

# APPLICATION NOTE

## PUBLIC HOT SPOTS



### Secure Management Interfaces to Protect Hot Spot Service

#### The challenge:

From mischief-makers and petty theft to serious political activism, the Internet represents an opportunity for illegal activities of many kinds. The past decade has seen online credit card fraud, unpaid service "hitchhiking," rapidly evolving email worms, and full-scale denial-of-service attacks on major corporations. Without robust security measures, public wireless technology makes the Internet accessible to criminal invasion from outside locked doors. Consumer access points found in the home are not equipped to handle professional hacking attempts to which public networks are susceptible. They are optimized for easy access rather than careful service protection and billing integration.

#### The solution:

Proxim access points are designed with security measures to protect Wi-Fi service in the most publicly accessible locations in the world. Proxim's ORiNOCO AP-2500 integrates an access gateway which allows only authorized, paying users to gain access to public Internet service. Secure management interfaces on Proxim access points minimize the risk of hackers accessing and altering the device settings. Rogue access point detection proactively helps administrators find hackers that may attempt to snag unsuspecting subscribers or flood the airwaves and create a denial-of-service-attack. Proxim simultaneously supports multiple security methods to prevent unauthorized access, ensuring that network service is uninterrupted.

#### 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](http://www.proxim.com)