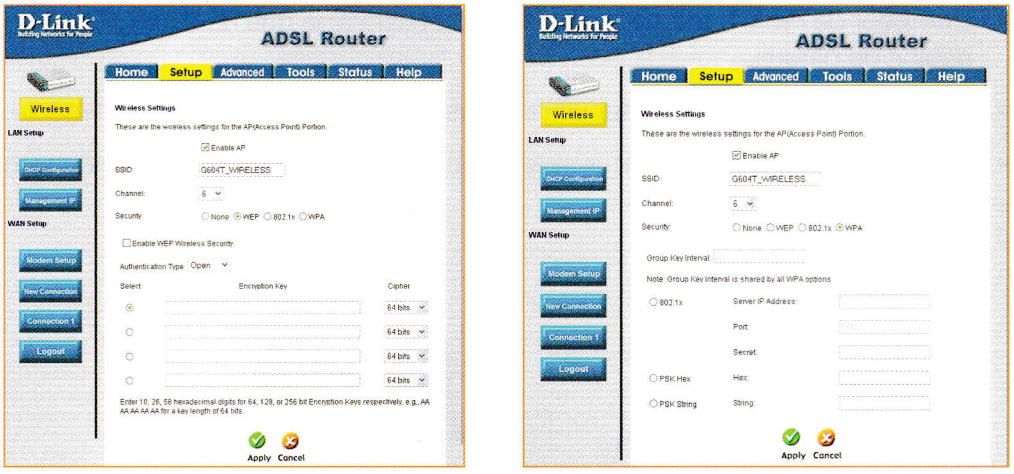
Les claus poden ser quatre, i d'aquesta manera podem donar una clau diferent per a cada equip. L'encriptació es pot fer per a 64, 128 o 256 bits; la trama de 64 bits es compon de 10 nombres hexadecimals (0 a F), i la de 128 bits, de 26 nombres.

Així doncs, podem dir que, seguint una taula ASCII, una codificació de 64 bits correspon a una paraula de 5 lletres, i una de 128 bits, a una paraula de 13 lletres.



Finestres de configuració de WEP i WPA.

L'encriptació **WPA (*Wi-Fi protected access* 'accés protegit a Wi-Fi')** es va crear per millorar la seguretat WEP, i per proporcionar l'autenticació de l'usuari, inexistent en WEP.

Habitualment, hi ha tres paràmetres per configurar: **PSK Hex (*preshared key* 'clau precompartida')**, basada en un màxim de 32 nombres hexadecimals; **PSK String**, clau en forma d'un màxim de 63 caràcters, o el servidor **RADIUS**, que va donant claus en funció de l'usuari que s'hi connecta.

Per a la majoria de xarxes petites, com una petita empresa o un particular, l'encriptació WAP és la manera més senzilla de tenir una seguretat efectiva. De les tres opcions, la PSK String és la més fàcil d'implantar.

Problemes

8. Calcula aquesta clau web en hexadecimal en cadena de caràcters ASCII, sabent que 61 = a i que 7A = z:

   a) 74 65 63 6e 6f

   b) 64 65 70 61 72 74 61 6d 65 6e 74 73 2e

   c) 61 75 6c 61 20 69 6e 66 6f 72 6d 61 74

- RADIUS (*remote authentication dial in user service*) és un protocol AAA ('autenticació, autorització i administració') per a aplicacions com l'accés a xarxes o mobilitat IP.
- El servidor més important és el FreeRADIUS (*www.freeradius.org*), llicència d'Open Source.

Taller d'informàtica 2

Seguretat d'una xarxa sense cable

Ara observaràs un altre dels paràmetres amb els quals es pot garantir la seguretat en una xarxa sense cable.

1. Busca al punt d'accés si hi ha un **filtre per a MAC**. Què pot significar?
2. Executa en un ordinador que tingui targeta Wi-Fi la instrucció *ipconfig/all* i llegeix l'adreça física. Aquesta adreça MAC (*media access control*) es podria posar en aquest camp, i aleshores obligaràs el punt d'accés a comunicar-se només amb ella.

   Si accidentalment posem una adreça MAC errònia, creus que podrem tornar a connectar amb el punt d'accés?