Technical Considerations for Implementing Wi-Fi in Retail Businesses

Evaluating network design, management and security options for Wi-Fi deployment

The potential business benefits of implementing Wi-Fi in convenience stores are clear. Roughly three-quarters of Americans (2017, Pew Research Center) now own a smartphone, offering Wi-Fi gives brick and mortar retail and restaurant businesses the opportunity to gain important marketing data, build customer loyalty, draw more customers inside stores and meet the expectation of their hyper-connected customers.

According to the PCI DSS Wireless Guidance document, "regardless of whether wireless networks have been deployed, periodic monitoring is needed to keep unauthorized or rogue wireless devices from compromising the security of the CDE (card data environment)." This could change how many companies view wireless since some work in this area is required even if the access isn't available in stores. The same document confirms that wireless access can be pushed out of scope by segmenting the CDE traffic away from the wireless traffic or by putting a firewall in between the wireless network and the CDE.

Network design, maintenance, monitoring, and security are all important considerations retailers must take into account before deploying free customer Wi-Fi programs in their stores. This paper will outline the technical opportunities and challenges associated with Wi-Fi networks, and examine the different options available to merchants.

Network design, maintenance, monitoring, and security are all important considerations to take into account

Getting Connected

Choosing the right access technology plays a key role in delivering a reliable and cost-effective high-speed connection for mission critical operational systems, such as credit card networks, as well as value-added services like Wi-Fi access. There are a number of high-speed Internet connection methods available to stores, including fixed-line options (DSL, Cable, Fiber, T1) and wireless options (3G/4GLTE, satellite).

If your company is just beginning to weigh the benefits of Wi-Fi for your stores, check out "Business Considerations for Leveraging Wi-Fi at C-Stores" for more information about the opportunities and caveats related to the technology.

The most popular and cost-effective connectivity options are DSL and cable, but reliability and availability depend heavily on local infrastructure. Stores in remote areas that are not served by more conventional broadband services can use either satellite or fixed wireless connection based on radio signals, but these options are more expensive than comparable broadband services. Since customer Wi-Fi tends to consume a lot of bandwidth, fiber-optic cable may be a good, high-speed option if it is available in your area. To learn more about the connectivity options available, take a look at "Getting your Retail Business Connected" for a side-by-side comparison of the different services and technologies.

Infrastructure Design

No matter which approach is used for initial connectivity, the Wi-Fi infrastructure must be configured to protect store and customer data, and meet Payment Card Industry (PCI) security standards. In addition, it should be set up so that it does not interfere with day-to-day operations of the store or the devices in it.

"Allowing outsiders on the private store network could open your company up to hackers and data the theft."

You might think the simplest way to offer public or guest Wi-Fi access is to let people on an existing Wi-Fi network used by the store, but this isn't secure. Allowing outsiders on the private store network could open your company up to hackers and data theft. Fortunately, there are two secure options that enable retailers to offer Wi-Fi to their customers, without compromising important information.

1. *Create a Separate Network*
   The most secure option involves creating an entirely separate connection for customer Wi-Fi so that the network is not tied to core store operations in any way. By setting up a new independent network for free customer access, you can eliminate the bandwidth and security issues that can be associated with adding free public Wi-Fi to an existing network. However, the additional costs for the hardware, connection, maintenance and monitoring of a separate network make this option the more expensive and time consuming for staff of the two available. On average, you are looking at spending an additional $50.00 per month per store.

2. *Partition the Current Connection*
   A lower cost option that can still be very secure involves partitioning a small piece of your store's current connection for the public Wi-Fi. This allows store operations and customer Wi-Fi to leverage the same network, but prevents them from interacting with each other by using a firewall so that no Wi-Fi device can access the store network.

Cable modem (or other type of network connection), wireless access point (AP), and uninterruptible power supply (UPS)

For any configuration your business adopts, it's a good idea to establish and publish a policy for customer access, and to enable "traffic shaping" to assure that access is fairly shared among all connected customers and doesn't impact store operations. In order to determine how much of your bandwidth should be dedicated to the customer Wi-Fi network, take some time to monitor the store's minimum and maximum bandwidth requirements. Once you know how much bandwidth your store needs (plus some safety margin) to operate without interruption then partition the remaining bandwidth to your public Wi-Fi. After everything is set up, store managers and associates should not even notice the activity on the public network, because the Wi-Fi users will be limited to whatever bandwidth you have specified.

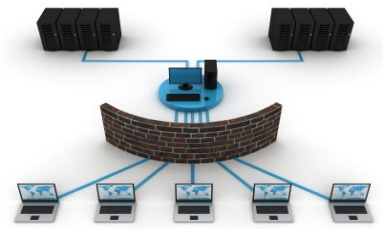
Hardware & Configuration

There are a few key things to think about regarding hardware and configuration of your Wi-Fi network –network connection, Access Point (AP) and power.
Whether you have a dynamic or static IP address, there is no important difference with respect to configuring customer Wi-Fi access, though static tends to be more expensive. Check with your supplier if you chose the less expensive dynamic network connection to make sure your provider can access and manage the AP equipment - not all suppliers can.

The AP serves as the source of connectivity that allows computers to connect wirelessly, but it is not as simple as setting up a wireless router in your home. There is a large variety of AP options available for business and retail locations, including APs that can securely serve both employees and customers using a tag-based segmenting switch. If you are already using Wi-Fi for employee use, then segmenting might be a good option for you.

You will also need to consider several variables to determine the appropriate power level and Wi-Fi signal strength for your store. The size of your footprint, interior and exterior structures and location of the router can all impact your power needs. Your supplier can help you with an evaluation and recommend which approach and hardware make the most sense for your store.

Operating in a 24/7 world? An uninterruptable power supply (UPS) can provide continuously available service, but keep in mind that the entire connection out to the Internet needs also to be continuously powered. It won't do any good to have the AP working with everything else between the store and the Internet powered down.



Once configured, it's important to monitor and maintain your free Wi-Fi network.

Maintenance & Security

Once configured, it is important to monitor and maintain your free Wi-Fi network on an ongoing basis to ensure that customer experience and network security continue to meet your expectations and requirements. You should treat it exactly like any other part of the network. In addition to monitoring for malicious activity on your public Wi-Fi network, PCI DSS standards state that you should have a documented process and test for the presence of unauthorized wireless access points on a quarterly basis. The PCI Council is planning to release a new set of Wi-Fi specifications later this year, so keep your eye out for these updates and our supporting paper, ""Wi-Fi and PCI 3.0."

As with your wired network, there is a not an out-of-the-box Wi-Fi solution or service out there that will make your company PCI compliant, so be careful when considering a provider that claims to do so.

Conclusion

Clearly, there are many technical opportunities and challenges tied to delivering public Wi-Fi. Beyond exploring the initial considerations for configuring and managing your Wi-Fi hot spot, you should talk to a couple of suppliers and ask questions to see what they know and recommend for hardware, security, PCI compliance and maintenance. The answers to these questions will depend on your unique business requirements and goals, but you are now equipped with a solid foundation from which to start the conversation.

About Acumera

Acumera provides managed security and network visibility for the payment systems and operations of multi-site retailers and restaurants. Our clients focus on growing their business by using Acumera's services, remote systems visibility, strong data security, and simplified compliance services. Since 2002, Acumera has been a trusted partner for thousands of networks.