Wi-Fi Range Extension: Network

John R. Joyce, Ph.D.

Continuing our exploration of Wi-Fi networks, there may well be times where addressing the connectivity of an individual machine just won't cut it, and you are looking to improve the overall status of your wireless network and expand its coverage.

Depending on the coverage problems you've been encountering, the least costly step might be to replace the antenna(s) on the wireless router you are currently using. Many of the mass-market wireless routers available incorporate very basic antennas in their design. It would not be at all surprising to find that, for marginal coverage situations, simply replacing the antennas with more efficient ones would resolve your network issue. You can purchase replacement antennas from a variety of sources, just compare the specs beforehand to make sure that you are trading up, instead of trading down. Remember to make sure that you look at not only the numbers, but the units as well. Most manufacturers spec the gain of their antennas in dBi,[1] but this is not always the case. Before ordering, also be very careful to confirm the connectors used. Many times, the same basic antenna can be ordered with a variety of connector types. The frustration of getting in a new piece of equipment only to discover that you can't use it because the connectors won't mate is truly one of the delights of system upgrading!

Another common way of upgrading your network coverage is by the use of what are commonly called range extenders. It is more descriptive to call these repeaters,[2] as what they do is receive the weak Wi-Fi signal and the rebroadcast the amplified signal. Configurations vary, but they'll generally have at least one antenna to receive the signal from your wireless router and another to rebroadcast it. Some systems may contain active antenna arrays to actually focus the retransmitted signal toward the client computers to use the radiated energy most effectively. In most situations, the same channel and network SSID is used, though this can slow the overall throughput, as both units can not be transmitting at the same time.

It is possible to incorporate more than one range extender into a system, whether employing them in a star configuration, with the wireless router in the center of the network or as a daisy-chain,[3] with one repeater feeding another. However, while it is possible to do this, as a general rule, it is not recommended, since each additional repeater will halve your available bandwidth, simply because it can't transmit while it's receiving. Now, this does not necessarily mean that your network throughput is going to be halved with each repeater, but it will be reduced, so carefully configure your network topology, just don't throw everything together to see if it works!

The Belkin Dual Band Wireless Range Extender[4] (Model FDK1106v1, $79.00) is an excellent example of this type of device. This unit is also an example of the trend toward fixed internal antennas. It is powered by an included external 100-120VAC/12VDC 1A power converter, allowing flexibility in unit positioning. It features support for Wi-Fi Protected Setup[5] (WPS) for the WPA/WPA2 security protocols, as well as configuration through a Web interface. I found that, in many respects, the manual setup is almost simpler than the WPS setup. It may actually be simpler if you run into some of the issues encountered using equipment from different manufacturers, particularly if any of the equipment was sold as ‘pre-N’, before the 802.11n standard was finalized. When configured via the Web interface, the recommended approach is to use an Ethernet connection for the link. I suspect that this was a design decision to simplify the steps someone needed to go through to configure the unit, as most users would be unlikely to have a technical computer background.

NOTE: To clarify, Wi-Fi Protected Setup (WPS) only works with the WPA[6] and WPA2[7] security protocols. If used, the WEP[8] security protocol must be manually configured. As this is a weaker protocol, the general recommendation is not to use it unless external conditions mandate it, e.g. some of the network devices do not support the stronger protocols.

All versions of the 802.11 standard, a, b, g and n, are supported. As its name indicates, the F9K1111 is a dual band extender, supporting both the 2.4 GHz and 5 GHz frequency bands. Depending on the standard used, this can result in physical link rates of 11 Mbps up to 300 Mbps. While not explicitly stated in the manual on the accompanying CD, the fact that it does state that these bands are simultaneously supported would indicated that this unit does contain two radio circuits and at least two internal antennas.

NOTE: Mbps refers to Mega Bits Per Second, while MBps refers to Mega Bytes Per Second. Additionally, keep in mind that stated speed specifications generally refer to the maximum link layer speed. The actual data transfer speed will always be less than the link layer speed due to protocol overhead and other factors.

A strong plus for this device is that it also can function as a network bridge, providing four ports for the connection of hardwired Ethernet devices. To take advantage of these ports, you just need to insert an Ethernet cable between the port on the F9K1106 and the device you want to connect. The IP address for the device can be manually set or can be assigned by the DHCP server in your wireless router, just be careful to not assign duplicate addresses.

According to the included documentation, the WN2500RP is also a dual band extender, supporting both the 2.4 GHz and 5 GHz frequency bands. All versions of the 802.11 standard, a, b, g and n, are supported. As with the Belken unit, this can result in physical link rates of 11 Megabits per second (Mbps) up to 300 Mbps depending on the standard used.The Netgear WN2500RP Range Extender[9] ($79.99) is another example of this type of device. It is powered by an included external

100-120VAC/12VDC 1A power converter, allowing flexibility in unit positioning. It too features support for Wi-Fi Protected Setup (WPS) for the WPA/WPA2 security protocols, as well as configuration through a Web interface. When configuring the unit manually, you can configure it using a Wi-Fi connection or the included Ethernet cable. The included installation guide includes a very detailed walk-through of all the configuration modes. I don't think anyone would have any difficulty finding a procedure with which they are comfortable, whether they have a computer background or not. By default, this system assigns the extended Wi-Fi network an SSID consisting of the SSID of the parent network with the string '_2GEXT' appended. While both the Belkin and Netgear units include a variety of status indicators, the Netgear unit provides more extensive information regarding the current condition of the system. Whether this information will be useful to most users, I don't know.

Again, a strong plus for this device is that it also can function as a network bridge, providing four ports for the connection of hardwired Ethernet devices. To take advantage of these ports, you just need to insert an Ethernet cable between the port on the WN2500RP and the device you want to connect. The IP address for the device can be manually set or can be assigned by the DHCP server in your wireless router, just be careful to not assign duplicate addresses. Devices attached to the Ethernet ports do not result in a bandwidth speed degradation, as the WN2500RP acts as a switch and does not rebroadcast packets directed to devices on the hardware ports.

An interesting feature of this unit is what Netgear calls 'Fastlane Technology.' This approach takes advantage of the WN2500RP being a dual band modem, but reconfigures it so that the two bands are used for different purposes. Basically, it dedicates one band to communicating with the wireless router and the other to communicating with the attached devices. It allows you to configure which band is used for each link. This effectively eliminates much of the bandwidth loss normally encountered with a range extender, but does limit the defined protocol modes available.

The Linksys RE1000 Wireless-N Range Extender/Bridge[10] ($89.99) is an alternate example of this type of product. The RE1000 comes with an internal AC/DC power supply accepting 100-240 VAC, 50/60 Hz, at 0.5A that, by default, is configured to plug directly into a wall outlet. However, it includes the required components to reconfigure it, without tools, to sit on a desktop.

The unit contains two internal non-removable antennas having a gain of 3.5dBi.

Configuration of the unit is very straight-forward. While the RE1000 does support Wi-Fi Protected Setup (WPS), for use with those routers that support it, it is almost as easy to set up via a browser connection, either wirelessly or through an Ethernet link. A CD with a setup utility also is included with the unit, which after connecting wirelessly to the extender, prompts you to select the network to which you wish to connect and the appropriate security keys for it, for those more comfortable with that approach.

This unit supports the 802.11 b/g/n wireless standards and both the Wi-Fi Protected Access2 (WPA2) and WEP security protocols. While it does not support the 802.11a standard that the other two units we've examined did, I doubt that would affect most people, as this standard is seldom used in comparison with b/g/n, particularly in home installations. By default, the RE1000 uses the same SSID as the original network. Its maximum specified range is 300 meters, though the practical range will be less.

Once you have completed the configuration of this unit, the Ethernet port functions as a bridge port, allowing you to plug a hardwired piece of equipment into it and have it connect to the wireless router. The IP address of the attached equipment can be manually assigned locally or automatically by the DHCP server on the router. Cisco Technical Support indicates that you can multiply this bridge port by attaching an Ethernet switch. Their caveat was that everything be connected so that only the router/access port (AP) that was connected to the Internet be configured to assign IP addresses, other than those that were manually set. They also indicated that running more than five to eight devices through the range extender would cause a noticeable degradation in the user experience.

Now, a few general caveats regarding wireless extenders. If you are employing MAC filtering in your network, you must load both the devices physical MAC address, usually found printed someplace on the device, and the translated MAC address reported by the wireless extended into your wireless routers filter table. To determine what the translated address is, the easiest way is to just turn off filtering and check your router to see what address is being reported. The translated address needs to be added for each device that might connect through the extended network. After adding the translated address to your filter table, you can then reactivate your MAC filtering.

Keep in mind that, even if you assign the same SSID and security key to both the

wireless router and your wireless extender, movement between them is not transparent. While you can configure your client to auto-connect to whichever access point has the strongest signal, there still will be a glitch when the system disconnects and reconnects. This is a result of there not being a standard protocol to manage the hand-off of the network connection. If you are working from a set point in your network coverage, this shouldn't be an issue, but if you are actively trying to use your network while randomly strolling through it, you are likely to experience network glitches and possible data corruption. This problem is not due to the failure of a particular manufacturer's equipment, but rather to no effective standard existing for roaming connections. At one point, the Trial Use Recommended Practice IEEE 802.11F[11] existed, but was withdrawn due to the long hand-off delay. The requirements of a roaming protocol have been complicated by more stringent security requirements, at least some of which have been addressed in the proposed 802.11r-2008[12] amendment to the standard.

NOTE: On January 6, 2012, the United States Computer Emergency Readiness Team (US-CERT) issued Alert (TA12-006A)[13] stating that a flaw had been discovered in the Wi-Fi Protected Setup mechanism making it vulnerable to a brute force attach. Their recommendation was to disable this feature on your wireless router until this vulnerability had been addressed. They also made a point that testing showed that even though a product's Web interface indicated that the WPS functionality was disabled, not all systems actually disabled it. As the WPS security synchronization process is an industry standard, this alert should not be taken as an indication of a failure on the part of a particular vendor. While some vendors may have already updated their systems, this does not remove the vulnerability from existing hardware. To correct existing systems, you must acquire the corrected code from the vendor and then update the firmware on your systems.

As the US-CERT estimate is that it would still take four to 10 hours to recover the WPS PIN, the average user is probably not at a lot of risk, as those holding high value/confidential information are more likely to be targeted. Even if the underlying WPS vulnerability has not yet been corrected, as long as you can indeed disable the functionality, it should be reasonably safe to use the WPS functionality to configure a system, as long as you disabled the feature immediately after. Personally, as with a lot of systems that are designed to be 'consumer friendly,' I generally found it easier to just connect to the device and manually configure it than to try and use WPS. I suspect that this is particularly true if you are working with a network composed of devices from different vendors.

While not being a literal Wi-Fi extender, the Linksys PLSK400 Powerline AV 4-Port Network Adapter Kit[14] ($149.99) may be the solution you are looking for to resolve our home network connectivity problems. By superimposing your network traffic over your existing home power lines, it allows you to extend your network to a Wi-Fi dead-zone without stringing any Ethernet cables.

If you are doing a base install, nothing could be simpler, you plug the PLE400 in near your wireless router and the PLS400 near your devices to be networked. Connect an Ethernet cable between one of the routers LAN ports and the Ethernet port on the PLE400 and between the Ethernet ports on the PLS400 and the remote

equipment to be networked and you are set to go. You can set the IP addresses of the remote equipment manually or have it automatically assigned by the DHCP server on your router. While some people have reported issues with powerline network equipment, I have encountered no problems during our testing. In fact, in our test scenario, these units have proven to be much more reliable than the Wi-Fi configuration they replaced.

Communication between the two units is encrypted, so the fact that other houses may be running on the same transformer circuit shouldn't be a major concern. If you need to expand the network into other areas, you can add additional modules to the system. The security codes that the boxes use can be set without external software using buttons on the boxes or via a software utility that can be downloaded from the Cisco Web site. While admittedly the powerline connection restricts mobility more than a Wi-Fi connection would, for connections to a docking station or relatively static device like a printer, I wouldn't consider that to be a major issue. Of course for the security conscious, the fact that you're not broadcasting over the radio waves might actually be a plus. There obviously still would be ways to tap the signal if someone really wanted to put the effort into it, but it would add another layer to the effort required.

The PLSK400 is stated to be compatible with other HomePlug[15,16] network devices. However, if you are looking to integrate this system into a network containing devices from other vendors, I suggest you carefully check the specs first or contact the appropriate vendor technical support, as HomePlug incorporates a number of standards and not all of these are compatible.

It also would be wise for you to check the version of the firmware currently running on your Wi-Fi devices and cross check that with the versions available for download from the manufacturers Web site. It is not uncommon to discover that your observed network issues can be resolved by updating the firmware being used.

Hopefully, one of the above approaches to extending your network coverage will resolve the issues you've been encountering. Having said that, I do realize that, with everyone pushing the envelope in different directions that exceptions — I'm sorry, special cases — exist where these won't solve your problems. We haven't even touched on approaches, such as setting up wireless bridges, other than superficially addressing the bridges built into some of the featured units. For example, another option would be to use the Linksys PLSK400 kit as a bridge and attach a Wi-Fi access point at the far end. This would allow you to provide Wi-Fi coverage in two locations without having to provide coverage in-between and without the bandwidth loss that a repeater entails. I suspect that, if you were having to add several access points for full coverage, you would end up with higher overall network speed than you would get by installing multiple range expanders, it would take just a little more effort to set up. But, we can discuss designing a network bridge system in another column.

We'd love to hear about the networking problems you've encountered and the approaches you used to solve them. If there is enough interest in a topic, it might even become another column.

References

1. Young, M. F. Understanding Decibels and Their Use in Radio Systems. http://wireless.fcc.gov/outreach/2004broadbandforum/comments/YDI_understandingdb.pdf [1]
2. Geier, J. Extending WLAN Range with Repeaters. Wi-Fi Planet (2004). http://www.wi-fiplanet.com/tutorials/article.php/1571601/Extending-WLAN-Range-with-Repeaters.htm [2]
3. RE1000 - can it be 'daisychained'? - Cisco Home Community. Cisco Home Community (2012). http://homecommunity.cisco.com/t5/Range-Expanders/RE1000-can-it-be-daisychained/m-p/504292#M5000 [3]
4. Belkin Dual-Band Wireless Range Extender F9K1106. (2012). http://www.belkin.com/IWCatProductPage.process?Product_Id=577752 [4]
5. Wi-Fi Protected Setup - Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup [5]
6. Wi-Fi Protected Access (WPA) - Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access [6]
7. IEEE 802.11i-2004 (WPA2) - Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/WPA2 [7]
8. Wired Equivalent Privacy (WEP)- Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy [8]
9. Netgear WN2500RP. http://www.netgear.com/WN2500RP [9]#
10. Cisco Linksys RE1000 Wi-Fi Range Extender. http://homestore.cisco.com/en-us/adapters/linksys-RE1000-range-extender-bridge_stcVVproductId136607179VVcatId543809VVviewprod.htm [10]
11. Inter-Access Point Protocol - Wikipedia. Wikipedia, the free encyclopedia (2011). http://en.wikipedia.org/wiki/Inter-Access_Point_Protocol [11]
12. IEEE 802.11r-2008 - Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/IEEE_802.11r [12]
13. US-CERT Alert TA12-006A - Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack. US-CERT (2012). http://www.us-cert.gov/cas/techalerts/TA12-006A.html [13]
14. Cisco Linksys PLSK400 Powerline HomePlug Kit. http://homestore.cisco.com/en-us/powerline/cisco-linksys-powerline-PLSK400-homeplug-adatper-kit_stcVVproductId142797759VVviewprod.htm [14]
15. IOGEAR HomePlug Powerline Network Guide. (2010). http://www.iogear.com/guide/homeplug_guide.pdf [15]
16. HomePlug - Wikipedia. Wikipedia, the free encyclopedia (2012). http://en.wikipedia.org/wiki/HomePlug [16]

John Joyce is a laboratory informatics specialist based in Richmond, VA. He may be reached at editor@ScientificComputing.com [17]

Links:
[1] http://wireless.fcc.gov/outreach/2004broadbandforum/comments/YDI_understandingdb.pdf
[2] http://www.wi-fiplanet.com/tutorials/article.php/1571601/Extending-WLAN-Range-with-Repeaters.htm
[3] http://homecommunity.cisco.com/t5/Range-Expanders/RE1000-can-it-be-daisychained/m-p/504292#M5000

[4] http://www.belkin.com/IWCatProductPage.process?Product_Id=577752
[5] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
[6] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
[7] http://en.wikipedia.org/wiki/WPA2
[8] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
[9] http://www.netgear.com/WN2500RP
[10] http://homestore.cisco.com/en-us/adapters/linksys-RE1000-range-extender-bridge_stcVVproductId136607179VVcatId543809VVviewprod.htm
[11] http://en.wikipedia.org/wiki/Inter-Access_Point_Protocol
[12] http://en.wikipedia.org/wiki/IEEE_802.11r
[13] http://www.us-cert.gov/cas/techalerts/TA12-006A.html
[14] http://homestore.cisco.com/en-us/powerline/cisco-linksys-powerline-PLSK400-homeplug-adatper-kit_stcVVproductId142797759VVviewprod.htm
[15] http://www.iogear.com/guide/homeplug_guide.pdf
[16] http://en.wikipedia.org/wiki/HomePlug
[17] mailto:editor@ScientificComputing.com