

Executive Summary

Wireless LAN (WLAN) deployments have become a standard part of business networks. According to In-Stat research, more than 70% of businesses in a recent survey use WLANs in their organizations. Currently, most of these are limited deployments to extend the wired LAN for employee or guest access to email and the Internet.

Businesses face the two key challenges with managing wireless in their organizations:

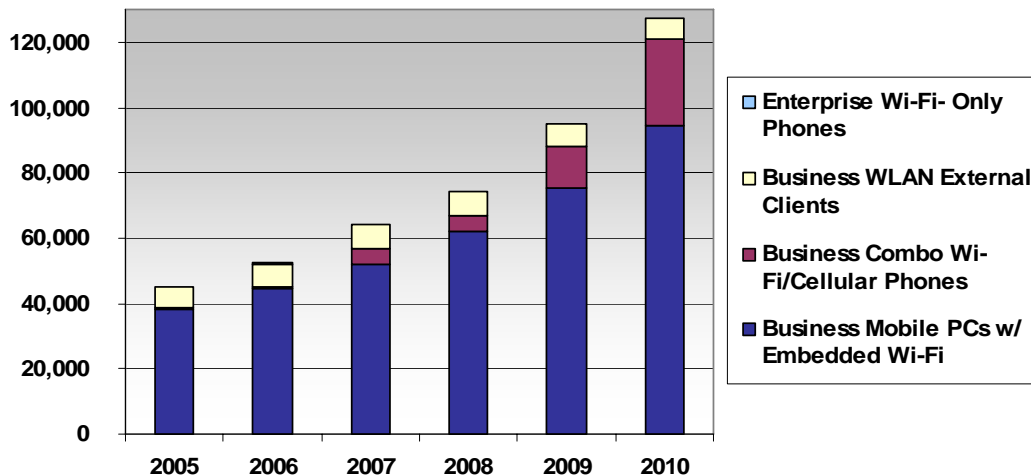
- Use of inexpensive, consumer-grade WLAN products in the business premise
- Proliferation of portable client devices that are wireless enabled

The unit volume forecasted for wireless clients confirms the continuing pervasiveness of devices with wireless capability, as shown in the following figure.

HIGHLIGHTS

- By 2010, more than 128 million new client devices with wireless capability will ship into the business premise, including mobile PCs and Wi-Fi handsets.
- Despite the ratification of key wireless standards, In-Stat research shows the actual use of stronger security mechanisms in current WLAN deployments is low.

Figure 1. Business WLAN Client Forecast—by Form Factor (Units in Thousands)



Source: In-Stat, 4/06

For WLANs to successfully move beyond limited installations, businesses need to employ a variety of security mechanisms to protect their operations and assets. Although industry standards prescribe architectural approaches to wireless security, the required equipment and system upgrades may be too costly for many organizations to deploy right away. There are practical steps businesses are taking immediately, including user education and wireless security policies. Security conscious companies are also deploying encryption solutions to protect data on mobile clients. In the long term, the integration of wireless security into wired security and networking platforms will be critical for scalability and operational efficiency.