

# WLANs Outside?

A quick introduction why 802.11-based systems are not appropriate for broadband wireless access



## Introduction

Wireless LANs are now everywhere. The main reason for their tremendous success is their design, drawn by the IEEE under the collective name 802.11. The standards were engineered to be easy to implement, not to require sophisticated electronics, and therefore to make WLAN equipment inexpensive. It is the simplicity of the 802.11 protocol design that made WLANs as popular as they are today.

## The 802.11 WLAN goes outside in a box – or does it?

Drawing from the success and subsequently lowered costs of standard WLAN equipment, some vendors have attempted to adapt the same technology to outdoor broadband wireless access applications, by installing indoor WLAN access points into outdoor enclosures and equipping them with large antennas. This seems to work, but there are fundamental flaws with this approach, stemming from one of the protocols that made WLANs so popular – the 802.11 standard called CSMA/CA.

## Serious problems in a nutshell

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the MAC protocol defined by IEEE that is used by products based on the 802.11a and 802.11b/g WLAN standards. It deals with medium access – the technique used to moderate how wireless nodes use the radio channel. It was designed for indoor office environments, where all nodes are within a hundred meters or so from each other. It is assumed that all the wireless nodes are within this certain area and can all receive each others' transmissions, because the protocol requires that each node "listens" to the wireless channel before transmitting data. If the channel is free, the node can transmit. In the indoor office environment it works, because all the nodes can "hear" each other and know when the channel is free and when it is not. However in an outdoor, access network this is no longer the case, and some severe problems appear, the worst being the so-called "hidden node" issue.

The "hidden" node problem occurs when a wireless node cannot receive the transmissions of other nodes, and in an outdoor access network with directional antennas this will happen very often. The node does not receive the transmissions of other nodes and, safely assuming that the channel is free, transmits on the channel. If the channel really happens to be free, then that's not a problem; but in a working wireless network that's very unlikely and most probably, a collision will occur. What's even worse, there will likely be more than one "hidden" node in such a network, and collisions will happen even more often.

While the protocol does have a basic mechanism to deal with collisions (wait and retransmit), in this scenario they will keep happening again and again and the more nodes start to use the network, the more serious the problem will become. Extensive collisions result in lots of lost frames, extensive retransmits, and delays and will most probably bring the entire network to a standstill.

The next page discusses what are the business implications of this, and what do Alloyant products do to solve it.



### **Try to save a penny today, pay ten tomorrow– the business case, if any**

While 802.11 CSMA/CA MAC protocol proved to be a success in indoor, short range Wireless LAN environments, it is not suitable for outdoor, long range access applications. When choosing a wireless access system, it is very important to check whether it is based on the stock 802.11 designs, and many systems are. If so, the system will suffer from the problems described above and will most likely not perform well.

The lower cost of standard WLAN equipment and the proliferation of vendors who try to sell them for outdoor broadband, have led to many startup ISPs to get into business quickly. On the other hand however, the limitations of the technology quickly prevent them from scaling and increasing their business – they simply can't add more customers without decreasing service quality. This leaves them vulnerable to attack from other alternative providers who may be offering DSL or using a superior wireless technology and who can quickly overrun the small ISP.

### **StreamStar saves the day**

Alloyant StreamStar systems are designed for serious, large scale, outdoor broadband wireless deployments. For that very reason one of the main differentiators of the system is a highly advanced MAC protocol, which is proprietary and is pending patents. This technology is entirely different from the 802.11 protocols and is capable of high performance and superior system capacity, and that is a matter of life and death to a wireless ISP. StreamStar is superior to any 802.11-based system on the market.

A superior wireless access system means more subscribers, more revenue, a stable service, and continued business.

For more information, please check the StreamStar pages on our website at <http://www.alloyant.com>