SIM2K
Adapting Technology to Your Business Needs

2•17
Information you can use

SIMformation

Wireless Networks Need Planning

Wireless networks are going through a second evolution as new protocols enhance connectivity. People now expect to be able to connect wirelessly at work, home, stores, restaurants and more. If you are a business and have clients coming in for meetings, they will want to have access to a wireless network. If you are in retail, do you offer your customers the opportunity to connect to a wi-fi network? Again, they will be expecting this perk.

So let’s say you need to install wi-fi. You have been in the stores and have seen “Wireless Routers” on the shelf. Heck, even Wal-Mart sells them. You buy one, (preferably the one that looks like a porcupine for all the antennas sticking out of it – after all, the more antennas the better, right?) then you take it to your office, plug it in and you have wi-fi. Easy peasy...

Unfortunately, this is the approach many people take, and then are disappointed in the results. Plus, this also raises issues with security of your data and unauthorized access to your network, as well as allocating traffic on your network given new devices connecting now that there is wi-fi available.

SIM2K has worked with many clients in setting up a secure, robust wi-fi network now, and we understand that there is a considerable amount of pre-planning that must take place before installing a wi-fi network. We would hope that any SIM2K client would involve our Network Engineers before just putting a wireless router in the office and then calling to say “it doesn’t work right.”

First of all, wireless networks aren’t magic, they’re radio. Just as your car radio signal drops because of distance or obstacles like buildings, mountains, and tunnels, your wireless network signal has limitations. In fact, a wi-fi signal is much less robust than a radio station because of the frequency used. While a mountain will block a radio station, a file cabinet might block your network connection.

The most common wireless network types are “two wall” technologies. This means the signal can only go through two normal walls before it becomes too degraded. Extra thick walls, or plaster walls with a steel mesh inside will degrade or stop the signal more quickly. Floors and ceilings count, too, so this becomes a three dimensional exercise when deciding to place wireless access points (WAPs).

Good coverage is the goal for the planning process. Placing access points intelligently will support the most users with the fewest number of access points. This is one time “the more the better” is not the case, as too many WAPs leads to overlapping coverage and dropped connections as the network tries to locate connected devices in the office.

Completing a site survey first speeds deployment and reduces the number of access points by locating them correctly. Proper placement of access points goes a long way toward user satisfaction, so plan ahead a bit to ensure happier users.

Then, adding wireless to your network requires more than just a couple of access points plugged into your existing router. In fact, wireless access points are one of the major reasons companies invest in switches with PoE (Power Over Ethernet). Placing access points on the ceiling is much faster and less expensive when you don’t need to run electrical power through conduits to each location.

When planning for user capacity, take into consideration more than just laptops and some wireless-enabled desktops. Will iPhone users start surfing via their Wi-Fi interface? iPad users certainly will. Your network hardware, software, and management processes will change more when you add wireless networking than you expect. Use the addition or expansion of a WLAN to examine and update your existing infrastructure. Bolting a new, high speed wireless network to an outdated and overworked router will only lead to complaints.

Then you need to consider security. Wired networks have one great edge: hackers have to be inside your building to connect to your network. Wireless networks, especially when configured incorrectly, broadcast to the world. Proper placement of WAPs can cut down on the “spill over” of a signal outside your office space. And, security must be taken up a couple of notches when you add wireless. Good security demands WPA2 (WiFi Protected Access) for authentication. This supersedes the earlier WEP (Wired Equivalency Protocol) that wasn’t, unfortunately, as robust as the industry hoped. In fact, if your company handles customer credit card information, the PCI (Payment Card Industry) audits demand you use WPA2 for wireless security, or you fail the audit. Also, those Wal-Mart wi-fi routers all use the same user ID and password, so there is a real hole in your security if you don’t know to change this default setting.

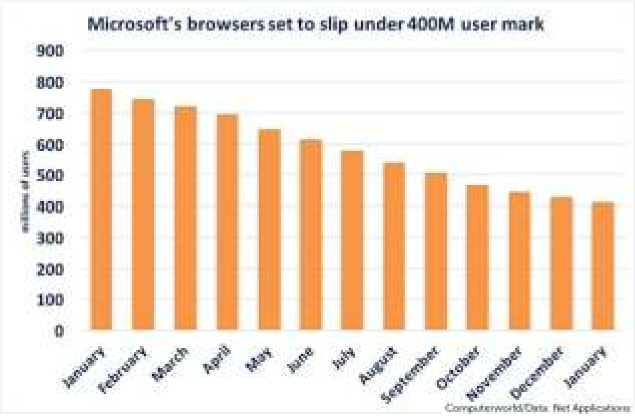
Another factor to consider is managing your wireless network. While a very small office can get by managing wireless clients manually, larger offices should consider automated tools such as a WLAN controller. These tools use less intelligent wireless access points but manage, configure, and secure them more completely than so called “fat” access points do. In addition, they provide a single management interface for all wireless access points and users. A WLAN controller is highly recommended as a management upgrade that saves time and increases security.

There is much more than this to consider when adding Wi-Fi, so that is why we encourage you to call us first when installing or adding to an existing wireless network.

Microsoft Browsers Fading

Microsoft's browsers last month again lost significant usage share to end January with just over 25%, a milepost that would have been rejected as absurdly low only a year and a half ago.

According to data published Wednesday by analytics vendor Net Applications, the user share of IE and Edge – an estimate of the proportion of the world's personal computer owners who ran those browsers – fell by a percentage point last month to a combined 25.2%. The one-point decline of IE + Edge was substantially larger than the drop of December, when experts interpreted that month's 0.7% reduction as a sign that Microsoft's browsers might be nearing the end of their slide. Instead, January's jump refuted that idea.



Computerworld/Data: Net Applications

By Net Applications' measurements, IE has already dropped under the 20% mark – for January, the former kingpin accounted for 19.7% – and the gains by Edge, which added just 0.15 % to its share in the month, have not been nearly enough to cover IE's decay. For January, Edge accounted for 5.5% of all browsers.

Projections of the IE + Edge combination hint at an increasingly ugly future. IE and Edge could fall under 20% as soon as April, and likely no later than June, according to the 12- and three-month trends in the Net Applications data. January's biggest beneficiary was again Chrome, which added another 1.4% to its user share, reaching a record 57.9%. The forecast -- again using Net Applications' data trends – puts Chrome over the 60% bar by the end of April at the latest.

Mozilla's Firefox, which in the last third of 2016 recovered much of the share it lost earlier in the year, returned to its slump, losing half a percentage point and dropping to 11.8%.

Although Microsoft has tried to promote Edge, touting changes and feature additions to the browser due in the upcoming Windows 10 update, the effort has not paid off. Last month, just 22% of all Windows 10 users (down from 26% last year) ran Edge as their primary browser.

Li-Fi is... "En-Lightening"

Just when you thought that Wi-Fi was the answer, researchers have gone one better - Li-Fi. This technology harnesses light waves from LED lamps an overhead lights to stream data and connect users to the Internet.

The Li-Fi technology uses a much more abundant slice of the wireless spectrum, and is more energy-efficient that Wi-Fi. Light waves can't pass through walls like radio waves, so while that may create issues with office connectivity, it also increases security as signals can't pass outside office walls.

The technology works by embedding Li-Fi in LED lamps, modulating the light's intensity faster than the human eye can detect. This transmits the data stream to a special USB drive that serves as a receiver/transmitter to pick up the signals from the LED lamps.

There are several companies working on this technology. One claims that it is reaching speeds up to 43 megabits per second (Mbps), compared to average US broadband speeds of 16 Mbps). A second company believes they can reach speeds of up to 100 Mbps with advances in coding and modulation.

As for other applications of this technology beyond the office, the developers are considering this for use in airplanes, for in-air connections for both the cabin and cockpit, as well as ways to incorporate this technology for outdoor use. And, Li-Fi is not limited to overhead lighting, as a Li-Fi desk lamp is in the works, so this connection can be isolated down to individual users rather than be all-office encompassing.

The technology was first introduced in 2011 in a TED talk, and is moving forward quickly. IEEE, the technical association that oversees standards in this field, is working on the Li-Fi protocol and hopes to have it in place by the end of the year so that this technology can move out of the lab into full commercialization. Now we'll just wait to see if anyone actually has the light go on over their heads .... ok, bad pun.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Android Apps on Chromebooks

The line between Google Chrome and Android operating systems is becoming less distinct. This is great news for Chromebook users, and as Google rolls out the ability for more Chromebooks to use Android apps, the future is looking bright for these inexpensive notebooks. This will go a long way toward minimizing criticism that Chromebooks are just low-power laptops running a web browser. Chromebooks have become an inexpensive web portal that allows users to perform many daily tasks that don't require powerful and expensive hardware, and things are just going to get better now that Android application support is a reality.

Chromebooks access to Android apps is not yet universal, although that is changing, as all new Chromebooks that are released in 2017 will include Android app support.
If you have an older Chromebook, hope is not lost. While not all older Chromebooks will support this feature, a number of existing and legacy models will also feature Android app support. It requires that Chome OS version 53 or later be installed on your machine, but with the rapid updates to the OS that are a hallmark of these little laptops, that shouldn't be an issue for most users. If your Chromebook currently supports Android apps, all you need to do is go to Google Play while on your Chromebook, click on the settings icon in the upper-right and enable the Google Play Store on your Chromebook. After that, just follow the instructions to get started installing apps.

There are still some hardware limitations that prevent some Android apps from working on Chromebooks. Not all include GPS and accelerometers, for example. If an app requires those sensors, obviously that's a problem. If the developer specifically required touchscreen use when they created the app, that is also an issue, and the app will not work properly.

Some Android apps will need to be modified to run on a Chromebook, such as accounting for keyboards, trackpads and mouse use. Also, the app must consider the lack of on-board storage in most Chromebooks and look to Cloud-based backups in stead. There are also issues with screen size compatibility and the use of multi-window display on Chromebooks. While unmodified Android apps may run on a Chromebook, they may not always run well if they haven't been optimized.

The lack of a touchscreen is the most obvious difference between an Android phone or tablet and a Chromebook, but it is not as big of a problem as one might initially think. Google has thought of this and Chromebooks that will run Android apps support the "faketouch" feature that allows the touchpad or mouse to take the place of the touchscreen. How well this works may vary from app to app, but it shouldn't be too much of an issue for most apps.

Running Android apps on Chromebooks should add to the appeal for people in the market for an inexpensive laptop, and should make ownership more pleasant for existing owners. If enough developers put in the effort to optimize their Android apps to run well on Chromebooks, this could be a game changer and dramatically increase the flexibility of these laptops. It could also expand the target audience for new Android apps and lead to unexpected innovations as cross-platform app support becomes the new normal.

"Random Tid-Bytes"

Do You have a Yahoo! Account?

Google has announced that Gmail will stop supporting older versions of the Chrome browser soon, a move that will affect anyone still running Windows XP or Vista. Users of Chrome version 53 and older editions of the browser could start being redirected to the basic HTML version of Gmail. Starting this month, users who will be affected by the change will see a banner at the top of Gmail telling them to upgrade to an up-to-date version of Google's browser. The affected browser versions include Chrome v49, the last version of the software that supports XP and Vista. While Microsoft officially ended support for XP more than two and a half years ago, Gmail has continued to work with it. Vista Service Pack 2 will reach the end of it's extended support period on April 11 of this year.

Indy Gets "Bleeding Edge" service from AT&T

AT&T will launch its first 5G wireless service in Indianapolis and Austin, TX later this year, offering theoretical top speeds of 400Mbps or higher. Current 4G LTE networks used by customers may be far less, often no higher than 30Mbps on downloads, from the nation's major wireless carriers, according to various field tests by independent testing companies. Massive bandwidth and low latency from 5G will help self-driving cars and mobile augmented reality and virtual reality headsets, AT&T said. New technologies atop the 5G network and greater density of wireless transmitters could bring the theoretical test speeds even higher – to 1Gbps in 2017, AT&T said. The 5G rollout in Austin and Indianapolis will occur "in coming months," AT&T said. The company also said it will build two new 5G testing labs this spring in Austin. The testbeds will be used to support a fixed wireless 5G connection to stream DirecTV Now for residential and small and medium business customers.

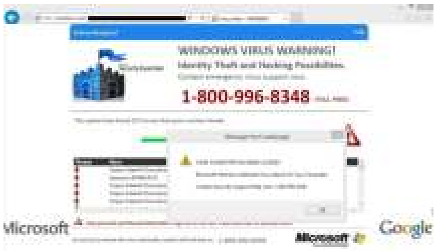
4K TV Broadcasting Closer

The Federal Communications Commission has taken the first step toward the eventual rollout of over-the-air terrestrial 4K television broadcasting in the U.S. The proposed regulations would allow TV stations to begin broadcasting using the ATSC3.0 format, the newer version of the digital transmission format used today. ATSC 3.0 uses an IP data stream, so it is much more flexible than current broadcast standards. Using the system, broadcasts can simultaneously send several video streams of varying bandwidths and additional streams of data.
Proponents of the technology say this would enable 4K broadcasting and is a way to rapidly disseminate public safety information, but whether such services will be offered is up to individual broadcasters. As proposed, the regulation will allow the voluntary use of ATSC3.0. To receive the new format, upgrades will be required to televisions and reception equipment, so the FCC proposes allowing TV stations to continue broadcasting in the current version 1 format. Cable TV companies won't be required to carry ATSC3.0 signals, and broadcasters will still need to abide by public interest obligations.

Scareware, E-Mail Scams and Misdirection Domains

Several SIM2K clients have reported being hit with an incessant series of pop up messages on computer screens that warned they had a virus on their computer. They presumed that the warnings were legitimate, but in fact, this is the latest attack now dubbed "scareware." The term scareware describes software products that often generates a bombardment of pop up warning messages that makes using your computer difficult.

The FBI has investigated these pop up messages claiming that you have a virus and you are in need of anti-virus software which may, ironically, actually contain a virus that could harm your computer, cause costly repairs or, even worse, lead to identity theft. The FBI states that those pop up messages contain scareware, fake or rogue anti-virus software that looks authentic, but they are not.



WINDOWS VIRUS WARNING!
Identity Theft and Hacking Possibilities.
1-800-996-8348

Scareware is sold to unsuspecting computer users who fear viruses on their computers. The scareware is either useless or contains damaging malware programs. The cyber criminals convince users that he or she has a virus that has infected their computer and then offers anti-virus software to remove it. The virus does not in fact exist until the user downloads the scareware progam "recommended" when the user calls the number on the pop-up and the "technician" delivers the malware either by e-mailing a file to install or by the user allowing the scammer to access their computer.

The message may display what appears to be a real-time, anti-virus scan of your hard drive. The scareware will show a list of reputable software icons; however, you can't click a link to go to the real site to review or see recommendations. Once the pop-up warning appears, it can't easily be deleted by clicking on the "close" or "X" buttons. If you click the pop-up to purchase the software, a form to collect payment information for the bogus product launches. In some instances, the scareware installs malicious code onto your computer, whether you click the warning or not. This is more likely to happen if your computer has an account that has rights to install software.

The Federal Trade Commission (FTC) notes that the scareware scam has many variations, but there are some telltale signs. For example:

- You may get ads that promise to "delete viruses or spyware," "protect privacy," "improve computer function," "remove harmful files," or "clean your registry;"
- you may get "alerts" about "malicious software" or "illegal pornography on your computer;"
- you may be invited to download free software for a security scan or to improve your system;
- you could get pop-ups that claim your security software is out-of-date and your computer is in immediate danger;
- you may suddenly encounter an unfamiliar website that claims to have performed a security scan and prompts you to download new software.

The FTC reports that scareware schemes can be quite sophisticated. The cyber criminals purchase ad space on trusted, popular websites. Although the ads look legitimate and harmless to the website's operator, they actually redirect unsuspecting visitors to a fraudulent website that performs a bogus security scan. The site then causes a barrage of urgent pop-up messages that pressure users into downloading worthless software.

If you're faced with any of the warning signs of a scareware scam or suspect a problem, shut down your browser. Don't click "No" or "Cancel," or even the "X" at the top right corner of the screen. Some scareware is designed so that any of those buttons can activate the program. **If you use Windows, press Ctrl + Alt + Delete to open your Task Manager, and click "End Task."** Lastly, make it a practice not to click on any links within pop-ups.

Some of our clients hit with scareware pop-ups have called in, as they were afraid they had triggered a Ransomware attack. Fortunately, the malware behind scareware is not as dangerous as Ransomware, as it will not encrypt your data and force you to pay to unlock the encryption. But if you have any questions about an odd screen you see, please stop and call us. Better safe than sorry.

Another sneaky attack that has plagued some of our clients is the use of a misdirection domain name. Here the scammer purchases a domain name similar to a legitimate company's domain, but makes a slight variation. For example, rather than "abccorporation. com" the scammer registers "abccorporatlon .com" substituting an L for the I in the name.

Then, the scammer uses LinkedIn or other on-line business directories to find the name of the company president and some other employee. The scammer uses this altered domain to send the employee an e-mail that purports to be from the company president wherein the employee is asked to initiate a wire money transfer , or send personal information on employees that can be used for identity theft, or other confidential information.

If you follow the Indianapolis news, the Scotty's Brewhouse restaurant chain, Monarch Beverages and American Senior Communities were all targeted by one of these attacks and someone in these companies sent the scammer W-2 tax forms on all employees. These employees thought they were replying to a request from the company president. In an actual SIM2K incident, one of our clients was asked to wire money – but fortunately they had been forewarned about the similar-appearing domain being registered, and also, when the e-mail came in, the scammer used the president's full name whereas within the company he uses a nickname for all business, another tip-off that this was not a legitimate request.

So be very cautious about any e-mail request you might receive asking for something not in the common day-to-day business activities. Always look carefully at the sender's e-mail address to verify if it is legitimate, and if anything smells funny, always call and verify the request before taking any action.