

APPLICATION NOTE

PUBLIC HOT SPOTS



Secure Airwaves to Protect Corporate Data

The challenge:

As workers become more mobile, confidential company information becomes more dispersed in public hot spots. Despite the most secure access point interfaces and the most effective management gateway devices, the air itself must also be “locked” in order to prevent snooping over the airwaves. The traffic passing from a client laptop or PDA to the access point, if not encrypted, can be vulnerable to industrial espionage or credit card fraud. In the past, service providers recommended VPNs to ensure data privacy, but are now offering an encrypted service to meet the demands of their clients. Yet inexpensive access points lack the full-scale data protection that corporations are demanding of their service providers. Much like the advent of laptop computing brought the sudden awareness that a fellow plane passenger could be a competitor looking over your shoulder – wireless computing forces the realization that an under-featured access point could open a window for Peeping Toms.

The solution:

Wi-Fi Protected Access (WPA) and IEEE 802.1x technologies protect corporate intellectual property by encrypting data between client and AP – and providing mutual authentication between the client and the network. This alone is not sufficient though, as service providers have differentiated client needs and need to simultaneously support more secure access methods as well as open, unencrypted sessions for other subscribers. ORiNOCO access points support simultaneous WPA and unencrypted data, allowing support for all types of subscribers.

The products:

- ORiNOCO AP-4000
- ORiNOCO AP-2500
- ORiNOCO AP-2000
- ORiNOCO AP-600
- ORiNOCO client cards



Proxim Corporation
935 Stewart Drive
Sunnyvale, California 94085

tel: 800.229.1630
tel: 408.731.2700
www.proxim.com