Successfully Planning a Scalable and Effective Patron Wireless Network

Robert A. Caluori, Jr.

Abstract

Patron wireless networks are considered an essential component of the modern public library, yet the ever-increasing demand for the service presents challenges that seriously impact the ability of a library to meet the needs of the community they serve. This chapter of The Transforming Public Library Technology Infrastructure *provides recommendations for the planning, implementation, and monitoring of an affordable high-availability patron wireless network.*

Retrospective

Wireless technology that could be used to deliver Internet connectivity to consumer-level devices started to enter the market more than ten years ago. Using the IEEE (Institute of Electrical and Electronics Engineers) 802.11b standard, which was released in 1999, libraries that implemented wireless networks to deliver Internet access to their patrons were on the cutting edge of technology. However, business-class equipment was hard to find and very expensive. Many libraries chose to implement this emerging technology using consumer-grade equipment with those trademark blue Linksys access point/routers. Over the years, some may have even upgraded those access point/routers with open source firmware alternatives Tomato or DD-WRT. These oftentimes give the device a second life.

However, if that technology is still in use today, with or without new firmware, those same libraries that were once on the cutting edge now find themselves far behind the curve. Those aging access point/router combinations can no longer handle the volume of users and devices or keep up with the throughput demands of the modern wireless age. In addition, wireless equipment manufacturers have released affordable, high-quality business-class wireless equipment that can make the modern, high-availability wireless network a reality for libraries.

Overview

The patron wireless network is an essential component of the modern public library. In addition to expanding Internet access in the library without adding PCs, a patron wireless network is a vital public service, especially in areas where few people have high-speed Internet access at home. This service is equally as essential in the academic library, especially if the campus does not have a wireless network itself. The library may indeed be the only place where students and faculty can come to access the Internet on their own devices.

Allowing people to bring in and use their own device also adds a level of comfort to the library. Sometimes people are reluctant to use library PCs to access websites that may expose their personal information. Even though the wireless network is a public network, some people feel more at ease when they are using their own device. When word gets out, people will be drawn to the library to use the wireless network.

A key element to take note of is that this is the *patron* wireless network. This is not the network for librarians, support staff, or any library business operation. Keeping this network separate is in the best interests of both the patrons and the staff. It serves the patrons by providing dedicated access so that they don't have to compete with staff for bandwidth and serves staff by keeping the network they use secure. Data traversing a wireless network are easily captured. Performing tasks in the ILS (integrated library system) or any other library business system, especially one

that contains personally identifiable information (PII), should be strictly prohibited on this network.

Planning

There are three important things that one must do before implementing a patron wireless (Wi-Fi) network. Plan. Plan. Plan. Plan for bandwidth requirements. Plan for management, monitoring, and control. Plan for signal coverage and scalability.

Planning all of these elements may seem to be a daunting task, so it's important to take it one step at a time. The best place to start is to answer the simple questions that will help drive the answers to the more complicated ones. How many simultaneous users will this network need to support at its peak usage, and where are these users located when they are using it? Using that information, start at the access points for the network and begin working your way in.

A Note about Wi-Fi

Wi-Fi is neither a standard nor a technical term. Wi-Fi is a term coined by the Wi-Fi Alliance. This group works to help gain use and acceptance of the 802.11 standard through certification programs that focus on interoperability and backward compatibility. The term Wi-Fi has become synonymous with wireless networks and wireless-equipped devices.

Wi-Fi has been integrated into so many different types of technologies that it is safe to plan for every person who will use the wireless network having two or more Wi-Fi devices. Consider all of the Wi-Fi–enabled cell phones, game systems, tablets, and PDAs that walk into the library with patrons. There may even be a laptop once in a while. Even if the patrons aren't using these devices, any or all of them may seek out open networks automatically, connect to the network, and take up wireless bandwidth. If at this point it is known how many people will use the wireless network and where they will be located, double it to compensate for all of these potential nodes on the wireless network.

Access Points

The first consideration in access point (AP) selection is which protocol standard to use. Choosing between 802.11n and 802.11g can leave you in a state of analysis paralysis. The 802.11n standard is clearly superior in range, speed, and susceptibility to interference, but it comes at a significantly higher cost than 802.11g APs. Exploring purchase of a higher quantity of 802.11g APs may prove to be beneficial. It is likely that the amount of Internet bandwidth provided over the network will not exceed the capacity of the APs. Therefore more 802.11g access points will allow the network to have better signal saturation.

Good signal saturation is a valuable element in a wireless network. The business-class access points that will eventually outfit the network will undoubtedly have the capability of reaching the limits of the protocol. However, the patron's devices that the APs interface with do not. Small devices often do not have strong radios because of the power needed to operate them. Therefore, it may prove beneficial to consider lowering the signal strength of the APs to ensure integrity in both directions of the wireless data stream. Some wireless network controllers will also use the access points to sense one another's signal strengths and automatically adjust the strengths and channels to optimize coverage. If this is the case, placing APs closer together and within the manufacture's specifications is recommended.

Wireless Controllers

A wireless controller does just that; it gives the administrators control over the new network. The wireless controller can do everything from pushing out policies, settings, and upgrades to gathering usage statistics and AP status. This centrally managed system will be especially invaluable if the library has multiple branches or campuses or if this network is installed across a library system.

Monitoring and control will have benefits in managing problems. The controller can be configured to send system administrators notifications when an AP is reaching its usage capacity or goes down. Having usage statistics will help in managing the network by giving administrators the information they need to plan AP moves and additions. It is also helpful when justifying the costs associated with the network to decision makers and stakeholders.

Remote management will save time and money. Pushing firmware upgrades, policy changes, and settings remotely will speed up the execution of these changes and reduce travel costs. When justifying the upgrade of the current network to this new network, this is key factor to highlight to decision makers, and it contributes greatly to the return on investment.

How the communication between the APs and the wireless controller is set up can vary. The following are two examples. The first scenario is geared toward multiple locations, where having all APs on the same physical network is not possible; the wireless controller resides on another network such as the staff network. The second scenario outlines a possible configuration where all of the APs as well as the controller reside on the same network.

Scenario 1

In this scenario, the wireless controller is set up on the staff network. The access points are set up on a

network of their own at each branch, campus, or system library (location). A routing firewall can be used to establish a VPN tunnel between the patron wireless networks at each location and the staff network. The tunnel will be used exclusively to send management data back and forth between the APs and the wireless controller while the traffic from the patrons goes directly out to the Internet.

The benefit in this configuration is that it does not require the Internet connections at the multiple locations to have static IP, only on the staff network where the wireless controller resides. This set of requirements permits the use of less expensive Internet connections at the locations. This could be an attractive option if the library is looking to keep control of the recurring costs associated with Internet access.

The routing firewalls initiate the VPN tunnel with the staff network, and the APs send management data for statistics gathering and status monitoring. Settings and policies are passed to the APs when they connect with the wireless controller.

In addition to the reduced Internet costs the wireless controller is on the staff network. This may be more desirable from a security perspective, and the IT department may prefer all of their servers on the staff network.

Scenario 2

In this scenario, all of the APs are on the same network. This may be one physical network or multiple networks connected by VPN tunnels. The variable that makes this scenario different is that the wireless controller resides on the same network as the APs.

However, there are some variables to consider. If it is one physical network, this can reduce the complexity of the configuration. If not, one location will have to act as the main location. The main location will require static IP or minimally an implementation of a dynamic DNS service. This location is where the wireless controller will also reside.

This also changes the administration of this network for the IT folks. Rather than connecting directly to the wireless controller, a connection to the server will have to be established. This can be done through a variety of methods. VPN could provide remote access to the network so that the wireless controller can be reached. Alternatively a remote desktop web service such as LogMeIn or GoToMyPC could be used to access the wireless controller. Depending on the wireless controller used and the platform it runs on, the latter may not be an option unless a host PC is set up on the wireless network.

Either method is a viable option, and there are several variables could be introduced to fit the needs of your organization. The key to success is verifying that all of the equipment implemented in the network can and will work together and have all of the functions required to operate the network as designed.

Proof of Concept Testing

Proof of concept (POC) testing is a critical step, especially if the patron wireless network is a large-scale network spanning a dozen or more locations. Prior to investing time and materials in an RFP and spending money on large quantities of hardware, it's best to put together a smaller-scale test to make sure it will do all that it should.

Many vendors have excess spare or rental equipment that can be acquired for POC testing. Take this opportunity to set up the main site and at least one remote site, if applicable. If VPN tunnels are being used, ensure that the equipment will communicate without issue over the tunnel. If stats are being gathered, run sample reports to verify that the data desired can be retrieved and in a format that is acceptable. The POC will present a unique chance to iron out implementation issues before the big day. This will avoid having to push back a go-live date due to configuration issues and will help prove the viability of the project when it is presented to decision makers and stakeholders.

Bandwidth Planning

Bandwidth planning is an important step that is often overlooked when planning a patron wireless network and can be either the cornerstone of its success or the root of its eventual failure. There are two aspects of bandwidth to consider when planning the implementation of a patron wireless network, and they are interdependent. The wireless network is capable of delivery very high-speed connections to the devices connected to it. Therefore, the connection to the Internet is usually the potential bottleneck on the network.

The first aspect to consider is the bandwidth supplied for Internet access. This decision is critical and will eventually determine the overall success of the network when it is deployed. If the network does not have enough Internet bandwidth, it will be too slow. The demand will far exceed the capacity of the Internet connection and will result in what looks similar to a denial of service (DoS) attack during peak usage periods. If patrons are denied access, they will lose patience with waiting and errors and seek other sources of Internet access.

So the key is to make sure that there is a large enough Internet connection to suit the number of patrons. ISPs now offer a wide range of high-speed connections at very affordable prices. In fact, ISPs in some markets are in bandwidth wars to offer the highest speed for the best prices. This is your greatest advantage. When implementing it may also be possible to have multiple Internet connections for bandwidth load balancing and fail-over protection. However, depending on the scale of the network, even the highest speed connections may not completely avoid a bottleneck.

The second aspect of bandwidth planning depends on whether the new wireless network implements quality of service (QoS) that allows for setting the speed of connections to devices (or nodes) on the network. QoS will allow for setting maximum bandwidth to each device in the network. This will ensure that no one user or device takes up all or most of the available Internet bandwidth.

Throughout the planning of this network, the number of devices on the network has been the focal point in determining the scale of the network. The same applies to balancing assigned bandwidth in QoS and selecting an Internet connection. It is important that the Internet connection speed is at least the as high as the peak number of devices planned for multiplied by the maximum bandwidth designated to each in the QoS settings.

It is OK if the Internet connection is close to or smaller than what has been determined to be the peak potential demand. However, if possible, consider limiting the number of devices that connect to the network simultaneously. When the network reaches its maximum allowable devices, new connections will be denied access until there is room. If this measure is taken, it is equally important that the network provide statistics on denied connections. Monitoring this information closely will allow administrators to see how often denials occur, if at all, and determine if additional Internet bandwidth is needed.

Authentication

Another consideration in planning the patron wireless network is authentication. All patron wireless networks should have some level of authentication. Additionally, authentication may not be optional. Academic libraries may need to comply with school policy and public libraries with municipal law or policy. However, authentication should not be confused with requiring credentials. The main question to ask is what credentials, if any, will be required when authenticating users.

If there are no requirements for authentication, then all options are available, including no authentication. However, an authentication process may still prove to be a wise decision. Rather than simply deploying an open network, use an authentication system to present users with an End User License Agreement (EULA) acceptance page. The EULA is a powerful tool that will help announce the network to patrons and give the library some insulation from liabilities should someone choose to engage in unsavory activity on the network or contract malware or a virus while using their device on the network. The user would have to accept the EULA before full access to the network is granted.

There is no shortage of institutions and businesses that offer free Wi-Fi access to the public. Many of them present a EULA, and it may be a good idea to visit some of these places to see their EULA to "borrow" some aspects of it for your own. A good EULA will warn the user about the fact that they are about to enter a public network; that they are responsible for providing adequate protection from viruses, malware, and other malicious software; and that the library is not responsible for damage due to viruses, malware, or other malicious software the user's device is exposed to while connected to the network. Other considerations include stating that illegal activities are prohibited and perhaps specifying not using BitTorrent or other peer-to-peer network to pirate software or media. The library may also want to state that is reserves the right to block access from devices found to be in violation of the terms of the EULA.

Below is a sample EULA to use as a model for your own. However, it is vital that the legal counsel for the library, library system, or academic institution review and approve the EULA before deploying it.

> By accepting this End-User License Agreement (EULA), you, the user, acknowledge the use of this Patron Wireless Network, a free service provided by the Anytown Public Library (APL). By accepting this EULA, you, the user, also acknowledge APL is not responsible for any damages caused by the use of this system or by any software, malware, spyware, viruses, or any other content, program, or code that may be retrieved, compiled, stored, or executed by the use of this system. By accepting this EULA, you, the user, acknowledge and accept all risks associated with use of the public Internet. There is no warranty, express or otherwise.

If it is decided to require credentials to access the network, make the credentials something that is already known or familiar to the user. Users do not like having to remember new passwords, and it will go a long way toward user acceptance of the network not to have to remember another one. This can be easily accomplished if all users already have credentials on an LDAP server. This is usually the case with academic libraries. Even some public libraries may already use an LDAP sever to host their patron accounts or have the ability to synchronize their patron database with an LDAP server.

Another option may be developing a method to query the SIP service on the ILS. Using SIP in the same way database vendors do to authenticate users, the wireless network would collect library card number and PIN credential on the authentication page and pass that to the SIP service to verify them.

If SIP is not available on the ILS, a final option may be using API (application programming interface) code. Using API, it may be possible to script verification of library card number and PIN combinations to facilitate authentication on the wireless network.