05

Wireless segurança

Transcrição

A comunicação wireless trabalha de forma similar ao HUB, passando as informações para todos os dispositivos que estiverem ao alcance. Para evitar que dispositivos que não possuam permissão acessem essas informações, é preciso fazer configurações de segurança.

O primeiro método de segurança utilizava um protocolo chamado ***Wired Equivalent Privacy*** (**WEP**), que usava um algoritmo de criptografia chamado de **RC4** - considerado pouco eficaz e, por isso, comprometia a segurança. Ele trabalhava com **chaves compartilhadas**, que basicamente configuravam uma senha e caso um dispositivo desejasse acessar a rede era necessário que possuísse tal senha. O problema das chaves compartilhadas é que se quisermos remover o acesso de um determinado usuário, será necessário a troca da senha para que ele não consiga mais acessar a rede. Algo bem trabalhoso para empresas com muitos funcionários.

Com o intuito de corrigir os problemas do WEP, foi desenvolvido o protocolo ***Wi-Fi Protected Access*** (**WPA**), que usa um algoritmo de criptografia chamado **Tkip** e é considerado bem mais eficiente que o RC4. Mas continua trabalhando com chaves compartilhadas, o que acaba gerando desafios em empresas com grande rotatividade de funcionários.

O WPA sofreu um evolução, apesar de manter o seu protocolo de segurança do WPA, agora passou a trabalhar com a autenticação **802.1x** (não confundir com o padrão IEEE 802.11). Em vez de chaves compartilhadas, a autenticação **802.1x** vai solicitar um usuário e senha. Após entrar com as informações de acesso, o roteador fará a consulta em um servidor com um banco de dados onde estão armazenados todos os usuários e senhas que possuem permissão de acessos. Se o usuário e senha existirem, o servidor vai enviar uma resposta confirmando por roteador e ocorrerá uma abertura de sessão com o usuário. Para remover o acesso de um ex-funcionário, basta que os dados de usuário e a senha sejam apagados do servidor.

O WPA sofreu uma segunda evolução, passando a ser conhecido como **WPA2** ou pelo nome da especificação **802.11i**. Ele manteve a autenticação 802.1x, porém, adotou o algoritmo de criptografia e segurança para o **AES**. A versão WPA2 garante uma segurança considerada mais eficiente que as anteriores.