Summary

One of the things that always need to be considered in deploying wireless networks is security. Security needs to be the primary concern. It also needs to be the primary focus.

In deploying wireless LAN and security, you must at a minimum, use WPA2 with a pre-shared key and AES encryption. Anything less than that sets up an opportunity for vulnerability.

Guest wireless access when deployed in an enterprise environment should also adhere to that same minimum security of WPA2 with a pre-shared key and AES encryption. In the event that the organization does not find that feasible, use a WebAuth Splash page with disclaimers and a login prompt that you could have users put in their email address and a common password. You could have a document that you update or change weekly or monthly with a specific login IDs and passwords for guests that could be deployed through the reception desk.

In Enterprise wireless LAN deployments, you should always separate your guest access from any corporate access. That separation should always be done with unique wireless VLANs and completely separate SSIDs. Doing that you can actually have different security methods that we have discussed throughout the series for both the guests as well as the corporate.

Lastly, your wireless LANs are always being scanned. Someone is always turning on a packet capturing device, and watching and monitoring your wireless frames. Be aware of that and monitor your RF environment yourself, and you might actually find an intruder.