You have conducted a wireless survey and identified that your office’s wireless access point’s signal can be received from the parking lot. You want to prevent this from occurring, which of the following actions should you perform?

Change the encryption from WEP to WPA2

Reduce the transmission power on the WAP

Disable the SSID broadcast

Enable MAC filtering

Answer: B

Explanation: If your wireless signal is reaching beyond your walls, you can reduce the power of the transmission to keep it within the building. Additionally, you could switch to a more directional antenna to reduce the signal from being radiated in all directions.

During your wireless survey, you detected another wireless access point with the same SSID as your access point. What kind of attack might be occurring?

IV Attack

Rogue AP

Evil Twin

Bluesnarfing

Answer: C

Explanation: An evil twin is an access point that is controlled by the attacker which uses the same SSID as your access point and usually is transmitting at a higher power level in an attempt to get your users to connect to the evil twin instead of your WAP.

Which of the following is the most secure type of cabling and produces no data emanations?

Fiber optic

Coaxial

UTP

STP

Answer: A

Explanation: A fiber optic cable uses light instead of electricity to transmit the data across the network. It doesn’t produce any data emanations, is the most difficult to wiretap, and is considered the most secure option for cabling.