[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@210c1d6a0130413e85b52cfc1df03897?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref: <https://www.computerworld.com/article/2577244/top-10-vulnerabilities-in-today-s-wi-fi-networks.html>

**Top 10 Vulnerabilities in Today's Wi-Fi Networks**

By Sandeep Singhal

Computerworld | JUL 15, 2002 12:00 AM PST

How can you plug the holes in your wireless network? Here are 10 tips:

**1. Hackers are looking for easy targets.**

Avoid advertising the presence of your wireless LAN: The easier it is to find, the more likely it will be a target. Be sure to change the Service Set Identifier (SSID) so that it's not the factory default, and turn off SSID broadcasting. If possible, adjust access point (AP) antennas and power levels to avoid signal leakage to areas where coverage is neither required nor desirable.

**[ Related:**[**How IT can keep remote workers’ Windows 7 PCs safe**](https://www.computerworld.com/article/3574873/how-it-can-keep-remote-workers-windows-7-pcs-safe.html)**]**

**2. It is easy to "convert" a device so that it looks like another device.**

Lost or stolen devices are also a severe threat. Media Access Control addresses are, therefore, a poor method of network authentication. Instead, rely on device-independent authentication, such as user names and passwords, with integration with existing network directories or authentication schemes. Wireless LANs are a natural extension to RSA SecurID token deployments.

**3. Wireless data requires data encryption.**

Built-in wireless LAN encryption (such as Wired Equivalent Privacy) is weak. Instead, use virtual private network technologies such as IPsec with triple DES to protect data. Avoid proprietary schemes in order to assure maximum interoperability.

**[**[**Download CIO's new Roadmap Report on 5G in the enterprise!**](https://www.cio.com/resources/form?placement_id=1f19e814-6f17-4eda-aff9-23032698928b&brand_id=256&locale_id=1)**]**

**4. Limit or control where wireless LAN traffic can go.**

If the wireless LAN is to be used for a selected purpose, such as to access an enterprise resource planning system, then place specific packet filters on the wireless LAN to allow only that access.

**5. Don't place APs on desks or other places that can be easily accessed.**

Unscrupulous visitors or careless employees can easily move, replace or reset the APs. Security can't be assured in such insecure locations. Instead, move management and security to the wiring closet.

**6. Actively monitor AP configurations.**

It's not sufficient to configure an AP correctly; once configured, the AP must *stay* properly configured. Consider that it is easy for someone to perform a hardware reset on an AP that sits on a desk or ceiling. By actively monitoring the AP configuration, you can ensure that the AP is automatically reconfigured should such an event occur.

**7. Be aware that APs are easily installed by employees and intruders and may easily bypass the enterprise's wireless security policies.**

Active sniffing for these rogue devices is a critical operational requirement. New tools to ease this task are readily available.

**8. Over a wireless LAN, an intruder can attack the wireless clients themselves in a peer-to-peer fashion.**

This attack can give the intruder network access by simply using a legitimate client as an accepted entry point. To address this issue, desktop firewalls should be deployed, along with network management tools that actively audit and manage the client before permitting access via the wireless LAN.

**9. Prevent denial-of-service attacks by ensuring adequate bandwidth management on the wireless LAN.**

The wireless LAN bandwidth is relatively limited and shared by multiple users. Particularly in environments in which different users need to perform different mission-critical tasks, this bandwidth must be policed to provide fair access.

**10. Deploy real-time policy management.**

As they are deployed, wireless LANs will span entire campuses and incorporate multiple global sites. Security policies (e.g., valid user lists or access rights) will naturally change. These changes must be reflected in real time throughout the wireless LAN to reduce the window of opportunity for intrusion and, more important, provide immediate lockdown of detected security holes.

*Singhal is chief technology officer at*[*ReefEdge Inc.*](http://www.reefedge.com/)*in Fort Lee, N.J.*