# Discussion: Security Features of Wireless Technologies

2223

22 unread replies.

23 replies.



**Discussion: Security Features of Wireless Technologies**

**Learning Objectives and Outcomes**

* Identify security features of current wireless technologies.

**Assignment Requirements**

You are researching the following wireless security features for your company network:

* WEP and WPA2
* MAC address filtering
* SSID broadcast

Answer the following question(s):

1. Which combination of wireless security technologies are most appropriate in the enterprise, and why?

In the enterprise, WPA2 would be the only viable option when considering encryption based security for access points. As we learned in our lab this week, WEP is pretty massively insecure, and it really shouldn’t be used anywhere.

SSID broadcast may be advantageous in some areas of enterprise implementation where you have numerous employees that need access to an access point or where you have new employees coming and going with frequency, but you may also want to consider turning this off if you are implementing security for a network that will be transmitting sensitive data or have an access point that is placed in such a way that it is more likely to broadcast to a range outside of the enterprise.

1. Which combination of wireless security technologies are most appropriate for public access, and why?

I believe WPA2 is really the only option of the two when considering encryption based security for public access as well. There are still routers that do offer WEP as an option, but they all offer a better standard of encryption as well, so why not use the better standard?

In public access networks, you would likely want to broadcast your SSID as you can’t reliably get this information to everyone who might connect.

In the case of public access, mac address filtering may also be useful in the case where the user is presented with a captive portal. If you want to present the users with a set of terms and conditions for using the public access network before giving them full access, you could use a captive portal that captures their mac address and then adds it to the list of allowed devices by mac address.

Fully address the question(s) in this discussion; provide valid rationale for your choices, where applicable; and respond to at least two other students’ views.

**Required Resources**

* Course textbook
* Internet access

**Self-Assessment Checklist**

* I fully addressed the question(s) in the discussion instructions.
* I included justification or rationale for my choices, where applicable.
* I responded to at least two other students’ views.
* I followed the submission guidelines.

Please follow the outlined guidelines of this discussion:

* *Be respectful and open to opinions and ideas that differ from yours. The exchange of diverse thoughts, ideas, and opinions are an essential part of the scholarly environment. Keep in mind that the people in your classes may come from backgrounds and have views that may vary significantly from your own.*
* *Flaming is not appropriate under any circumstances. While everyone (learners and instructors alike) is encouraged to share ideas and opinions openly, you should never use insults or resort to name-calling even if you disagree strongly with what someone else has written. Insulting remarks and name-calling are never appropriate in an academic setting. Flaming is the posting of messages that are deliberately hostile and insulting in an online social context.*
* *When responding to messages or posts made by others, address the ideas, not the person.*
* *Be careful when using sarcasm and humor. Without social cues, such as facial expressions and body language, a remark meant as humorous could come across hurtful or offensive. Don't assume that the use of emoticons, such as :-) are enough to convey your tone or intent.*
* *Capitalizing whole words is generally seen as SHOUTING and is often offensive to the reader. Use all capital letters sparingly, such as to highlight a meaningful word or point*