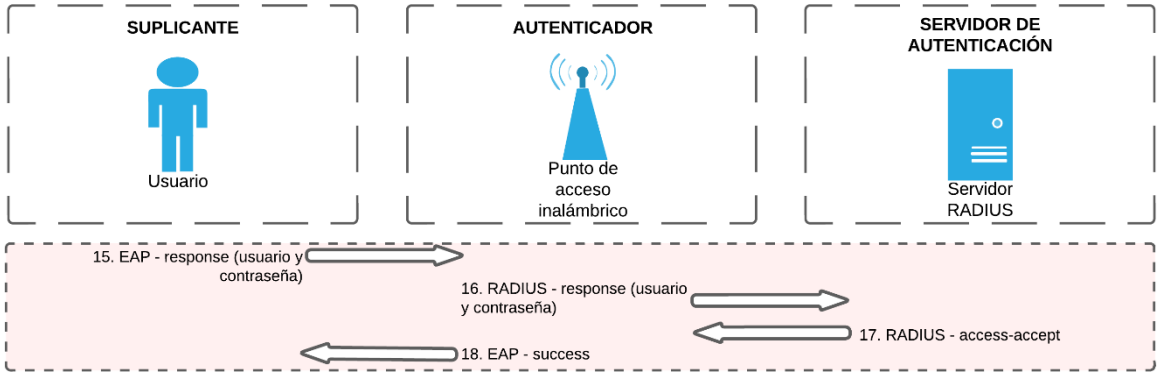
RADIUS – access-challenge (Change Cipher Spec)

```
Radius Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x0 (0)
    Length: 119
    Authenticator: 03e0e4f0409a968cbcea2e507885ae71
    [This is a response to a request in frame 106]
    [Time from request: 0.698469000 seconds]
    [Duplicate Response: 0]
    Attribute Value Pairs
        AVP: l=63  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Request (1)
                Id: 7
                Length: 61
                Type: Tunneled TLS EAP (EAP-TTLS) (21)
                EAP-TLS Flags: 0x80
                EAP-TLS Length: 51
                Secure Sockets Layer
                    TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
```

PRUEBAS Y RESULTADOS

Autenticación EAP-TTLS

Fase 5. Transmisión de credenciales



EAP – response (usuario y contraseña)

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 67
Extensible Authentication Protocol
    Code: Response (2)
    Id: 6
    Length: 67
    Type: Tunneled TLS EAP (EAP-TTLS) (21)
  ⊞ EAP-TLS Flags: 0x00
  ⊟ Secure Sockets Layer
    ⊟ TLSv1 Record Layer: Application Data Protocol: Application Data
```

RADIUS – response (usuario y contraseña)

```
⊟ Extensible Authentication Protocol
    Code: Response (2)
    Id: 7
    Length: 67
    Type: Tunneled TLS EAP (EAP-TTLS) (21)
  ⊞ EAP-TLS Flags: 0x00
  ⊟ Secure Sockets Layer
    ⊟ TLSv1 Record Layer: Application Data Protocol: Application Data
        Content Type: Application Data (23)
        Version: TLS 1.0 (0x0301)
        Length: 56
        Encrypted Application Data: 966149761352ce60d67d35ccdaa844c7b578ad5d31735ec8...
```

EAP – response (usuario y contraseña)

```
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 171
    Authenticator: 73f5d7cd24df6aacc7e247f945af0f6a
    [This is a response to a request in frame 1061]
    [Time from request: 0.719138000 seconds]
    [Duplicate Response: 0]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊟ AVP: l=6  t=EAP-Message(79) Last Segment[1]
        EAP fragment
      ⊟ Extensible Authentication Protocol
          Code: Success (3)
          Id: 7
          Length: 4
    ⊞ AVP: l=18  t=Message-Authenticator(80): 9c95b8f1b1d50e66cf0afae57dabed80
    ⊞ AVP: l=11  t=User-Name(1): anonymous
```

EAP - success

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 4
Extensible Authentication Protocol
    Code: Success (3)
    Id: 6
    Length: 4
```

CONCLUSIONES

- El estudio del desempeño de los sistemas de autenticación EAP (Extensible Authentication Protocol) del estándar de seguridad IEEE 802.1X de este trabajo de investigación, ha permitido identificar una serie de criterios que se pueden usar para comparar diferentes métodos EAP. Estos criterios fueron identificados con la ayuda de la norma RFC 4017 EAP Method Requirements for Wireless LANs desarrollada por la IETF (Internet Engineering Task Force). Y así tuvo lugar el desarrollo de un análisis comparativo de los métodos EAP en función de la seguridad, resistencia a ataques informáticos, ocultación de identidad en la red, reconexión rápida, costos computacionales, entre otros criterios.
- Analizando la situación inicial de la infraestructura inalámbrica en la empresa Compu Seguridad, se determinó un alto nivel de vulnerabilidad, teniendo como seguridad inalámbrica una configuración de LAN de hogar. Para un ISP (Internet Service Provider), estas vulnerabilidades son blanco perfecto para ataques cibernéticos, los cuales pueden acarrear varias pérdidas de datos y económicas.
- Mediante el estado del arte de este trabajo de investigación se logró determinar las políticas de seguridad más relevantes para un ISP. Con la implementación del estándar de seguridad 802.1X y el sistema AAA en una WLAN, se puede mejorar el nivel de autenticación, tener un control sobre los usuarios que acceden a la red y crear políticas de seguridad que restrinjan el uso de la infraestructura inalámbrica. Con la finalidad de controlar la información que viaja por la red interna de la empresa Compu Seguridad.

CONCLUSIONES

- Para la empresa Compu Seguridad se determinó que el método más adecuado de autenticación es el EAP-TTLS. Este mecanismo de autenticación es compatible con todos los dispositivos y la infraestructura interna de red inalámbrica. Este método EAP crea un canal seguro entre los suplicantes y el servidor RADIUS mediante certificados digitales, los cuales garantizan que los datos brindados en el proceso de autenticación se mantengan cifrados.
- Se diseño e implementó en la empresa Compu Seguridad un sistema de autenticación EAP-TTLS, mediante el estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el sistema AAA y así brindar los servicios de red. La infraestructura de red inalámbrica de la empresa fue reutilizada y configurada para mejorar los protocolos de seguridad de la red.
- El servidor de autenticación o servidor RADIUS que se utilizó en la empresa Compu Seguridad fue a través del dispositivo MikroTik RouterBOARD RB951Ui-2HnD, el cual mediante la herramienta User Manager (UM) se aplicó los criterios de un sistema AAA que son autenticar, autorizar y contabilizar a los usuarios que se conectan a la red interna de la empresa.
- Se definieron los permisos de usuario dependiendo del nivel dentro de la empresa y del uso que le dará a la red. Así fue como se limitó el uso de tiempo, de tasa de transmisión, de dispositivos que pueda conectar a la red y de expiración de credenciales.

CONCLUSIONES

- Se realizó el portal cautivo a partir de la plantilla que entrega el dispositivo MikroTik RouterBOARD RB951Ui-2HnD, agregando información de importancia para la empresa y haciendo anuncios de los servicios que brinda esta. Asimismo, se utilizó la plantilla de vouchers del dispositivo de MikroTik para generar boletos con credenciales para poder ingresar a la red.
- Finalmente, se evaluó el diseño y se analizó el correcto funcionamiento de la red inalámbrica con autenticación EAP-TTLS bajo el protocolo IEEE 802.1X, con la incorporación de un portal cautivo. Se utilizó herramienta Wireshark para capturar los paquetes que viajan entre el suplicante, autenticador y servidor de autenticación, y compararlos con la literatura del protocolo RADIUS. Obteniendo como resultado al sistema de red funcionando perfectamente.

RECOMENDACIONES Y TRABAJOS FUTUROS

- Se recomienda realizar una capacitación a los técnicos de redes de la empresa Compu Seguridad, en los temas de Cyber Ops, protocolos de redes inalámbricas y fundamentos de RouterOS.
- Se recomienda realizar verificaciones periódicas de los dispositivos que se conectan a la red inalámbrica, para determinar anomalías que se pueden presentar en el sistema.
- Se recomienda tener el software de los diferentes dispositivos actualizados, con la finalidad de poder parchar vulnerabilidades que se pueden presentar.
- Si se va a aumentar la infraestructura de la red inalámbrica se recomienda analizar el datasheet de los dispositivos que se desean adquirir, para comprobar que sean compatibles con el sistema implementado.
- Tener en cuenta el tiempo de validez de los certificados digitales, ya que, si se pasa el tiempo de vida útil, se vuelven obsoletas y podrían corromper al sistema.
- Se recomienda socializar el nuevo sistema implementado en la empresa con todos los trabajadores de la misma. Así mismo realizar una campaña para los clientes, que estos conozcan las nuevas características inalámbricas en las oficinas.
- Desarrollar un sistema de autenticación EAP basado en contraseñas seguras.
- Evaluar el desempeño de servidores de autenticación gratuitos y con licencia, mediante la aplicación de un sistema AAA para una red inalámbrica.

UNIVERSIDAD DE LAS FUERZAS ARMADAS - “ESPE”

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

“EVALUACIÓN DEL DESEMPEÑO DE LOS SISTEMAS DE AUTENTICACIÓN DEL ESTÁNDAR DE SEGURIDAD IEEE 802.1X PARA LA INTEGRACIÓN DE UN PORTAL CAUTIVO BAJO EL PROTOCOLO DE RADIUS”

AUTOR: ÁLVAREZ MISE LUIS FERNANDO

DIRECTOR: ING. ROMERO GALLARDO CARLOS GABRIEL

QUITO-ECUADOR
2022

VERSIÓN: 1.1