



mum
Mikrotik User Meeting

MUM BOLIVIA
LA PAZ, NOVEMBER 28, 2016

Wireless WPA2 EAP en Mikrotik

Casos de Uso con Windows
Server y FreeRadius

By Freddy Bohorquez Quevedo
TecTel

Tectel / Distratel

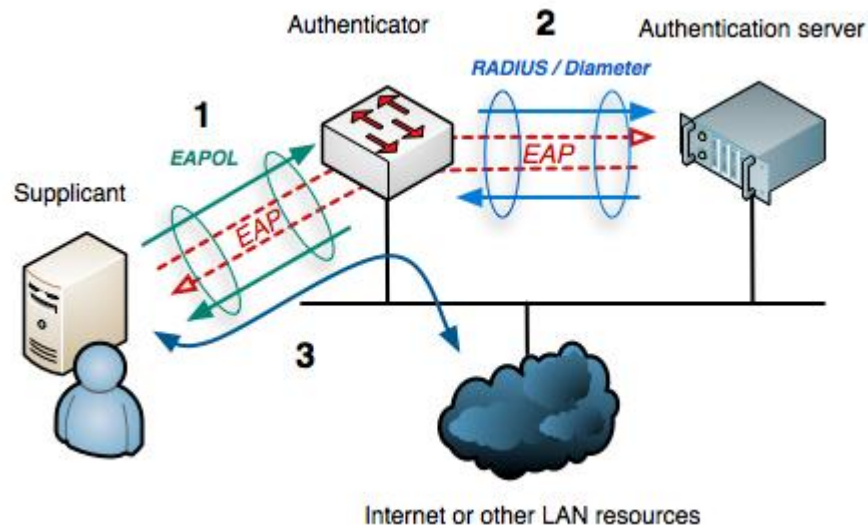
- 2004 Redes Inalámbricas Comunitarias
- 2005 Conectividad Rural
- Primeras Instalaciones basadas en WRAP/Mikrotik
- Despliegue de Redes PtP y PtMP: Públicas, Privadas, Comunitarias
- 2009 inicia Tectel como empresa especializada en Tecnología y Telecomunicaciones y Distribuidor de Mikrotik
- 2014 se 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 estándar fue aprobado y la Industria le dio el nombre de WPA2, compatible con 802.11i y con WPA.

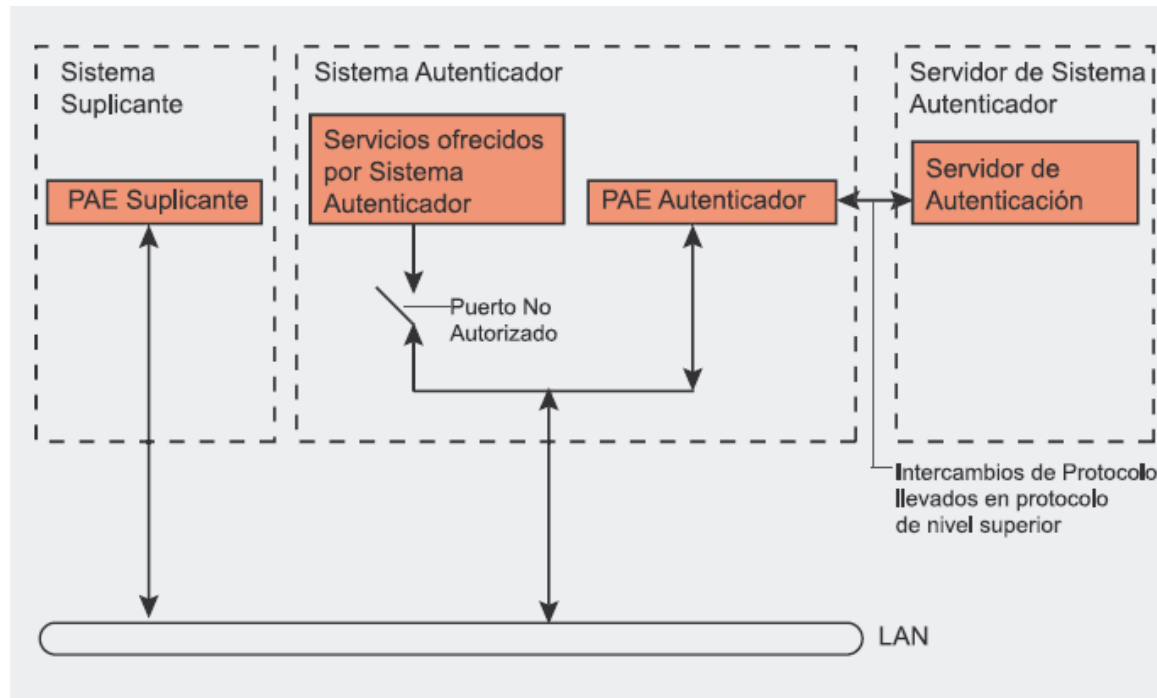
Como trabaja 802.11i

- 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



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

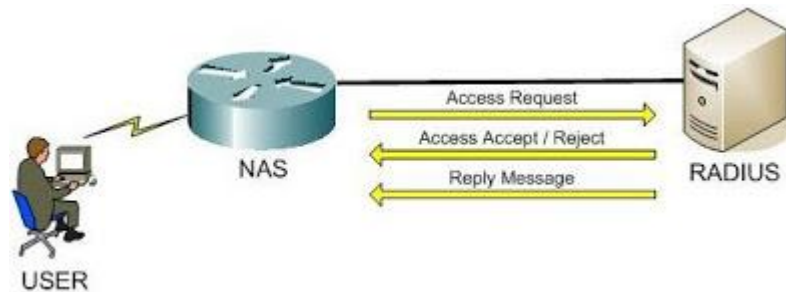
FreeRadius

Authentication Authorization Accounting

- 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

```
200 #}
201
202 client 192.168.14.10 {
203     secret = pwd-mum-bol
204     shortname = ap-test-mum-bol
205 }
206
207 #
```

radiusd.conf

```
737 #
738 $INCLUDE eap.conf
739
740 # Include another file that has the SQL-related configuration.
741 # This is another file only because it tends to be big.
742 #
743 $INCLUDE sql.conf
744
```

sql.conf

```
25 #
26 # mysql, mssql, oracle, postgresql
27 #
28 database = "mysql"
29
30 #
31 # Which FreeRADIUS driver to use.
32 #
33 driver = "rlm_sql_${database}"
34
35 # Connection info:
36 server = "localhost"
37 #port = 3306
38 login = "radius"
39 password = "radius"
40
41 # Database table configuration for everything except Oracle
42 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

Security Profile <profile 1>

General RADIUS EAP Static Keys

Name: prof-wpa2_eap

Mode: dynamic keys

Authentication Types

- WPA PSK
- WPA EAP
- WPA2 EAP

Unicast Ciphers

- tkip
- aes ccm

Group Ciphers

- tkip
- aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity: MikroTik

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK Cancel Apply Copy Remove

Security Profile <prof-wpa2_eap>

General RADIUS EAP Static Keys

- MAC Authentication
- MAC Accounting
- EAP Accounting

Interim Update: 00:01:00

MAC Format: XX:XX:XX:XX:XX:XX

MAC Mode: as username

MAC Caching Time: disabled

OK Cancel Apply Copy Remove

Security Profile <prof-wpa2_eap>

General RADIUS EAP Static Keys

EAP Methods: passthrough

TLS Mode: no certificates

TLS Certificate: none

OK Cancel Apply Copy Remove

Config Mikrotik (cont...)

Radius Server <192.168.14.83>

General Status

Service

- ppp
- login
- hotspot
- dhcp
- wireless

Called ID:

Domain:

Address:

Secret:

Authentication Port:

Accounting Port:

Timeout: ms

Accounting Backup

Realm:

Src. Address:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Status

Logging

Rules Actions

Log Rule <radius>

Topics:

Prefix:

Action:

OK Cancel Apply Disable Copy Remove

enabled

5 items (1 selected)

Log

Freeze

all

Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Authentic = 1
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Status-Type = 3
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Session-Time = 5640
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Octets = 446528
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Gigawords = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Packets = 3391
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Octets = 1362722
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Gigawords = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Packets = 2552
Jan/04/1970 03:50:30	memory	radius, debug, packet	NAS-Identifier = "MikroTik"
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Delay-Time = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	NAS-IP-Address = 192.168.14.8
Jan/04/1970 03:50:30	memory	radius, debug, packet	received Accounting-Response with id 218 from 192.168.14.83:1813

Contabilización (Accounting)

```
bohorquezf@srv-radius: ~
Going to the next request.
Waking up in 4.4 seconds.
rad_recv: Accounting-Request packet from host 192.168.14.8 port 50427, id=93, length=156
  Service-Type = Framed-User
  NAS-Port-Id = "wlan1"
  NAS-Port-Type = Wireless-802.11
  User-Name = "bohorquezf"
  Acct-Session-Id = "82100018"
  Acct-Multi-Session-Id = "D4-CA-6D-2B-9D-42-E0-DB-10-F6-9F-75-82-10-00-00-00-00-18"
  Acct-Authentic = RADIUS
  Acct-Status-Type = Start
  NAS-Identifier = "MikroTik"
  Acct-Delay-Time = 0
  NAS-IP-Address = 192.168.14.8

# Executing section preacct from file /etc/freeradius/sites-enabled/default
+group preacct {
++[preprocess] = ok
[acct_unique] WARNING: Attribute NAS-Port was not found in request, unique ID MAY be inconsistent
[acct_unique] Hashing ',NAS-Identifier = "MikroTik",NAS-IP-Address = 192.168.14.8,Acct-Session-Id = "82100018",User-Name = "bohorquezf"'
[acct_unique] Acct-Unique-Session-ID = "c9af43fd51c0916b".
++[acct_unique] = ok
[suffix] No '@' in User-Name = "bohorquezf", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] = noop
++[files] = noop
+) # group preacct =
# Executing section accounting from file /etc/freeradius/sites-enabled/default
+group accounting {
[detail] expanded
[detail] expanded
```

```
bohorquezf@srv-radius: ~
root@srv-radius:/home/bohorquezf# tail -f /var/log/freeradius/radacct/192.168.14.8/detail-2016112
detail-20161123 detail-20161124 detail-20161125 detail-20161126
root@srv-radius:/home/bohorquezf# tail -f /var/log/freeradius/radacct/192.168.14.8/detail-20161126
  Acct-Input-Packets = 240
  Acct-Output-Octets = 147913
  Acct-Output-Gigawords = 0
  Acct-Output-Packets = 227
  NAS-Identifier = "MikroTik"
  Acct-Delay-Time = 0
  NAS-IP-Address = 192.168.14.8
  Acct-Unique-Session-Id = "c9af43fd51c0916b"
  Timestamp = 1480174070

Sat Nov 26 11:28:50 2016
  Service-Type = Framed-User
  NAS-Port-Id = "wlan1"
  NAS-Port-Type = Wireless-802.11
  User-Name = "bohorquezf"
  Acct-Session-Id = "82100018"
  Acct-Multi-Session-Id = "D4-CA-6D-2B-9D-42-E0-DB-10-F6-9F-75-82-10-00-00-00-00-18"
  Acct-Authentic = RADIUS
  Acct-Status-Type = Interim-Update
  Acct-Session-Time = 180
  Acct-Input-Octets = 23670
  Acct-Input-Gigawords = 0
```

phpMyAdmin

Enviar: localhost » Base de datos: radius » Tabla: radacct

Examinar Estructura SQL Buscar Operaciones Seguimiento Disparadores

me	acctstoptime	acctsessiontime	acctauthentic	octets	acctoutpctoctets	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 Microsoft.
- 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

Introducción

El Servidor de directivas de redes (NPS) le permite crear y aplicar directivas de acceso a toda la organización para mantenimiento de clientes, autenticación de solicitudes de conexión de solicitudes de conexión.

Configuración estándar

Seleccione un escenario de configuración en la lista y haga clic en el vínculo siguiente para a escenarios.

[Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X](#)

Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X
Al configurar NPS como servidor RADIUS para conexiones 802.1X, se crean directivas de red autenticar y autorizar conexiones desde puntos de acceso inalámbrico y conmutadores de aut denominados clientes RADIUS.

[Configurar 802.1X](#) [Obtener más información](#)

Configuración avanzada

Configurar 802.1X

Seleccionar tipo de conexiones 802.1X

Tipo de conexiones 802.1X:

Conexiones inalámbricas seguras
Al implementar puntos de acceso inalámbrico 802.1X en la red, NPS puede autenticar y autorizar solicitudes de conexión realizadas por clientes inalámbricos que se conecten mediante los puntos de acceso.

Conexiones cableadas (Ethernet) seguras
Al implementar conmutadores de autenticación 802.1X en la red, NPS puede autenticar y autorizar solicitudes de conexión realizadas por clientes Ethernet que se conecten mediante los conmutadores.

Nombre:
Este texto predeterminado se usa como parte del nombre de todas las directivas creadas con este asistente. Puede usar el texto predeterminado o modificarlo.

[Anterior](#) [Siguiente](#) [Finalizar](#) [Cancelar](#)

Configurar 802.1X

Especificar conmutadores 802.1X

Especifique conmutadores o puntos de acceso inalámbrico 802.1X (clientes RADIUS)

Los clientes de autenticación...

Para especificar...

Cientes

Nuevo cliente RADIUS

Nombre y dirección

Nombre descriptivo:
MikroTik

Dirección (IP o DNS):
192.168.100.30 Comprobar...

Secretos compartidos

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.

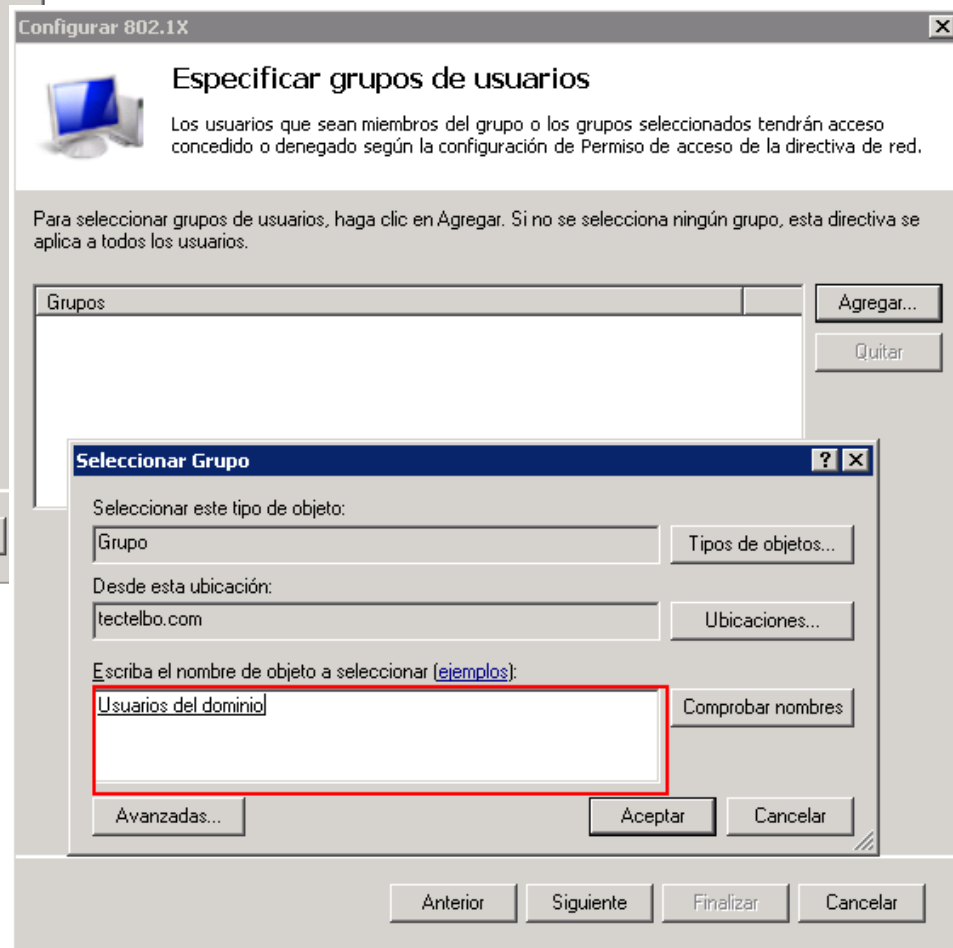
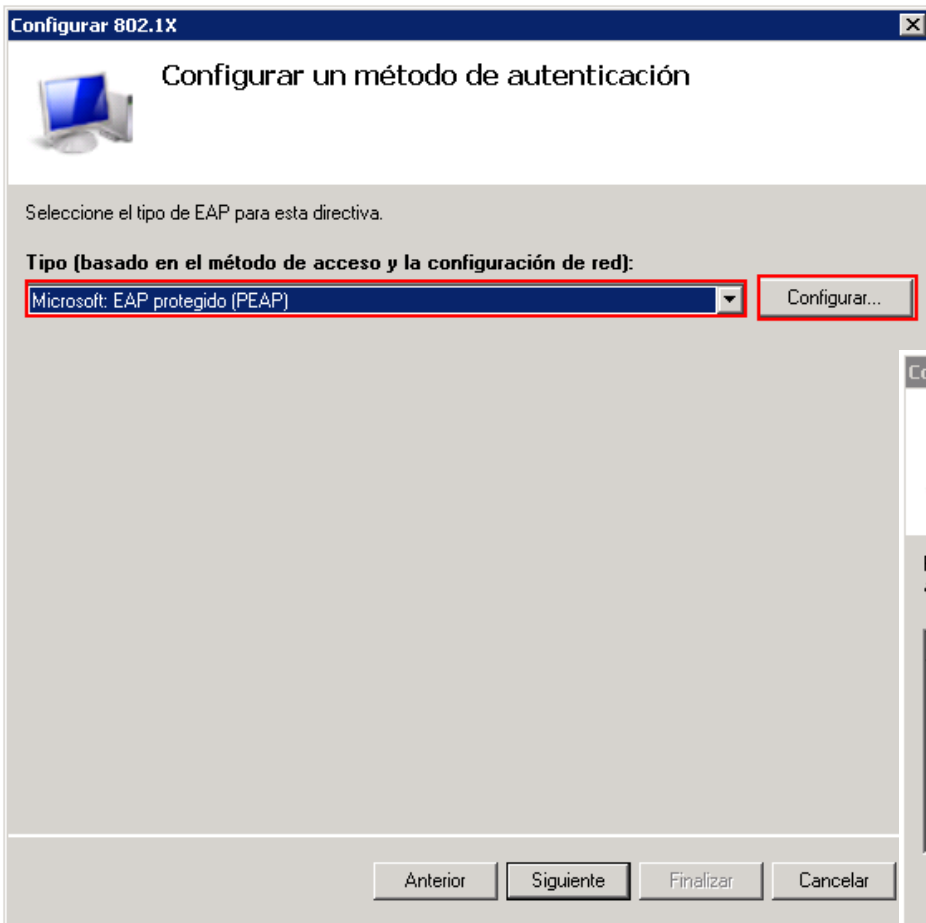
Manual Generar

Secretos compartidos:
.....

Confirmar secreto compartido:
.....

Aceptar Cancelar

Anterior Siguiente Finalizar Cancelar



Configuración Mikrotik

Security Profile <profile 1>

General RADIUS EAP Static Keys

Name: prof-wpa2_eap

Mode: dynamic keys

Authentication Types

- WPA PSK
- WPA EAP
- WPA2 EAP

Unicast Ciphers

- tkip
- aes ccm

Group Ciphers

- tkip
- aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity: MikroTik

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK Cancel Apply Copy Remove

Security Profile <prof-wpa2_eap>

General RADIUS EAP Static Keys

- MAC Authentication
- MAC Accounting
- EAP Accounting

Interim Update: 00:01:00

MAC Format: XX:XX:XX:XX:XX:XX

MAC Mode: as username

MAC Caching Time: disabled

OK Cancel Apply Copy Remove

Security Profile <prof-wpa2_eap>

General RADIUS EAP Static Keys

EAP Methods: passthrough

TLS Mode: no certificates

TLS Certificate: none

OK Cancel Apply Copy Remove

Config Mikrotik (cont...)

Radius Server <192.168.14.83>

General Status

Service

- ppp
- hotspot
- dhcp
- login
- wireless

Called ID:

Domain:

Address:

Secret:

Authentication Port:

Accounting Port:

Timeout: ms

Accounting Backup

Realm:

Src. Address:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Status

Logging

Rules Actions

Log Rule <radius>

Topics:

Prefix:

Action:

enabled

5 items (1 selected)

OK Cancel Apply Disable Copy Remove

Log

Freeze

all

Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Authentic = 1
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Status-Type = 3
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Session-Time = 5640
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Octets = 446528
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Gigawords = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Input-Packets = 3391
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Octets = 1362722
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Gigawords = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Output-Packets = 2552
Jan/04/1970 03:50:30	memory	radius, debug, packet	NAS-Identifier = "MikroTik"
Jan/04/1970 03:50:30	memory	radius, debug, packet	Acct-Delay-Time = 0
Jan/04/1970 03:50:30	memory	radius, debug, packet	NAS-IP-Address = 192.168.14.8
Jan/04/1970 03:50:30	memory	radius, debug, packet	received Accounting-Response with id 218 from 192.168.14.83:1813

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 N° 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