Here are some relatively simple, low-cost ways to optimize the security of your wireless LANs. They're not perfect, but they do provide at least a first line of defense. They are listed in approximate order of difficulty and cost.

To Start With

1. Enable the highest level of WEP (Wireless Encryption Protocol) that ships with the access point. WEP may be flawed, however it does provide some protection. 802.11b and 802.11g provide up to 128-bit WEP, while 802.11a provides up to 152-bit WEP encryption.

2. Change the default SSID (Service Set ID) that ships with your access points and/or wireless router. The default name of a NETGEAR Access Point and Router is, "Wireless." We will be migrating to "NETGEAR" as the default SSID in the near future. Finding an access point with the default SSID signals an unguarded access point.

3. Implement infrastructure mode, where all wireless clients on a network link directly via an access point or wireless router. Disable the "Ad-Hoc" mode, which enables a peer-to-peer network and that allows a user to connect with other wireless LAN cards. This opens the door for any hacker in wireless range to access your network through a legitimate wireless user.

4. Set up MAC Address Authentication via access control lists (ACLs). Configure your access points so they allow only clients with specific MAC addresses to access the network, or allow access to only a given number of MAC addresses. This can be set up as part of a NETGEAR access point or router configuration.

5. Disable the "broadcast" mode in which access points periodically transmit their SSIDs. Since hackers know the default names of many access points, they can use freeware utilities, or even Windows® XP, to find the names of nearby wireless networks. NETGEAR products will have this block SSID broadcast feature in Q2’03.

A Little More Involved

6. If you're running SNMP (Simple Network Management Protocol) agents on your access points, assign a non-obvious name to the "community" that identifies which management applications can communicate with those agents. That way, wireless hackers can't just sniff around for the default community names that ship with many management tools.

7. Perform a regular audit for rogue access points. NETGEAR recommends that you scan at least once a quarter, if not once a month. This can be as easy as walking around with a wireless notebook equipped with free sniffer software such as NetStumbler (or Windows XP), or as ambitious as using SNMP queries to find new devices that have been added to your network. Once you find the rogue access points, you'll need to be able to shut them down or reconfigure them.
8. Place access points on separate subnets and put a firewall between that subnet and the main corporate network. This mimics the architecture of many security tools that puts a gateway or other security server between the access points and the wired network.

**Even More Secure**

9. Implement Virtual Private Networking (VPN) over wireless LAN. This technology makes it possible for users to communicate securely via a VPN tunnel between the client desktop or notebook PC and the wireless access point or router. VPNs employ encryption and strong authentication methods as mechanisms for hiding or masking information about the private network topology from potential attackers on the public network. This solution typically requires a separate VPN Server.

10. Educate your network users about the security risks of wireless, then create and enforce a wireless security policy.

**What Does All This Say?**

For home and small business: The combination of using a unique SSID + MAC Address Authentication + WEP encryption is most likely an acceptable level of wireless security. All currently shipping NETGEAR products support this level of security.

For medium and enterprise business: With centrally managed administration for a large number of users and the ease of deployment and control, VPN is a better choice for wireless security. VPN offers the most powerful methods to ensure that network access is strictly limited to users who can be authenticated via the VPN Server. All of NETGEAR’s wireless LAN products support VPN pass-through. Alternatively, the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall combines the capabilities of a router, access point and VPN server all in one simple-to-manage device.
L-com, a global leader in the manufacture of wired and wireless connectivity products, offers a wide range of solutions and unmatched customer service for the electronics and data communications industries. The company’s product portfolio includes cable assemblies, connectors, adapters, computer networking components, and custom products, as well as their HyperLink line of wireless products which include Antennas, RF Amplifiers, Coaxial lightning and surge protectors, and NEMA rated enclosures. L-com’s HyperLink wireless products are designed for WiFi, WiMAX, SCADA, 802.11a/b/g/n, RFID and Bluetooth applications. Trusted for over 30 years, L-com, which is headquartered in North Andover, MA, is ISO 9001: 2008 certified and many of its products are UL® recognized. www.l-com.com

For more information, contact your L-com sales representative at 1-800-343-1455 or e-mail sales@L-com.com.

Corporate Headquarters and Fulfillment Facility
45 Beechwood Drive
North Andover, MA 01845

Cable Assembly Manufacturing Facility
1755 Osgood Street
North Andover, MA 01845

Far East Manufacturing and Fulfillment Facility
7 ChunHui Road, SIP
Building 1
Suzhou, Jiangsu, China
P.C.: 215121

Wireless Manufacturing and Fulfillment Facility
1201 Clint Moore Road
Boca Raton, FL 33487