Education Roaming
Movilidad segura para la comunidad académica

Módulo 5 Cliente RADIUS (09 horas)

1. Configuración de un cliente RADIUS (NAS) (1h)

Para la configuración de los clientes NAS, se usará un a*ccess point*. Debemos saber que el NAS soporte IEEE 802.1X.

Ahora, en el servidor RADIUS de su RNIE, configure los parámetros necesarios para su conexión con el NAS.

```
client <ip_nas>{
secret = <secreto>
shortname = AP-<nombre_institución>
nastype = cisco
}
```

Para el Access Point, tomaremos como ejemplo el modelo Cisco Aironet 1240AG y la configuración se encuentra en la figura config-ap.jpg de la carpeta imágenes-eduroam.

2. Configurar protocolos de autenticación EAP (1h)

Configurar el archivo eap.conf

```
eap {
        default_eap_type = ttls
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = 4096
  tls {
            private_key_file = ${certdir}/radius.key
            certificate_file = ${certdir}/radius.<dom_institución>.crt
            CA_file = ${cadir}/ca.crt
            dh_file = ${certdir}/dh
            random_file = ${certdir}/random
            CA_path = ${cadir}
           cipher_list = "DEFAULT"
        }
  ttls {
             default_eap_type = md5
            copy_request_to_tunnel = no
```

Comentario [r1]: Protocolo de autenticación por default utilizada por el servidor radius

Comentario [r2]: Clave privada del servidor radius NREN

Comentario [r3]: Clave pública del servidor radius NREN.

Comentario [r4]: Clave pública de la autoridad certificadora PKI.

```
        use_tunneled_reply = no
        virtual_server = "inner-tunnel"
    }
    peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = no
        use_tunneled_reply = no

        virtual_server = "inner-tunnel"
        }
    mschapv2 {
        }
    }
```

3. Configuración de clientes para *eduroam* (2h)

En este punto, solo vamos a probar la autenticación de usuarios usando el protocolo EAP-TTLS-PAP.

Las siguiente figura muestra una captura de pantalla de la configuración de un suplicante hacia una red inalámbrica con SSID “EDUROAM”.

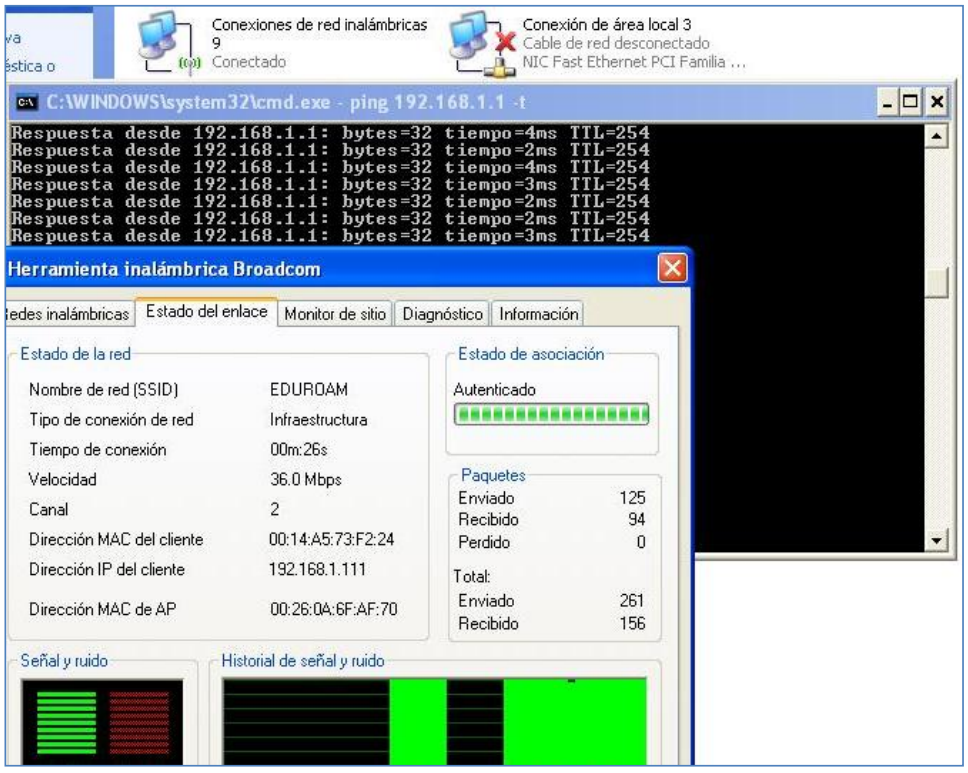

Figura 6: Pruebas de autenticación remota desde un suplicante en Windows XP.

Evaluación 6: Validación de usuarios usando como protocolo EAP-TTLS (1h) (10%)

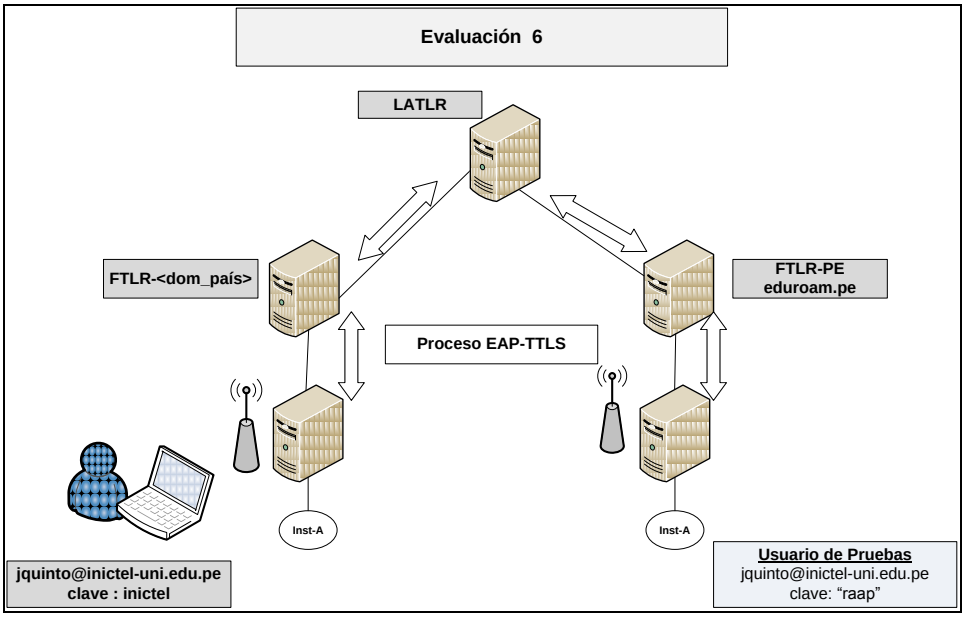

Figura 7: Autenticación remota usando un suplicante radius al servidor radius remoto usando EAP-TTLS

4. Monitoreo de los servidores RADIUS federados por un servidor RSYSLOG central (1h)

   Éste paso es muy importante para llevar un registro de las autenticaciones realizadas por los servidores RADIUS. Estos servidores deberían enviar sus actualizaciones de *Logs* a un servidor de *Log* central.

   Para la configuración de un *rsyslog* cliente, debemos escribir las siguientes líneas en el archivo /etc/rsyslog.conf

```
…
$DefaultNetstreamDriverCAFile /home/eduroam/CLAVES/ca.pem
$DefaultNetstreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode anon

…

local1.=notice          /usr/local/var/log/radius/radius-notice.log
local1.=notice          @@<ip_rsyslog_latlr>:10514
local1.=err             /usr/local/var/log/radius/radius-err.log
local1.=err             @@ip_rsyslog_latlr:10514
local1.=info            /usr/local/var/log/radius/radius-fticks.log
local1.=info            @@ip_rsyslog_latlr:10514
…
```

Comentario [r5]: Clave pública del servidor rsyslog central latlr.

Comentario [r6]: Envio de los logs a un servidor de Logs centralizado LATLR

Puede solicitar la clave pública ca.pem del *rsyslog* o descargarla desde la siguiente url:
wget --user=user_eduroam --password="eduroam" ftp://200.37.45.99/eduroam/ca.pem