BILL BOOTHE

Wi-Fi Basics

What You Need to Know - Part I

WIRELESS TECHNOLOGY IS ALL AROUND US – LITERALLY. IN ITS MOST COMMON FORM, WIRELESS IS WI-FI – AN INVISIBLE MESH OF RADIO WAVES ALLOWING US TO CONNECT OUR MOBILE DEVICES AND PCS TO THE CYBER WORLD. WE USE WIRELESS TO ACCESS EMAIL, SURF THE WEB AND CONDUCT MYRIAD SOCIAL AND BUSINESS ACTIVITIES.

Many private clubs are in a wireless quandary – with a board pulling one way to maintain traditional limitations on cell phone usage, and members pulling the other way to use their smartphones, iPads and other mobile devices and PCs throughout the club. The members are winning!

There are two basic ways for you to utilize wireless service – private and public. Private use is by the club's employees. Public access is all about members and guests – for Internet access, email and texting. The key here is separation. The members and guests must be separated from the club's private network. That means two separate wireless networks – one for club personnel, the other for members and guests.

As private clubs begin to deploy wireless systems, they quickly come to realize that this venture is no picnic. The technology is complex, the standards are confusing, the deployment methods are varied, and there are endless brands from which to choose. As with the deployment of all new technologies, mistakes are made. This article is intended to teach you the basics of wireless technologies, and help you avoid any missteps along the way.

In Part 1 of this article we address how Wi-Fi works and how it is best deployed in private clubs.

WI-FI – HOW IT WORKS

Wi-Fi uses radio waves to transmit data. The radio waves connect remote devices such as PCs, printers, smartphones and other mobile devices (iPad, Kindle, Nook, Galaxy, etc.) to a wired network. This wireless extension of the wired network provides access to the Internet, email and other applications.

Wireless signals are transmitted through WAPs – wireless access points. Essentially small antennas, each WAP can handle up to 30 active devices at a distance of up to about 200 feet indoors and 800 feet outdoors. However, these distances are under ideal conditions and can be reduced by as much as half based on the number of users and their type of activity. As well as signals might be obstructed when they must travel through walls, ceilings/floors, windows with reflective tinting, and other obstructions.

When deploying wireless solutions for business use, WAPs are typically positioned to create a "mesh" of "access cells" that provide coverage to all intended areas. This allows Wi-Fi-enabled devices to maintain a connection while moving from one WAP to another (similar to cell phone towers).

As with any type of communications technology, Wi-Fi speed is all-important. Transmission speed, or bandwidth, is measured by how quickly a "bit" of data can be sent. The standard unit of measure for transmission speed is Mbps (Megabits per second, or one million bits per second). The trick here is to provide enough transmission speed to accommodate the amount of bandwidth needed by the users on the wireless network.

WI-FI STANDARDS

Wi-Fi technology is governed by the I.E.E.E. (Institute of Electrical and Electronics Engineers) internationally, and the FCC (Federal Communications Commission) in the United States. These governing bodies have established standards that specify transmission speed, signal strength (distance), and other factors. The first consumer standard – 802.11b – set in 1999 limited the transmission speed to 11Mbps. At

SEE TECHNOLOGY BOOTHE - PAGE 99

that speed, wireless was used mostly for Internet access and email, which require a small amount of bandwidth.

Four years later in 2003, 802.11g was established with a top speed of 54Mbps, and wireless began to include the remote use of software applications such as accounting and POS. Today's standard – 802.11n – maxes out at 108Mbps and provides enough bandwidth for 4-5 users to run business applications such as POS, or about 30 users to access the Internet – all on a single WAP.

The thing to remember is that the overall performance slows incrementally as the WAP adds more active connections – and as the bandwidth requirements of those users increases. If too much bandwidth is used, the WAP becomes saturated and won't allow more users to connect. When in doubt, deploy more WAPs.

Since clubs have been adding new Wi-Fi equipment over time, it is common to find a combination of b, g and n devices attached to a club's network. This "alphabet soup" of Wi-Fi devices can be debilitating to network performance.

Here's why: 802.11n devices (using the current standard) are "backward compatible" to b and g devices. A club can add n devices to its mixture of b and g equipment and it all works. Clubs can save money by using older WAPs rather than replacing them every time a new standard is released, and everybody's happy – right?

Wrong. The b (11Mbps) and g (54Mbps) devices throttle the whole wireless network down to their transmission speed. Just one b device on a wireless network will make everything else run at 11Mbps. So if you have any b devices on your club's wireless network, get them off quickly.

WI-FI USAGE AT YOUR CLUB

There are two basic ways for you to utilize wireless service – private and public. Private use is by the club's employees. Examples are desktop or notebook PCs and printers used in the various club departments. Or wireless POS devices used on the patio or out by the swimming pool.

Public access is all about members and guests – for Internet access, email and texting. Members might access your wireless service in meeting rooms, specified "hot spots" around the club, or in guest rooms, if you have overnight lodging.

The key here is separation. The members and guests must be separated from the club's private network. That means two separate wireless networks – one for club personnel, the other for members and guests.

There is no gray area here. For security considerations, they must be separate. Luckily this separation can be accomplished with Virtual LANs (VLANs) at a reasonable cost, so deploying separate networks won't be much of a stretch on your technology budget (more on costs later).

Remember that the member/guest VLAN should be behind the club's firewall and should only allow access to the Internet. In Part II we'll address member use of Wi-Fi, security and costs. **BR**

Bill Boothe is president of The Boothe Group, LLC, an independent consulting firm that helps clubs understand computer technology, make good decisions and receive the highest value from their technology investment. Bill can be reached at bboothe@boothegroup.com. Tom Weiman, a partner with ClientFirst Consulting Group, LLC, provided technical input for this article. Tom teamed with Bill Boothe on a number of projects for private clubs. Tom can be reached at tweiman@clientfirstcg.com.

bulky power hungry POS and back office workstations with sleek energy efficient tablets and all-in-one devices, which access their processing power via the Internet.

No longer do local IT guys drive to and from the club (more carbon emissions) to install Windows one more time. Instead, users pull their iPad out of the box, and a few minutes later they are up and running.

Here's one novel solution. One club wanted to have board members use iPads for their board of director binders. Now each of their board members receives an iPad (or use their own), instead of a bulky binder with documents for a board meeting.

When changes are made to a document, everyone gets an electronic update. Gone are the days of 12 cases of paper a year, being delivered to the club, loaded into a copier, printed, sorted into binders, and thrown into the back of board member cars to just consume a little extra gas…not to mention the board members love this new approach.

Focus on synergy. Find a solution that reduces your IT expense, reduces your IT management effort, and improves your carbon footprint at the same time. These are solutions that everyone can get behind. The hosted solution and cloud computing options finally bring this synergy to fruition by leveraging state of the art technology managed by enterprise level technical talent.

Best of all, there's no sacrifice required. Your members should know about it too, it's important for them to know how committed their club is to a greener tomorrow. **BR**

Boyd Carr is a virtual solutions advisor with Virtual Shaping, Inc and can be reached at (925) 269-7177 or BoydCarr@VirtualShaping.com

BILL BOOTHE

Wi-Fi Basics

What You Need to Know - Part II

WI-FI TECHNOLOGY IS ALL AROUND US – LITERALLY. WE USE WIRELESS TO ACCESS EMAIL, SURF THE WEB AND CONDUCT MYRIAD SOCIAL AND BUSINESS ACTIVITIES.

But many private clubs are in a Wi-Fi quandary – with a board pulling one way to maintain traditional limitations on cell phone usage, and members pulling the other way to use their SmartPhones, iPads and other mobile devices, and PCs throughout the club.

The members are winning!

In Part 1, we addressed Wi-Fi deployment and standards. Now we'll complete our review of Wi-Fi by addressing member use, costs and security.

Member use of wireless devices: The ongoing battle between tradition and "progress" in private clubs is nothing new. For many clubs, a discussion is taking place regarding the appropriateness of members using their mobile devices in and around the clubhouse. Here are some factors to consider for that discussion:

Many of your club's members are "tethered" to their mobile devices:

- 51 percent of persons age 55-64 own a SmartPhone.
- 42 percent of persons age 65 or older own a SmartPhone.
- They use their SmartPhones to text, email and access the Internet – and, oh by the way, for voice calls as well.
- These are persons with household income of $100,000 or more – your members! (Source: Nielson Mobile Insights).

Today's members don't see mobile devices as a convenience – they're a necessity. Members have come to expect fast, reliable, free wireless access almost everywhere they go (stores, restaurants, schools, airports, etc.). Then they come to the club and enter a time warp. It doesn't have to be that way.

The main purpose of cell phone restrictions was to eliminate annoying one-sided phone conversations in and around the club. After all, members are at the club to interact with other members, not to carry on lengthy business or social conversations with outsiders.

But the world has changed, and cell phones are now powerful computers that are an integral part of many members' lives. Members understand and appreciate the voice prohibitions, but as time marches on their patience with data restrictions is growing thin.

Fortunately, there's a way out of this quagmire. Simply separate voice from data. Allow members to discretely use their mobile devices for texting, email and Internet access, but not to make annoying phone calls. A simple change to your club's rules can turn a major annoyance into a welcome amenity for more members than you might imagine.

WiFi costs: Some good news about wireless costs. Compared to most member amenities, wireless is a bargain. Here are three cost scenarios to consider:

1. Small Wi-Fi installation
   - Country club with two meeting rooms, one hot spot and no guest rooms
   - Two wireless APs
   - $2,400 for equipment and installation

2. Medium-sized Wi-Fi installation
   - Country club with six meeting rooms, 6-12 guest rooms and two hot spots
   - Four wireless APs
   - $3,600 for equipment and installation

3. Large Wi-Fi installation
   - City/athletic club or large country club with 12 meeting rooms, six hot spots and 50 guest rooms
   - 10 wireless APs
   - $6,300 for equipment and installation

No matter the size of the wireless installation, Wi-Fi is an excellent investment to provide a much-appreciated member amenity.

Wi-Fi security: Since the transmissions over a club's wireless network should be private and secure, proper access control and security measures should be deployed. Those measures can protect all users of the club's wireless network - staff, members and guests. The current standard for Wi-Fi protection is WPA2 (Wi-Fi Protected Access 2). This advanced system is

virtually impossible to compromise, and is the only system that should be used. Intruders can easily breach earlier versions such as WEP and WPA.

WPA2 requires that an access ID and password be issued to all users. These credentials should be changed every few days and can be published throughout the clubhouse. The goal is to make sure that these credentials are only known to members and guests, and not to the general public.

Many clubs find the issuance of login credentials a bother and simply leave their wireless networks open for anyone who is in range of the signal. Open networks are an invitation for unauthorized snooping as users conduct sensitive and confidential activities over the club's network.

Under no circumstances should staff access an unsecured network. If using access security is deemed too bothersome for the members/guests, be sure to provide a clear warning at sign-on that the wireless network is not secure.

There are a few other measures that can be deployed to beef up your club's wireless network:

1. Internet content filtering can be used to control the content that can be accessed on the Internet.
2. SPAM filtering can be added to prohibit users from using the club's wireless network to propagate SPAM.
3. Port-to-port security protects individual member/guest machines from access by other guests on the public network.
4. Virus containment protects member/guests from contracting viruses from other infected machines on the network.

These four measures are a must for all wireless networks. Note that these four security features should be included with the club's Internet router (firewall) and anti-malware products. There should be no additional investment required to acquire these features.

Service Considerations for Overnight Guests Rooms: Members and guests have come to expect fast, reliable wireless service when they stay overnight. To satisfy that requirement, you will need to provide 24x7 network monitoring and user support.

Round-the-clock support means the availability of a qualified technician to assist guests with the use of the club's wireless network. If your club does not have staff that can fulfill these responsibilities, it is recommended that you contract with a 3rd party source to provided the needed services. The costs and arrangements for these services vary widely, with a cost range of $250 to $500 per month or more depending upon the extent of the service needed.

Wi-Fi Wrap-Up: Wi-Fi services are making their way into many private clubs. Deployed correctly, Wi-Fi can provide club staff with the ability to attach to the private network from a variety of locations, plus members and guests can connect to the public network to enjoy a valuable communications amenity. All for a very small investment.

If your club has already deployed Wi-Fi services, be sure to follow our bandwidth standards and security recommendations. If your club has not yet deployed wireless, what are you waiting for? **BR**

Bill Boothe is president of The Boothe Group, LLC, an independent consulting firm that helps clubs understand computer technology, make good decisions and receive the highest value from their technology investment. Bill can be reached at bboothe@boothegroup.com. Tom Weiman, a partner with ClientFirst Consulting Group, LLC provided technical input for this article. Tom has teamed with Bill Boothe on a number of projects for private clubs. Tom can be reached at tweiman@clientfirstcg.com.