Trabalho Nº 3 - Redes WiFi e RADIUS

1. Introdução

A instalação de redes WiFi em ambiente institucional deve obedecer a padrões de segurança elevados, nomeadamente na forma como são trocadas e obtidas as credenciais de acesso à rede.

Uma das formas de garantir esse tipo de funcionalidade consiste em utilizar a família de protocolos de autenticação 802.1X, em conjunto com um servidor RADIUS (*Remote Authentication Dial In User Service*) que realiza as funcionalidades de autenticação, autorização e *accounting* (AAA).

No decorrer deste trabalho iremos realizar a configuração de um ambiente deste tipo, constituído por um servidor RADIUS (FreeRADIUS) e um Access Point WiFi de forma a criar um *Basic Service Set* obedecendo ao protocolo de autenticação PEAP – MSCHAPv2.

O trabalho irá ser realizado em duas partes: primeiro será efectuada a instalação e configuração do servidor RADIUS, e depois a configuração do Access Point e do *supplicant* nos clientes móveis.

A realização do mesmo segue de muito perto o *tutorial* "802.1X Port-Based Authentication HOWTO", disponível em http://www.tldp.org/HOWTO/8021X-HOWTO/index.html. Aconselha-se a leitura da Introdução antes de iniciar o trabalho.

2. Trabalho a efectuar

2.1 Instalação e Configuração do FreeRADIUS

No decorrer deste trabalho, cada aluno instalar e configurar um servidor FreeRADIUS na sua estação de trabalho.

Nota: É possível que nalgumas máquinas o servidor FreeRADIUS já tenha sido instalado por outro colega. Para saber, verifique se existe a directoria `/etc/raddb`.

No caso de não estar instalado, proceda do seguinte modo:

1. Abrir o utilitário Yast a partir do menu *System*, que irá requerer a *password* root. Se não a souber peça-a ao professor.

2. Seleccionar a opção "*Software*" e "*Install and Remove Software*".

3. Na caixa *Search*, digitar FreeRADIUS e lancar a procura. Irão aparecer vários packages com esse nome ou relacionados.

4. Seleccionar só o *package* freeradius no ecrã da direita e premir "*Accept*" no canto inferior direito da janela do Yast, e depois do *package* estar instalado seleccione "*Finish*".

5. Verificar se o FreeRADIUS está correctamente instalado listando a directoria `/etc/raddb`.

De seguida, iremos modificar os ficheiros de configuração do FreeRadius de modo a activar o tipo de autenticação pretendida.

Os ficheiros a editar encontram-se todos na directoria `/etc/raddb` e são os seguintes:

```
radiusd.conf
eap.conf
clients.conf
users
```

Antes de começar a editar estes ficheiros, leia com atenção o que se segue:

Se o FreeRADIUS já estiver instalado na sua máquina, é possível que esses ficheiros já tenham sido parcialmente modificados por um colega (podendo estar num estado incoerente - verifique as datas de modificação) e que os originais tenham sido guardados com um nome do tipo `radiusd.conf.save`.

Aconselha-se nesse caso a copiar os ficheiros modificados para uma directoria de backup (`/etc/raddb/config.other`) de forma a que o trabalho dos seus colegas não se perca, e a voltar a partir dos ficheiros originais. Em caso de dúvida, poderá desinstalar e voltar a instalar o servidor (peça conselho ao professor).

Depois de resolvido este problema, poderá então editar os ficheiros de configuração de acordo com o ponto 3.2 do Tutorial Configuring FreeRADIUS.

Para editar os ficheiros, deverá executar o editor de texto em modo root, utilizando por exemplo o comando:

```
su -c kate
```

2.1.1 radiusd.conf

Modifique o ficheiro `radiusd.conf` de acordo com o ponto 2 do *tutorial* identificando neste ficheiro os módulos `mschap, autohrize, authenticate` e descomentando as linhas indicadas.

Não esqueça que conteúdo dos módulos `module{…}` está contido dentro de chavetas curvas, devendo verificar se a chaveta final se encontra correctamente descomentada.

2.1.2 clients.conf

No ponto 3 relativo ao ficheiro `clients.conf`, deverá especificar os parâmetros para a rede do Access Point do Laboratório:

```
client 192.168.50.0/24 {
        secret          = testing123
        shortname       = Netlab
}
```

2.1.3 eap.conf

No ponto 4.b, configuração da secção TLS no ficheiro `eap.conf`, deverá utilizar os **certificados que gerou no trabalho anterior** procedendo da seguinte forma:

1. Copie os ficheiros `crt.pem` e `key.pem` contendo o seu certificado e respectiva chave privada para a directoria `/etc/raddb/certs`

2. O atributo `private_key_password` deverá ser preenchido com a password que utilizou na geração do certificado.

3. O atributo `private_key_file` deverá designar o seu ficheiro `key.pem`.

4. O atributo `certificate_file` deverá designar o seu ficheiro `crt.pem`.

5. Copie o ficheiro http://netlab.ulusofona.pt/cr/praticas/cacert.pem contendo o certificado da Certification Authority criada no Laboratório para a directoria `/etc/raddb/certs/demoCA`.

2.1.4 users

Seguidamente deverá editar o ficheiro `users` introduzindo dois utilizadores para os testes utilizando os seguintes padrões:

```
# Utilizador local para testar o funcionamento básico
# do servidor com envio de uma mensagem de saudação

"joao"     Auth-Type := Local, User-Password == "teste"
           Reply-Message = "Hello, %u"

# Utilizador da rede WiFi par testar a autenticação
# PEAP-MSCHAPV2

"jose"     User-Password == "teste"
```

2.2 Teste local do FreeRADIUS

Uma vez modificados os ficheiros de acordo com as indicações do pondo anterior, vamos testar o funcionamento básico do FreeRADIUS. Proceda do seguinte modo:

1. Abra uma consola e passe para modo supervisor utilizando o comando `su -l`

2. Digite o comando `/usr/sbin/radiusd -X` para lançar o serividor em modo *debug*

3. Verifique que o output gerado não apresenta erros e que acaba com a mensagem:

   ```
   Listening on authentication *:1812
   Listening on accounting *:1813
   Ready to process requests.
   ```

4. Caso haja erros de execução, deverá identificar o módulo em que ocorreram e corrigir os ficheiros de configuração até conseguir um arranque correcto do servidor.

5. Teste a autenticação local com o comando `radtest` executado numa outra janela:

   ```
   radtest joao teste localhost 1812 testing123
   ```

   Se tudo estiver a funcionar correctamente, deverá obter uma mensagem do tipo:

   ```
   rad_recv: Access-Accept packet from host 127.0.0.1:1812
   Reply-Message = "Hello, joao"
   ```

Pode também testar o user jose, mas não irá receber mensagem de resposta.

```
radtest jose teste localhost 1812 testing123

rad_recv: Access-Accept packet from host 127.0.0.1:1812
```

6. Verifique se o servidor FreeRADIUS recebeu os pedidos de autenticação e interprete os resultados.

7. Para verificar que o seu servidor está acessível na rede, experimente o mesmo comando a partir da máquina de um dos seus colegas. Poderá ter de adicionar um novo cliente no ficheiro `client.conf`.

Se obteve resultados correctos, poderá passar à segunda fase do trabalho.

2.3 Configuração do Access Point WiFi e Análise do Tráfego

Uma vez configurado o servidor RADIUS irá agora verificar se este responde correctamente aos pedidos de autenticação do Access Point WiFi instalado no Laboratório. Para tal, deverá lançar o servidor em modo *debug* como indicado no ponto anterior, e configurar a AP para utilizar o endereço desse servidor para realizar a autenticação 802.1X. **Lance também o Ethereal nessa máquina**.

Para realizar a configuração da AP, deverá ser utilizado um portátil ligado à tomada da rede nº 4 do Laboratório, que se encontra perto do armário que está ao lado do quadro e do ecrã de projecção (o cabo tem a indicação “AP” no conector).

Uma vez ligado a esse cabo, irá receber um IP da gama 192.168.60.0/24. Para configurar a AP deverá abrir um browser e aceder ao endereço 192.168.60.254. Será pedida uma password que deverá ser pedida ao professor. Para configurar o endereço do seu servidor RADIUS, deverá aceder ao menu Advanced Configuration > Wireless > 802.1X apresentado na Figura 1.

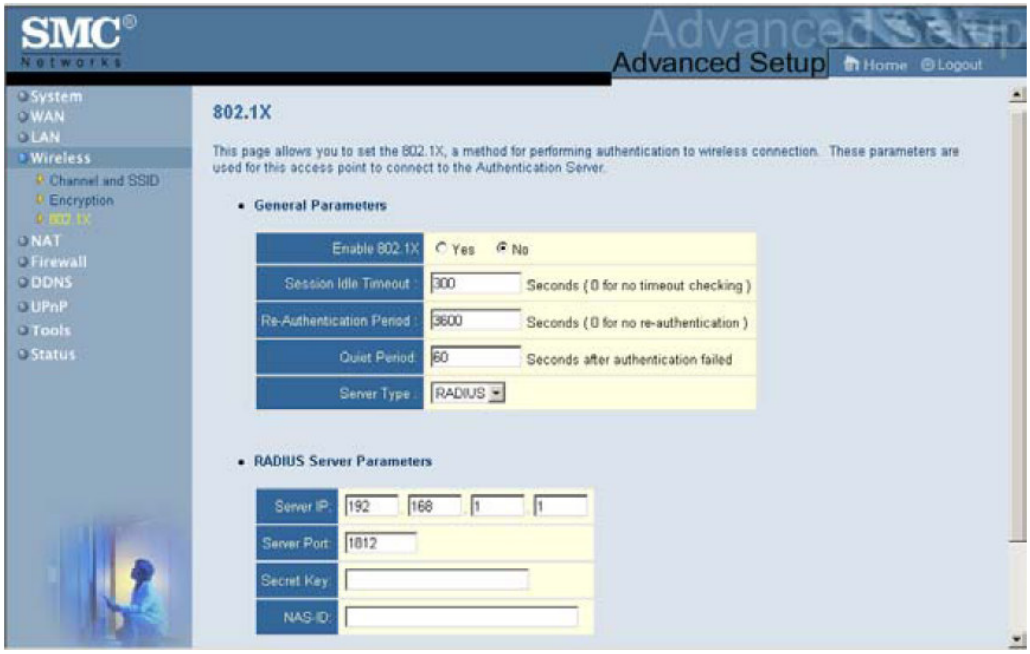

Figura 1

O campo Secret Key deverá corresponder ao que foi declarado no ficheiro `clients.conf` no ponto 2.1.2.

Deverá configurar também o Ethereal (Edit > Preferences > Protocols > RADIUS) com o mesmo Shared Secret que vai utilizar entre a AP e o servidor, para que ele possa desencriptar os pacotes que captura.

Deverá também verificar que o endereço (ou a classe de endereços) do cliente declarado nesse ficheiro é idêntico (ou contém) o endereço externo da AP (WAN IP). Para ver esse endereço deverá aceder ao menu Status que tem o aspecto apresentado na *Figura 2*.

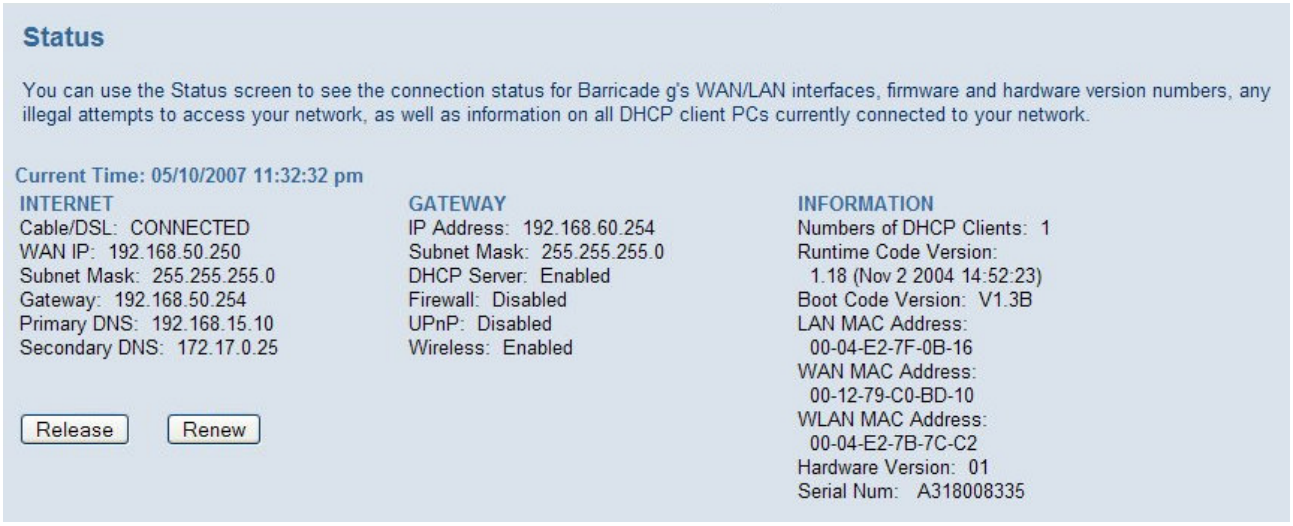

Figura 2

Uma vez introduzido o endereço do servidor a que a AP irá pedir a autenticação, deverá utilizar um portátil com interface Wireless para se conectar ao SSID Netlab que é divulgado pela AP.

Deverá configurar o *supplicant* utilizado com parâmetros semelhantes aos que utiliza para aceder à rede wireless universitária e-U, ou seja, no caso do Windows o que é apresentado na Figura 3:

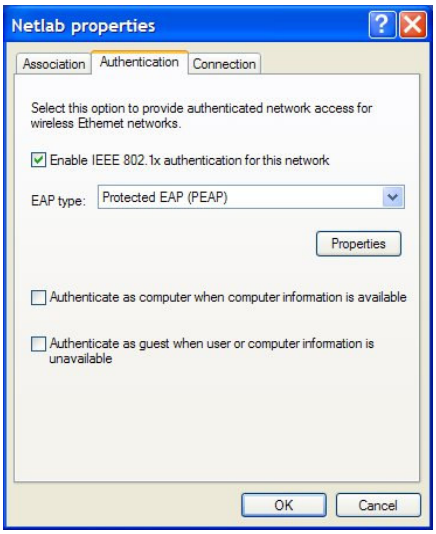

Figura 3

- *Association* → Open WEP / The Key is provided automatically
- *Autentication* → EAP de tipo PEAP (Protected EAP)
- *Properties* → *Authentication Method*: *Secured password* (EAP-MSCHAP v2). Só deverá seleccionar a opção *Validate server certificate* se no seu portátil tiver importado o certificado da CA que assinou o certificado utilizado pelo RADIUS server.
- Não esquecer de seleccionar o botão *Configure* e **retirar** a opção de enviar as suas credenciais de Logon no sistema Windows do portátil.

Uma vez esta configuração realizada, active a captura de pacotes no Ethereal que está lançado no servidor RADIUS, e invoque no *supplicant* a conecção ao SSID Netlab.

O *supplicant* irá pedir um *user name* e uma *password* para validar o pedido de ligação devendo fornecer as credenciais introduzidas no ficheiro `users` no ponto 3, deixando o campo Domain em branco.

Na janela da máquina onde lançou o servidor RADIUS em modo *debug* deverão aparecer mensagens de pedidos de autenticação da parte da AP e o Ethereal deverá capturar pacotes UDP com mensagens RADIUS.

Em caso de êxito, as mensagens deverão terminar com uma sequência do tipo:

```
Sending Access-Accept of id 11 to 192.168.50.250 port 32920
  MS-MPPE-Recv-Key =
0x65965a618354f03f0e8edec6120a99749b151a5ed0ec2d6d2c5c99032dceee80
  MS-MPPE-Send-Key =
0xd25bebabbce9b95c3b707b60739b5b0e140026cf7ae0b64a28483999dc1dff37
  EAP-Message = 0x030b0004
  Message-Authenticator = 0x00000000000000000000000000000000
  User-Name = "jose"
```

O portátil deverá estar ligado à rede Wireless Netlab, obtendo um endereço IP fornecido pela AP na gama 192.168.60.0/24.

Interprete os pacotes que capturou com o Ethereal.

3. Prazo de Entrega do Trabalho

O prazo para a entrega dos trabalhos é de três semanas a contar da aula em que o enunciado foi apresentado. Não serão aceites trabalhos fora do prazo. A entrega deverá ser feita por e-mail num ficheiro zip (ou rar) contendo um relatório (**obrigatório**) em PDF e as listagens dos programas realizados, obedecendo OBRIGATORIAMENTE ao seguinte formato:

`a123456-trabalho-N.zip`

4. Referências

"FreeRADIUS Home Page":

www.freeradius.org

"802.1X Port-Based Authentication HOWTO":

http://www.tldp.org/HOWTO/8021X-HOWTO/index.html