Wireless WPA2 EAP en Mikrotik

Casos de Uso con Windows Server y FreeRadius

By Freddy Bohorquez Quevedo
TecTel

Tectel / Distratel

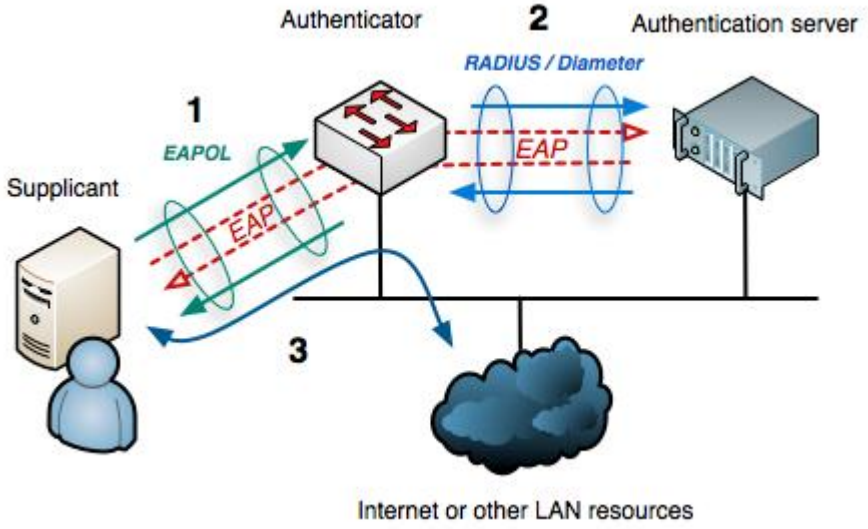
- 2004 Redes Inalámbricas Comunitarias
- 2005 Conectividad Rural
- Primeras Instalaciones basadas en WRAP/Mikrotik
- Despliegue de Redes PtP y PtMP: Públicas, Privadas, Comunitarias
- 2009 inicia Tectel como empresa especializada en Tecnología y Telecomunicaciones y Distribuidor de Mikrotik
- 2014 se crea Distratel, incorporando soluciones en control y automatización.

IEEE 802.11i

- R.I.P. WEP (Wired Equivalent Privacy)
- 2001 IEEE crea el Grupo de Trabajo 802.11i cuya tarea principal era hacer una nueva norma de facto segura.
- Ante la demora del IEEE 802.11i la Industria creó un estándar propio el WPA (Wireless Protected Access)
- En junio del 2004 por fin el stándard fue aprobado y la Industria le dio el nombre de WPA2, compatible con 802.11i y con WPA.

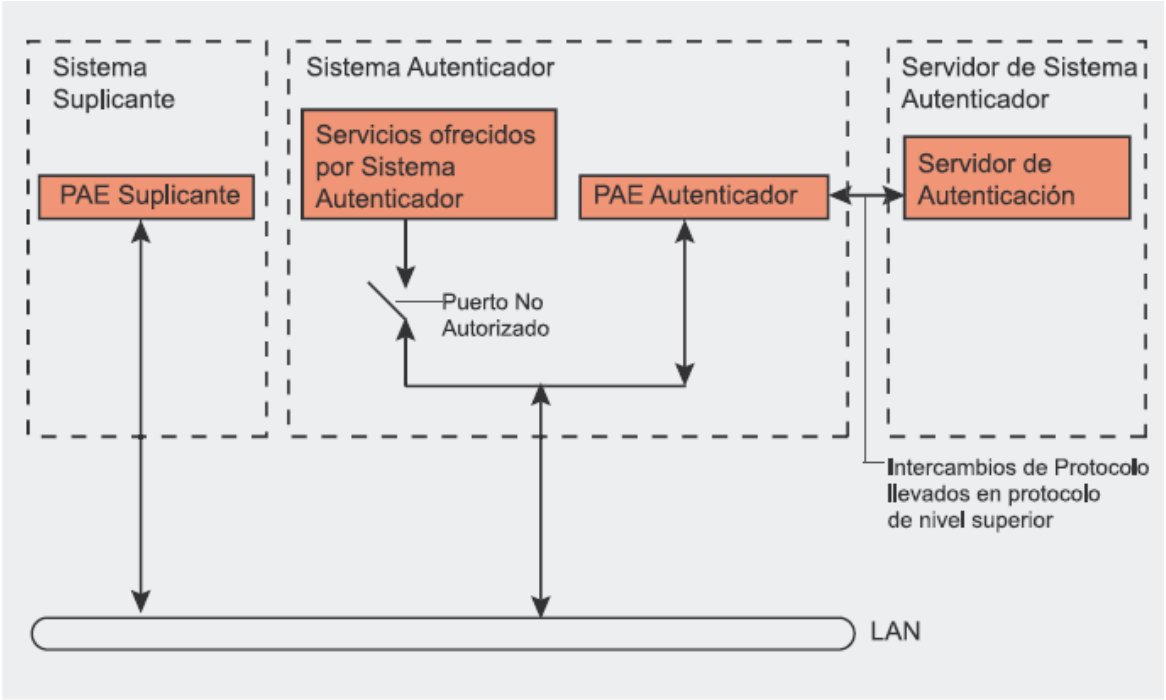
Como trabaja 802.11i

- 802.11i tiene 3 componentes
  - El suplicante que se une a la red
  - El autenticador que hace el control de acceso
  - El servidor de autenticación que toma las decisiones de autorización



Como trabaja 802.11i

- Opera por una combinación de protocolos:
  - 802.1X – A Port Based Network Access Control
  - EAP – Extensible Authentication Protocol
  - RADIUS – Remote Access Dial In User Service



Modelo de IEEE 802.1X según la especificación IEEE 802.1X

Variantes de 802.11i

		WPA	WPA2
Modo Corporativo	Autenticación	802.1X / EAP	802.1X / EAP
	Cifrado	TKIP/MIC	AES-CCMP
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

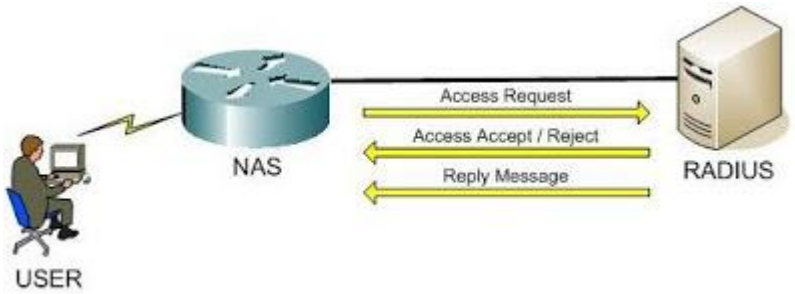
FreeRadius

Authentication **A**uthorization **A**ccounting

- La **A**utenticación es el proceso por el que una entidad prueba su identidad ante otra.
- **A**utorización se refiere a la concesión de acceso con privilegios específicos a una entidad o usuario basándose en su identidad.
- La (**A**) contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios.

Radius

- Protocolo basado en modelo cliente/servidor
- RFC 2865 (_AA) y RFC 2866 (A_)
- Listen ports UDP 1812 (_A) y UDP 1813 (A_)
- Funcionamiento:



FreeRadius

- AAA : Modelo de arquitectura de seguridad
- RADIUS: Implementación específica de AAA
- FreeRadius: Aplicación práctica de Radius

AAA → RADIUS → FreeRADIUS

Mikrotik: WPA 2 EAP - FreeRadius

- Instalar FreeRadius
- Instalar opcionalmente soporte a Base de Datos y web GUI (ej. mysql y phpmyadmin)
- Editar archivos de configuración de acuerdo a la solución a implementar: clients.conf, users, radiusd.conf, sql.conf, eap.conf, etc.

clients.conf

```
#}

client 192.168.14.10 {
        secret = pwd-mum-bol
        shortname = ap-test-mum-bol
}

#
```

radiusd.conf

```
        #
        $INCLUDE eap.conf

        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        #
        $INCLUDE sql.conf
```

sql.conf

```
        #       mysql, mssql, oracle, postgresql
        #
        database = "mysql"

        #
        #  Which FreeRADIUS driver to use.
        #
        driver = "rlm_sql_${database}"

        # Connection info:
        server = "localhost"
        #port = 3306
        login = "radius"
        password = "[redacted]"

        # Database table configuration for everything except Oracle
        radius_db = "radius"
```

FreeRadius - mysql

- Descomentar archivos necesarios para uso de consultas sql y no archivos planos
- Crear la base de datos en base a las plantillas para mysql (tablas)

```
root@srv-radius:/# mysql -u root -p
mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.00 sec)
mysql> exit;
root@srv-radius:/#
```

mysql

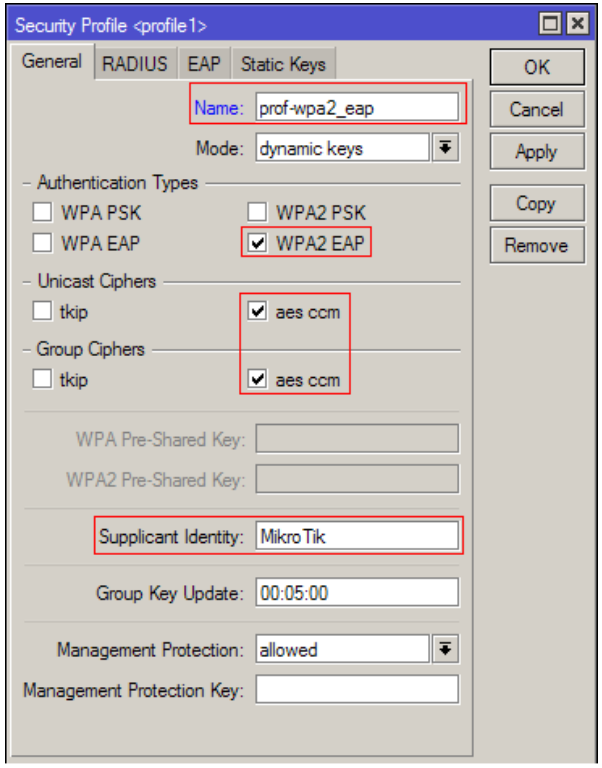
```
root@srv-radius:/# mysql -u root -p radius </etc/freeradius/sql/mysql/admin.sql
Enter password:
root@srv-radius:/# mysql -u root -p radius </etc/freeradius/sql/mysql/ippool.sql
Enter password:
root@srv-radius:/# mysql -u root -p radius </etc/freeradius/sql/mysql/schema.sql
Enter password:
root@srv-radius:/# mysql -u root -p radius </etc/freeradius/sql/mysql/nas.sql
Enter password:
```

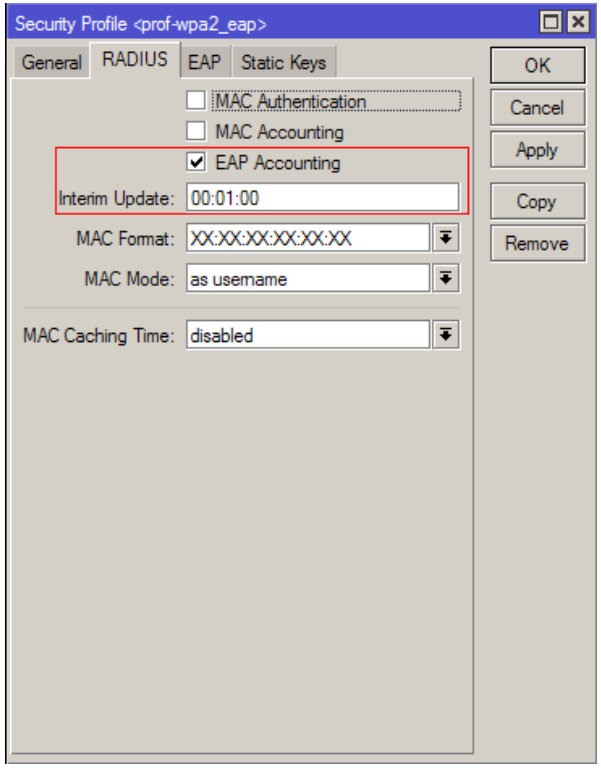
```
root@srv-radius:/# mysql -u radius -p
mysql> use radius
mysql> show tables;
+------------------+
| Tables_in_radius |
+------------------+
| nas              |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radippool        |
| radpostauth      |
| radreply         |
| radusergroup     |
+------------------+
9 rows in set (0.00 sec)
mysql>
```

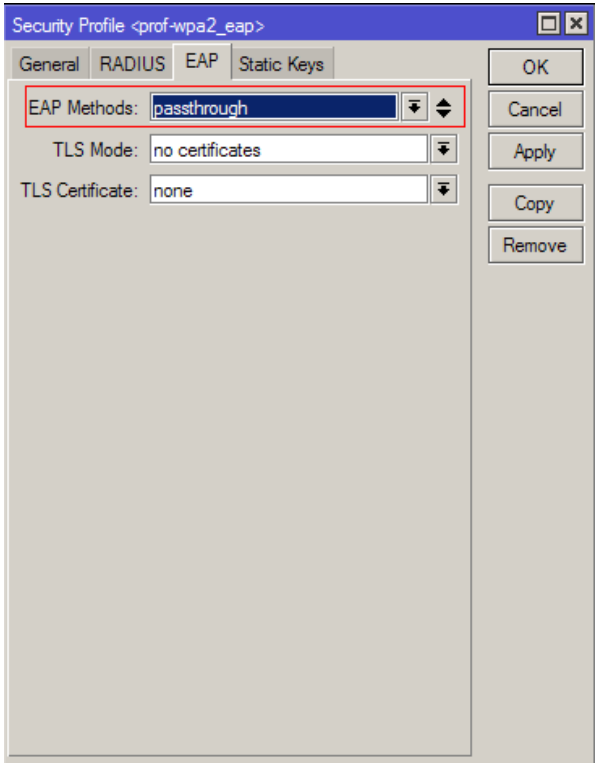
mysql

```
root@srv-radius:/# mysql -u radius -p
Enter password:

mysql> use radius
Database changed
mysql> INSERT INTO nas (nasname, shortname, type, ports, secret, description)
    -> VALUES
    -> ('192.168.14.8', 'MikoTik', 'other', 1812, 'pwd-mum-bol', 'RADIUS Client MT1');
Query OK, 1 row affected (0.08 sec)
mysql> INSERT INTO `radcheck` (username, attribute, op, value)
    -> VALUES
    -> ('bohorquezf', 'Cleartext-Password', ':=', '123456'),
    -> ('user1', 'Cleartext-Password', ':=', 'pwduser2'),
    -> ('user2', 'Cleartext-Password', ':=', 'pwduser2');
Query OK, 3 rows affected (0.19 sec)
Records: 3  Duplicates: 0  Warnings: 0

mysql> quit
```

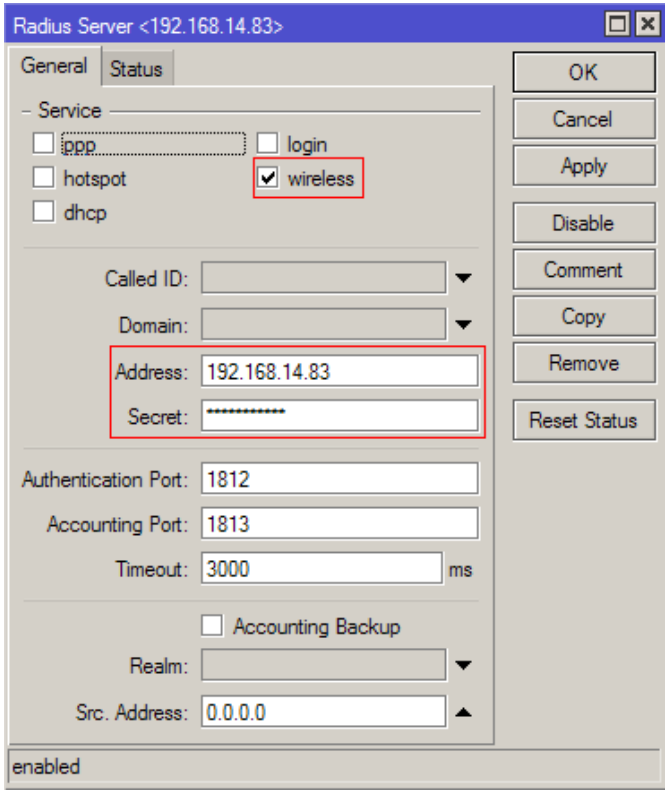
Configuración en Mikrotik

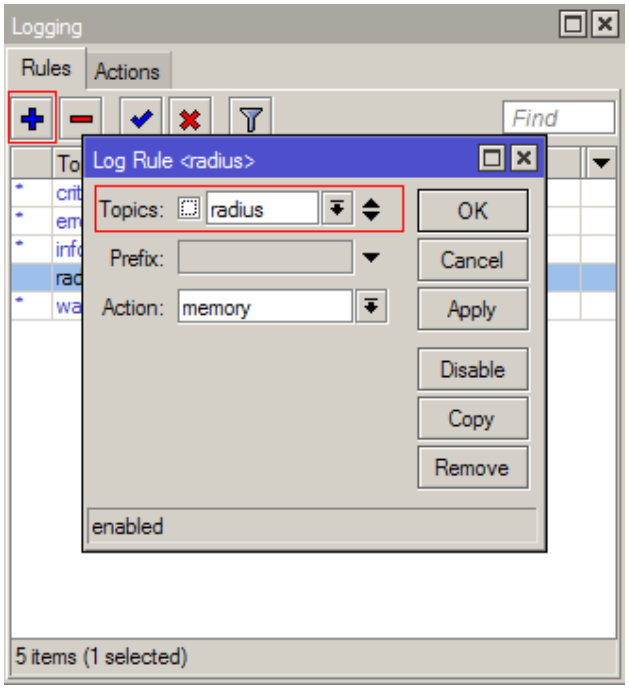


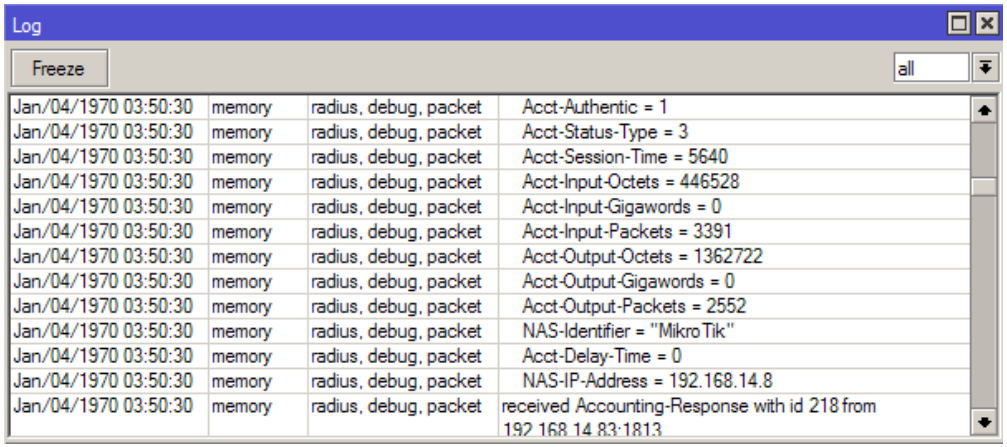




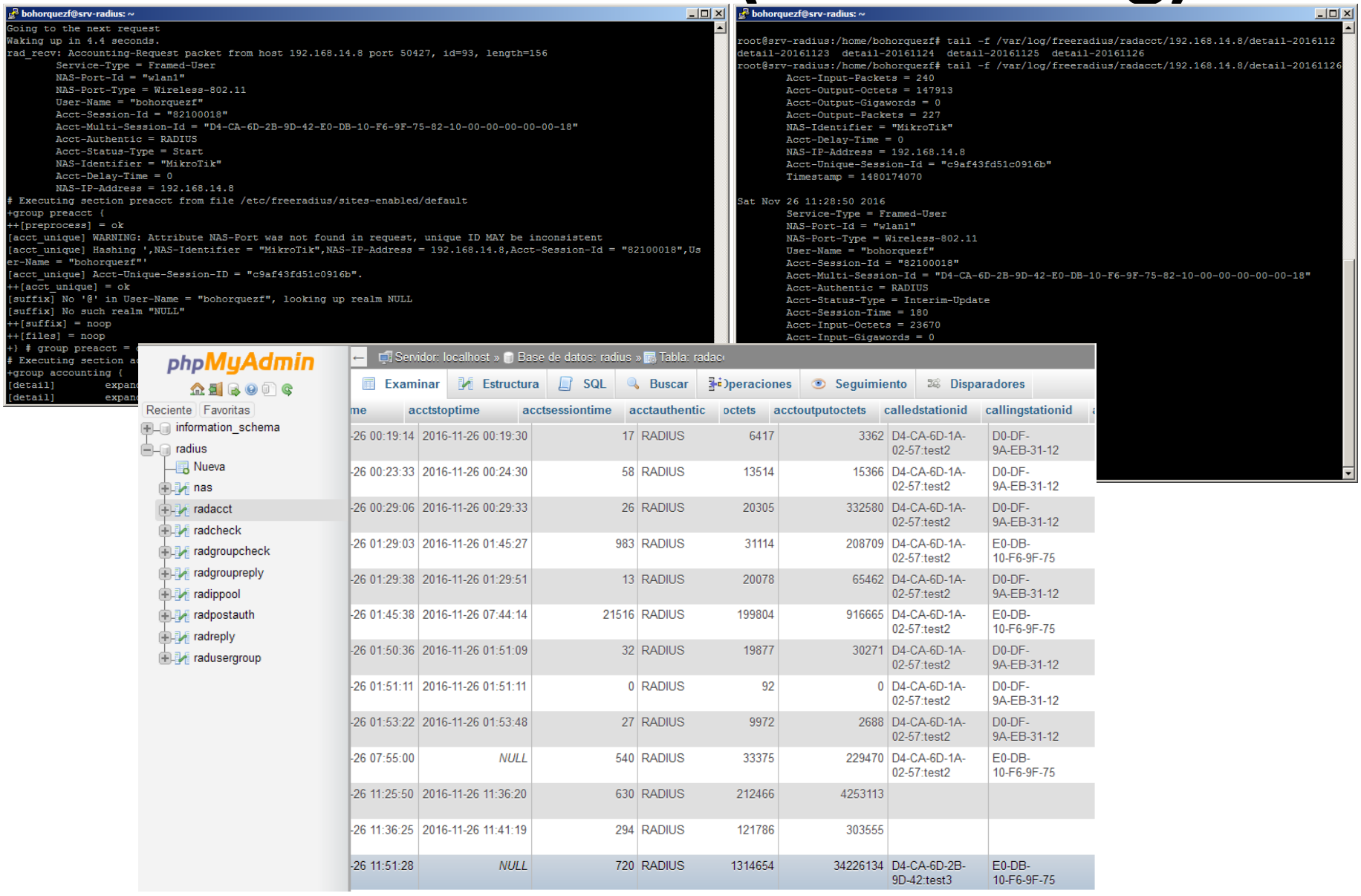
Config Mikrotik (cont…)







Contabilización (Accounting)



me	acctstoptime	acctsessiontime	acctauthentic	octets	acctoutputoctets	calledstationid	callingstationid
-26 00:19:14	2016-11-26 00:19:30	17	RADIUS	6417	3362	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 00:23:33	2016-11-26 00:24:30	58	RADIUS	13514	15366	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 00:29:06	2016-11-26 00:29:33	26	RADIUS	20305	332580	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 01:29:03	2016-11-26 01:45:27	983	RADIUS	31114	208709	D4-CA-6D-1A-02-57:test2	E0-DB-10-F6-9F-75
-26 01:29:38	2016-11-26 01:29:51	13	RADIUS	20078	65462	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 01:45:38	2016-11-26 07:44:14	21516	RADIUS	199804	916665	D4-CA-6D-1A-02-57:test2	E0-DB-10-F6-9F-75
-26 01:50:36	2016-11-26 01:51:09	32	RADIUS	19877	30271	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 01:51:11	2016-11-26 01:51:11	0	RADIUS	92	0	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 01:53:22	2016-11-26 01:53:48	27	RADIUS	9972	2688	D4-CA-6D-1A-02-57:test2	D0-DF-9A-EB-31-12
-26 07:55:00	*NULL*	540	RADIUS	33375	229470	D4-CA-6D-1A-02-57:test2	E0-DB-10-F6-9F-75
-26 11:25:50	2016-11-26 11:36:20	630	RADIUS	212466	4253113		
-26 11:36:25	2016-11-26 11:41:19	294	RADIUS	121786	303555		
-26 11:51:28	*NULL*	720	RADIUS	1314654	34226134	D4-CA-6D-2B-9D-42:test3	E0-DB-10-F6-9F-75

Windows Server

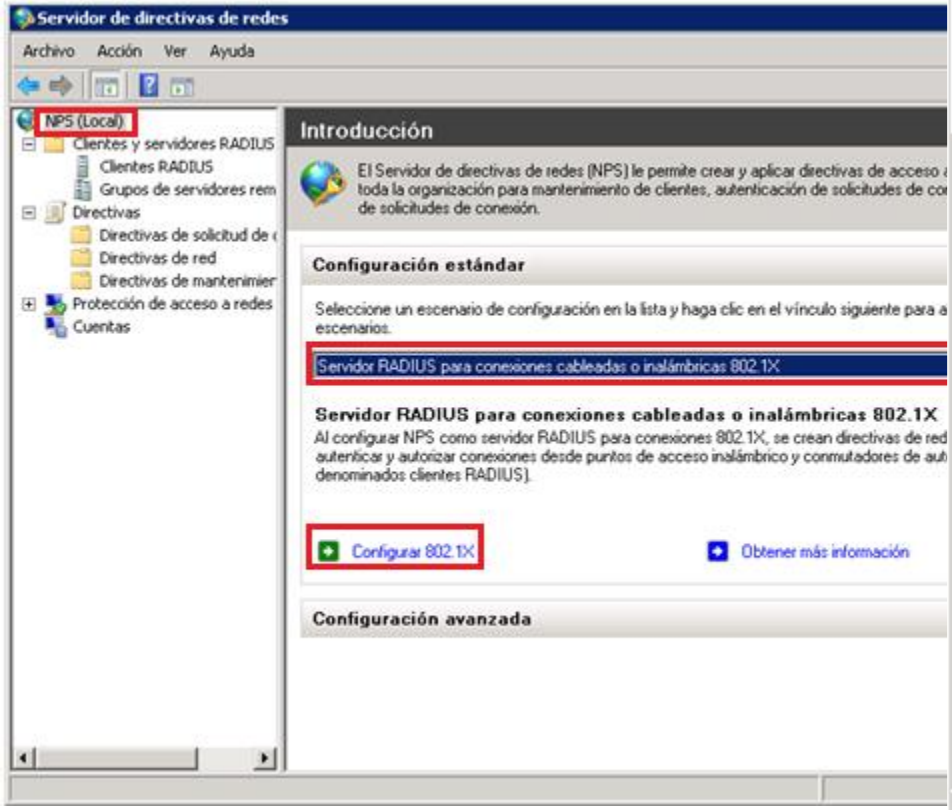
Active Directory (AD)

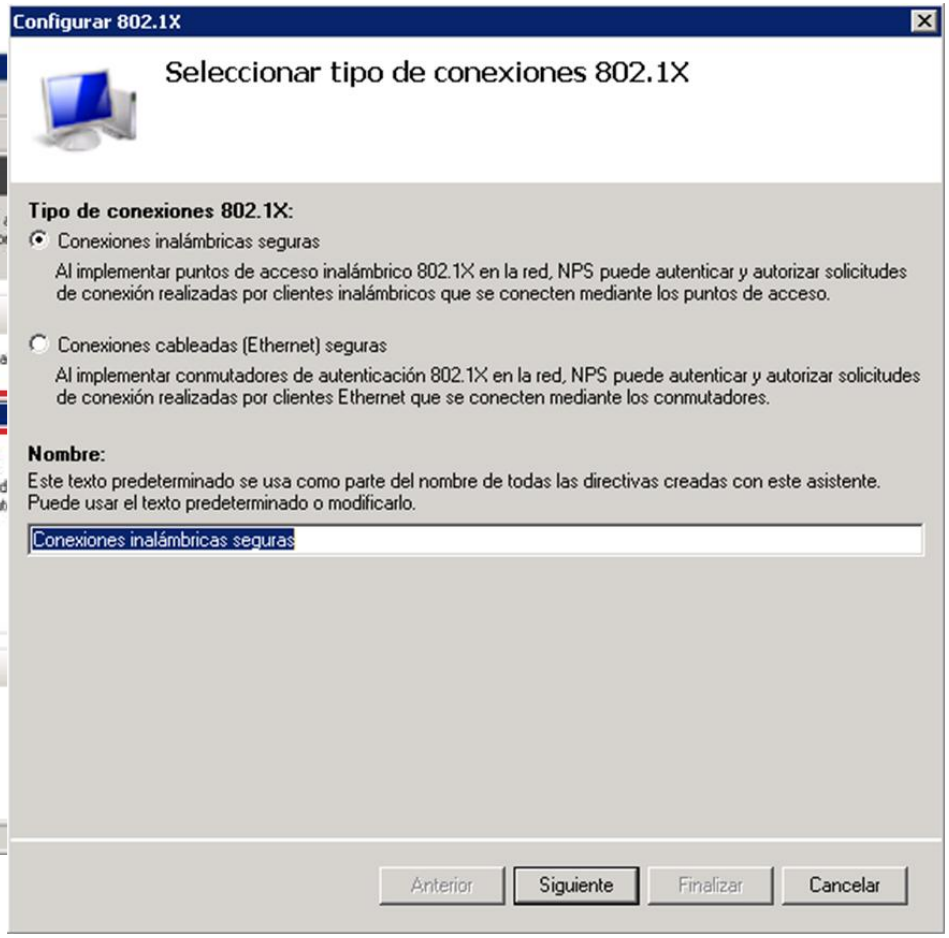
- Implementación Servicio de Directorio de Microsoft
- Protocolos: LDAP, DNS, DHCP, Kerberos, **Radius**.
- Administra inicios de sesión y políticas de acceso en una red Mikrosoft.
- Servicio de Acceso y Directivas de Redes: NPS (Network Policy Server)

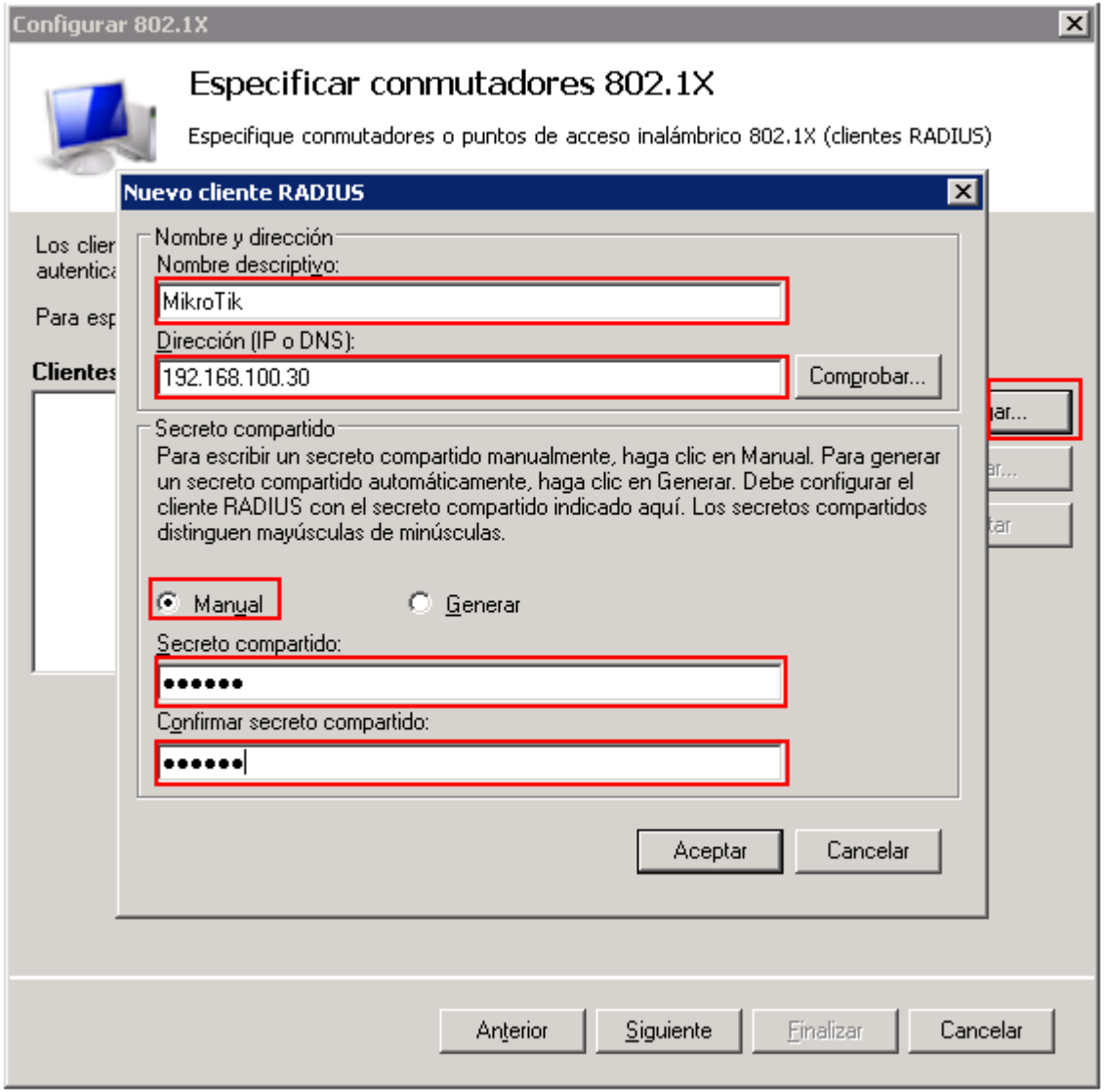
Implementación WPA EAP con AD

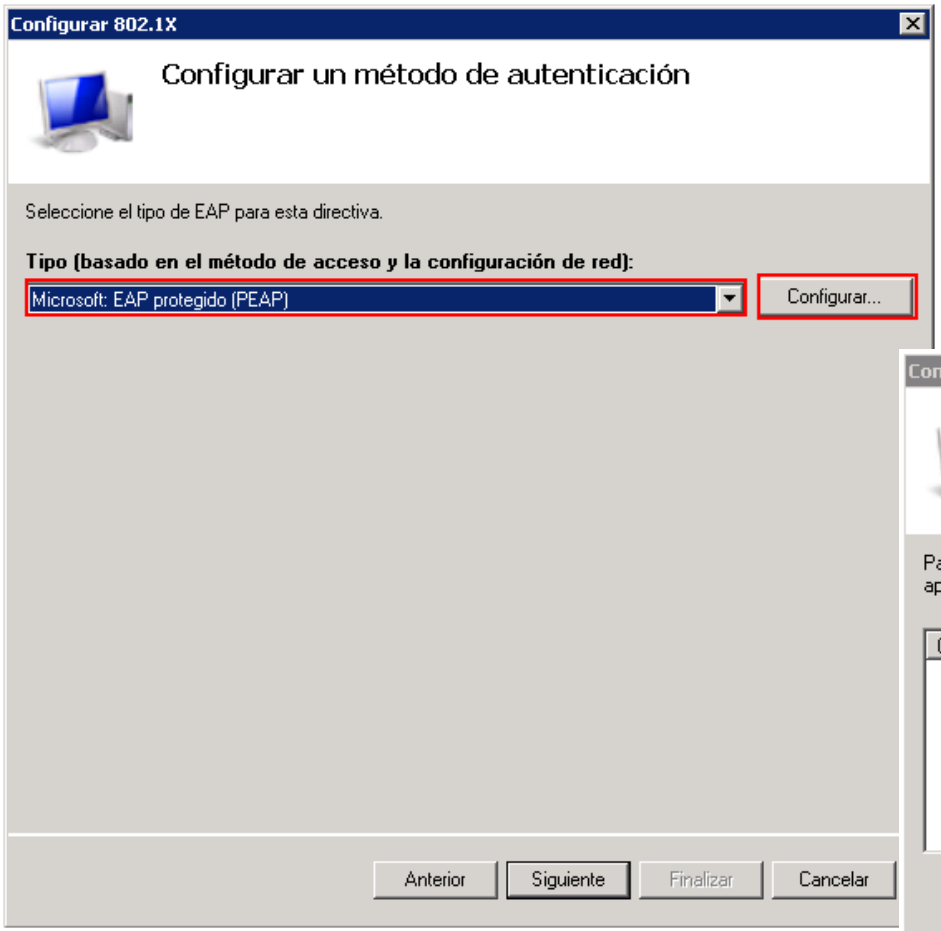
- Añadir AD y Domain Services + DNS y configurar OUs, Groups, Users, etc.
- Añadir rol de NPS (Network Policy and Access Services) y ADCS (Active Directory Certificate Services)
- Configurar Certificate Services y crear certificados
- Configurar NPS:
- + Clientes Radius
- Definir Tipo de Autenticación Cert, EAP, PEAP.
- Especificar grupos de acceso a red wireless
- Configurar Mikrotik AP
- Configurar los Clientes

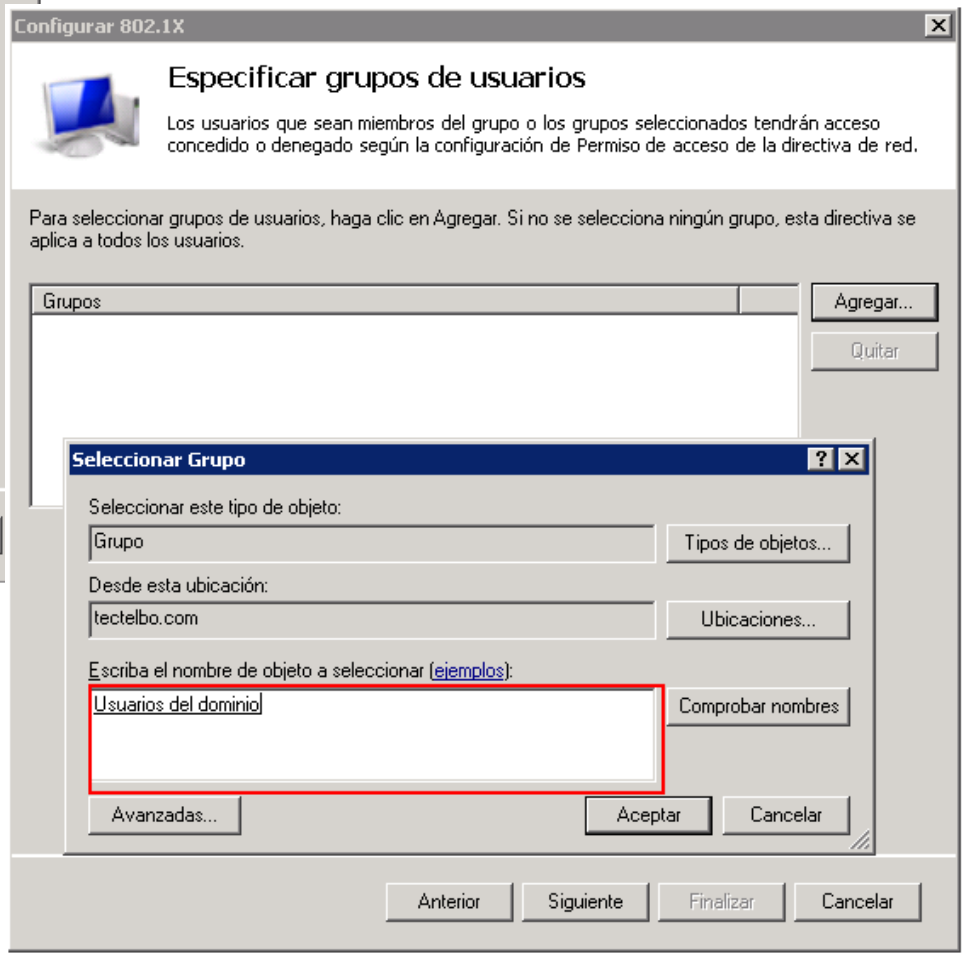
Configurar NPS



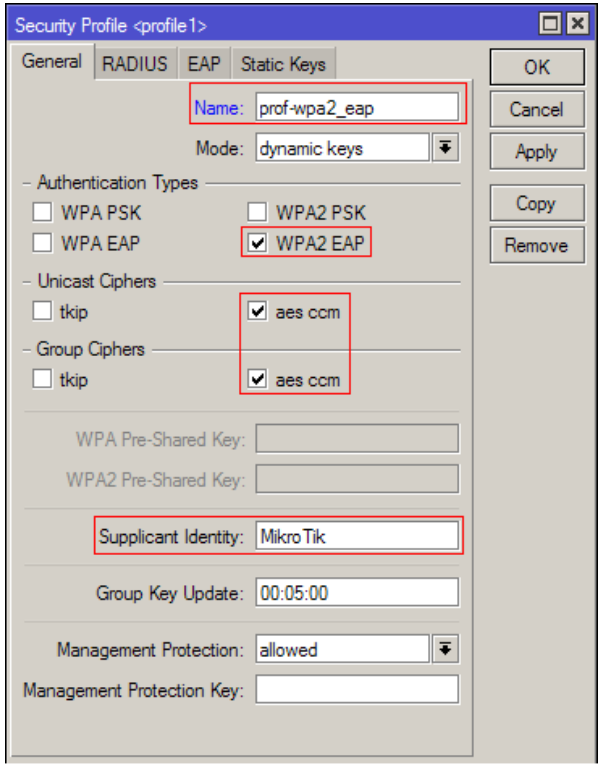


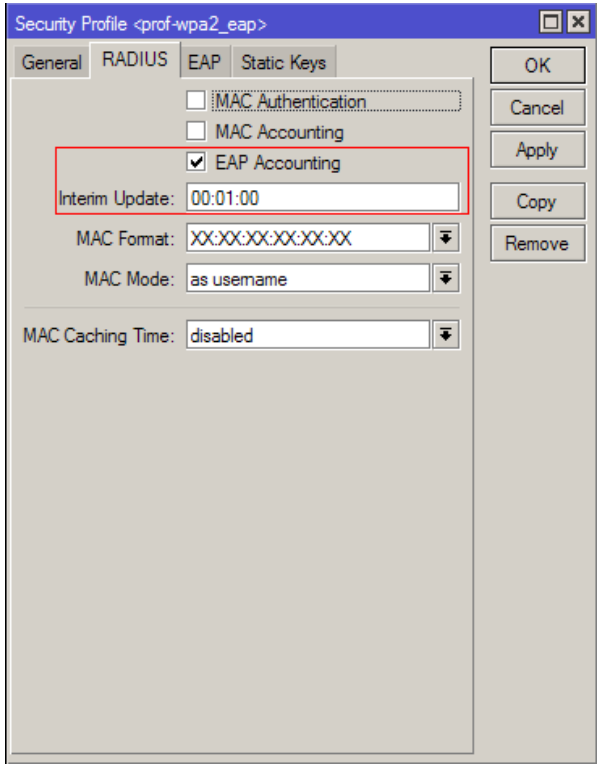

Configurar 802.1X
Especificar conmutadores 802.1X
Especifique conmutadores o puntos de acceso inalámbrico 802.1X (clientes RADIUS)
Nuevo cliente RADIUS
Nombre y dirección
Nombre descriptivo:
MikroTik
Dirección (IP o DNS):
192.168.100.30
Comprobar...
Secreto compartido
Para escribir un secreto compartido manualmente, haga clic en Manual. Para generar un secreto compartido automáticamente, haga clic en Generar. Debe configurar el cliente RADIUS con el secreto compartido indicado aquí. Los secretos compartidos distinguen mayúsculas de minúsculas.
Manual
Generar
Secreto compartido:
Confirmar secreto compartido:
Aceptar
Cancelar
Anterior
Siguiente
Finalizar
Cancelar

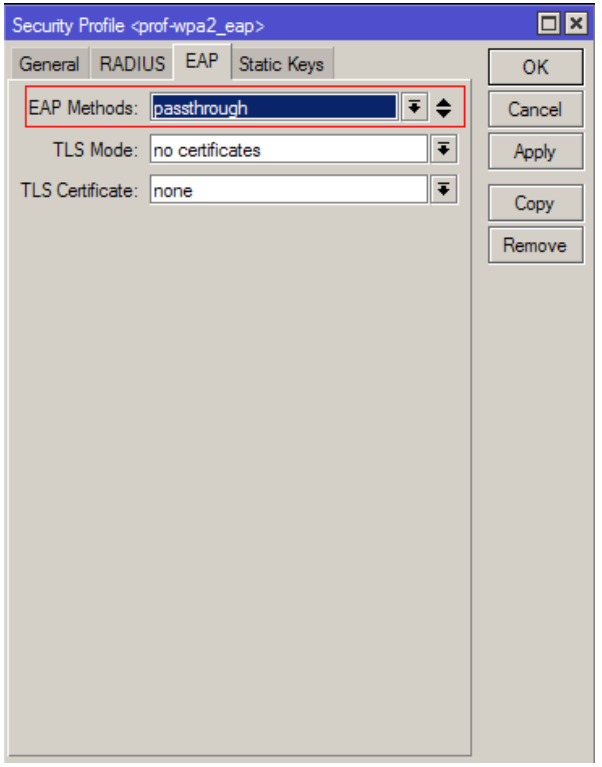

Configurar 802.1X
Configurar un método de autenticación
Seleccione el tipo de EAP para esta directiva.
Tipo (basado en el método de acceso y la configuración de red):
Microsoft: EAP protegido (PEAP)
Configurar...
Anterior
Siguiente
Finalizar
Cancelar


Configurar 802.1X
Especificar grupos de usuarios
Los usuarios que sean miembros del grupo o los grupos seleccionados tendrán acceso concedido o denegado según la configuración de Permiso de acceso de la directiva de red.
Para seleccionar grupos de usuarios, haga clic en Agregar. Si no se selecciona ningún grupo, esta directiva se aplica a todos los usuarios.
Grupos
Agregar...
Quitar
Seleccionar Grupo
Seleccionar este tipo de objeto:
Grupo
Tipos de objetos...
Desde esta ubicación:
tectelbo.com
Ubicaciones...
Escriba el nombre de objeto a seleccionar (ejemplos):
Usuarios del dominio
Comprobar nombres
Avanzadas...
Aceptar
Cancelar
Anterior
Siguiente
Finalizar
Cancelar

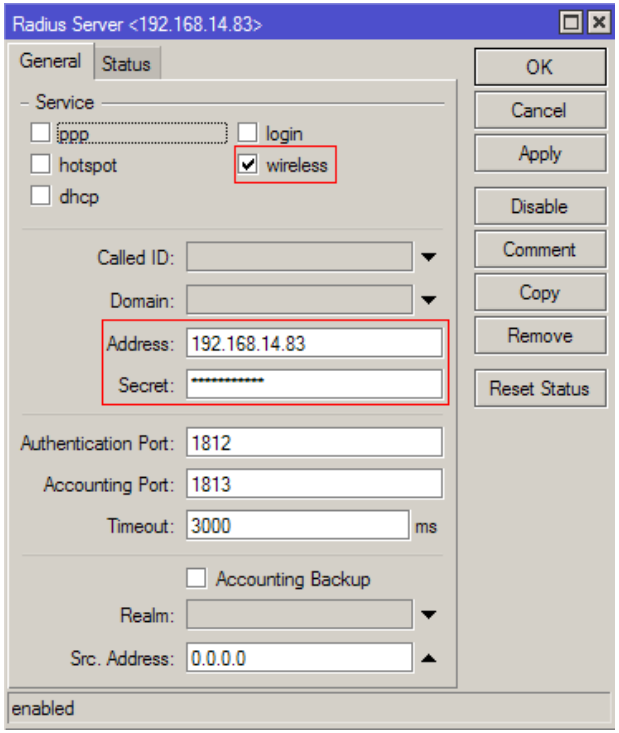
Configuración Mikrotik

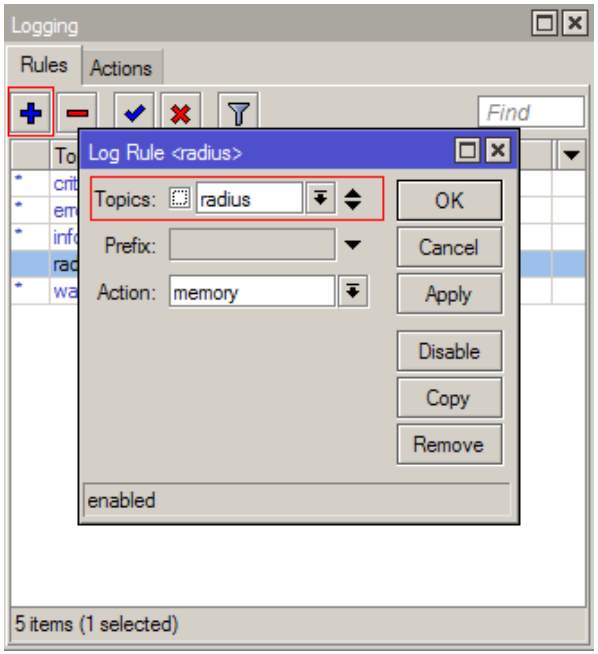


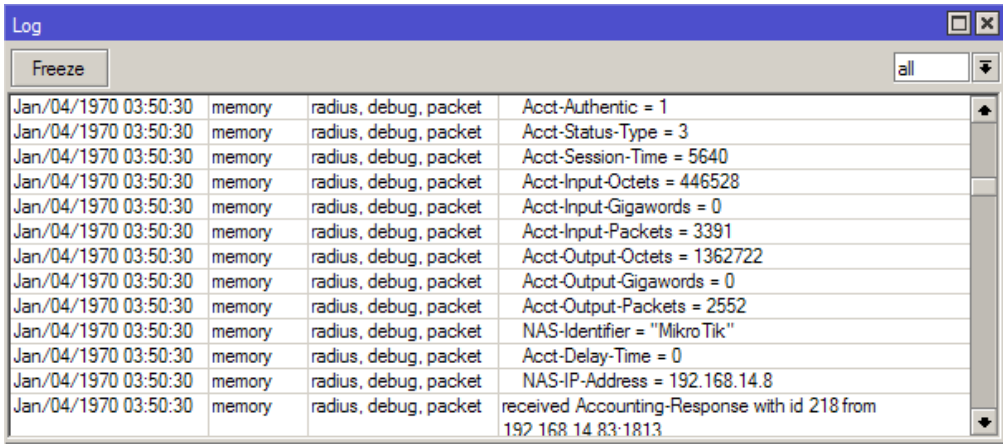




Config Mikrotik (cont...)







Gracias.

Referencias

- Seguridad de redes Inalámbricas, Eng. Wardner Maia, MUM Argentina Sep 7-8,2007
- Seguridad Wi-Fi WEP, WPA y WPA2, Guillaume Lehembre, hakin9 Nº 1/2006
- Wikipedia: https://en.wikipedia.org/wiki/IEEE_802.1X
- FreeRADIUS Beginner's Guide, Dirk van der Walt, Published by Packt Publishing Ltd., Livery Place, ISBN 978-1-849514-08-8