Interference and Metro-Scale Wi-Fi Mesh Networks

A Farpoint Group Technical Note

Document FPG 2006-373.3
January 2008

Farpoint Group has been performing detailed studies of the effects of interference on Wi-Fi-based wireless LANs (WLANs) for much of the past year. Our focus has been on exploring the nature of interference from a variety of angles, and a variety of traffic types, including general traffic, streaming video over Wi-Fi, and voice over IP over Wi-Fi (VoFi). Overall, we have observed that interference from common radio-based devices, including microwave ovens, cordless phones, and even other wireless LANs, can have a significant and indeed devastating impact on WLAN traffic of all types. We have also explored techniques for evaluating interference in production environments, most importantly the new class of spectrum assurance (SA) tools that bring the power of expensive spectrum analyzers to cost-effective and WLAN-oriented products. We have found that with reasonable precautions and monitoring, coupled with appropriate corrective action, a radio environment where the impact of interference is minimized and WLAN performance is optimized is indeed possible.

But there is one key application area for WLANs that remains to be explored with respect to the impact of interference, and that is metro-scale Wi-Fi mesh networks. The deployment of WLANs in public spaces completes the triumvirate of WLAN deployment scenarios, along with residential and enterprise. Public-access WLAN deployments originally began as “hot spots”, often with a single access point alone, thus provisioning service in a very limited geography. This model was gradually extended to “hot zones”, providing broader coverage through the use of multiple access points. And this approach is now being further extended to cover very large geographic areas, including urban centers, entire cities, and even suburbs as well. In short, a new era of *metro-scale Wi-Fi* enables an exciting option for mobile broadband access, for both voice and data (and perhaps video as well), for both consumers and business users on a global basis. And, as we will see below, metro-scale WLANs will, we believe, have a direct impact on the residential network market as well, challenging other broadband access technologies, and becoming pervasive over the next decade.

Since we anticipate that metro-scale Wi-Fi will become so common and even ubiquitous, two key questions consequently arise with respect to radio interference. The first of these is quite obvious: will residential and enterprise Wi-Fi systems potentially degrade metro-scale Wi-Fi network performance? And a far more interesting question is whether the reverse will also occur - will metro-scale Wi-Fi networks cause interference to otherwise unrelated Wi-Fi systems located nearby?

While we have tested the impact of mutual interference between two Wi-Fi systems, we have not empirically evaluated the effects of interference on metro-scale Wi-Fi network. As is the case with *benchmarking* metro-scale Wi-Fi networks, it’s simply too expensive today to perform meaningful real-world experiments. The purpose of this document, then, is to explore the possibility and impacts of both forms of interference that we noted above, and to discuss possible approaches to mitigation should either or both of these situations arise. As the reader might have surmised by now, we believe that both forms of interference will in fact occur, and that enterprise Wi-Fi networks will need to respond to this challenge.

Metro-Scale Wi-Fi Network Architecture

There are a number of architectural approaches to deploying a metro-scale Wi-Fi network. In principle, the problem differs from an enterprise deployment only in scale – all of the key features and requirements apply, including multiple classes of service, high throughput, security, and manageability. And we could, in fact, use equipment that is very similar to that employed in enterprise installation in metro-scale applications - just put an AP in a weather-proof housing, and off we go.

Except that such an approach, still used in smaller-scale hot-spot/hot-zone deployments, would be prohibitively expensive when attempted on a large scale. The reason for this is the cost of *backhaul*. All outdoor APs require a weatherproof housing, a place for mounting compliant with local regulations (building codes, safety requirements, etc.), and a connection to the rest of the network. This interconnect is called backhaul, and is usually implemented with wire in the case of typical wireless LANs (although limited wireless interconnect between APs is occasionally provisioned; this is known as a *Wireless Distribution System*, or *WDS*, and is part of the IEEE 802.11 standard). Wired backhaul, however, would be prohibitively expensive in metro-scale deployments, with enormous up-front costs. We could also use licensed wireless backhaul, such as Wi-MAX, but, again, the costs here can be significant, and the throughput too limited.

As a consequence, backhaul in metro-scale wireless LANs is most commonly implemented wirelessly, using a wireless *mesh* approach (see Figure 1). Meshes can be thought of as analogous to the Internet, in that packets in the Internet can be routed through a variety of paths between

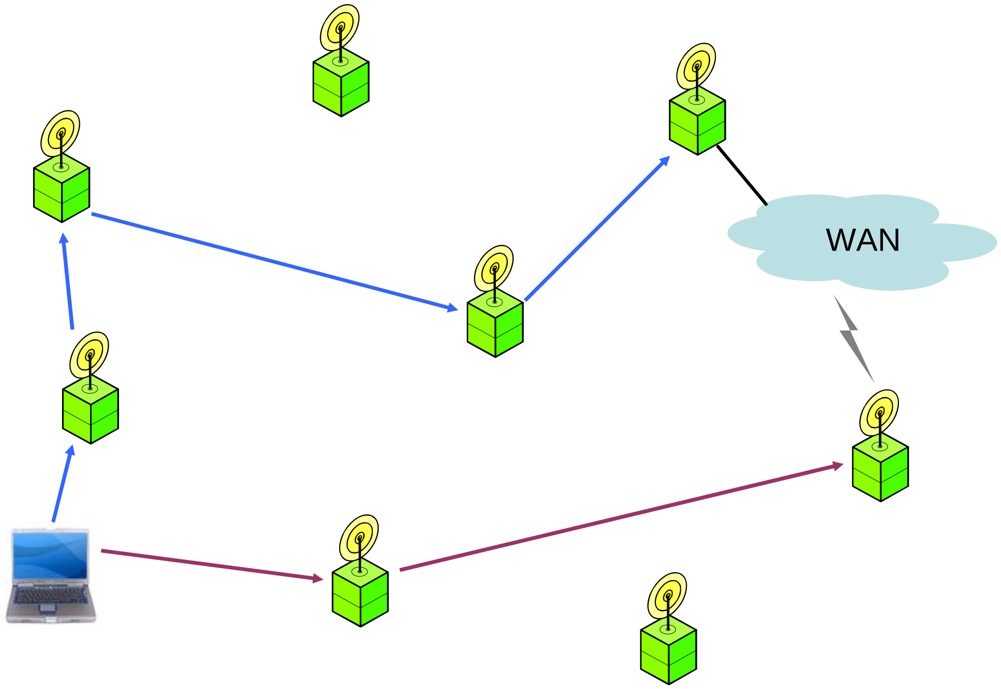

Figure 1 - A key characteristic and advantage to the mesh approach is dynamic routing, improving capacity, resilience, and time-bounded performance. Note the possibility of multiple simultaneous paths through the mesh. But adding capacity can involve more nodes and more radios per node, increasing the potential for interference to unrelated nearby Wi-Fi networks. *Source:* Farpoint Group.

source and destination. This allows the Internet to balance traffic loads and provides a degree of fault-tolerance in the event of disruptions to service within the infrastructure, the reason the Internet was conceived in the first place. Wireless-LAN meshes use Wi-Fi radio links between mesh nodes for backhaul, and the routing algorithms used to decide what to send over which link and when remain the "secret sauce" in most mesh implementations today. Note that meshes can (and do) grow organically as demand (which can be quantified as number of users, amount of data, and any time-boundedness requirements for that data) grows over time, increasing the requirement for both access and backhaul capacity.

Regardless of the intricacies of the specific routing algorithms employed, it can be seen that all of the radio traffic inherent in the mesh approach will quickly add up to a potentially large demand for capacity in a fairly compact area. Given the limited range of mesh nodes (we are still, after all, dealing with Wi-Fi radios subject to spectrum regulations regarding the use of the unlicensed bands), and the increasing demand for capacity on Wi-Fi networks of all forms, we expect that the demands of traffic on Wi-Fi meshes will grow dramatically over the next few years. The possible responses to this challenge on the part of the operators of these networks could exacerbate the potential for interference from these networks, as follows:

- *Increased density* − Farpoint Group generally estimates the number of mesh nodes required per square mile at between 15 and 45, depending upon terrain, obstructions, number of users, transmit duty cycle requirements, the size of objects transferred, and any time-boundedness requirements those objects possess. As the demand for capacity only increases over time, it can be assumed the number of mesh nodes required and installed in any given area will also increase over time.

- *Increased number of per-node radios* − It also makes sense to increase capacity by adding more radios per node, each on its own Wi-Fi channel, of course. Directional antennas could be employed to re-use Wi-Fi channels within an individual node.

- *Increased demands for backhaul* − And, of course, more user-radio capacity means more backhaul capacity is required, especially for time-bounded traffic like voice and streaming video. If this backhaul is implemented on Wi-Fi channels, as is most commonly the case, the potential for interference to external Wi-Fi networks within range is increased.

As we noted above, backhaul can also be addressed by using a non-Wi-Fi wireless technology, such as fixed WiMAX, and some mesh vendors are pursuing this approach. Given the requirements and expense inherent in using licensed bandwidth, however, we do not expect such to become very common in most parts of the world. Rather, the current strategy of using all three non-overlapping channels in the 2.4 GHz. band for user traffic and the 5 GHz. band for backhaul will likely remain dominant for some time, with increasing use of the 5 GHz. channels for access as well.

In summary, then, we have an ever-greater number of metro-scale Wi-Fi networks, with an ever-increasing number of nodes, which each node having an ever-increasing number of radios, and consequential ever-increasing requirement for backhaul, and we have the potential for significant radio interference between metro-scale Wi-Fi meshes and other Wi-Fi networks, both residential and enterprise, potentially on a very broad scale. We could, of course, also see interference between one metro-scale Wi-Fi operator and another, but solutions to this problem derive from the others we will present.

The Metro-Scale Mesh Interference Challenge

There are actually two separate potential problems with respect to radio interference and metro-scale Wi-Fi meshes. The first of these is interference *from* nearby unrelated (to the mesh) Wi-Fi nodes and networks to selected nodes within the mesh, and, more importantly, interference from the mesh *to* nearby residential and enterprise networks. In the case of the former, only the performance of the mesh would be affected. Operators of metro-scale Wi-Fi networks, contrary to some beliefs we've heard, have no special entitlement to the spectrum they use; they have exactly the same privileges and obligations as any other user of these bands. And they have no protection against other nearby metro-scale operators. The only exception here is the use of the 4.9 GHz. licensed bands available to municipal government entities. This spectrum, once licensed, however, belongs to the local government and not to any commercial operator. The bottom line here is that operators of metro-scale Wi-Fi networks needs to monitor for interference and take corrective action where possible.

The opposite situation, interference from the mesh to nearby unrelated Wi-Fi devices, is potentially much more serious. Commercial Wi-Fi services could be operating at much higher power levels than is typical for residential and enterprise users, and could be concentrating their transmissions using directional and otherwise high-gain antennas. Their transmit duty cycles can be quite high, and will most certainly increase, as we noted above, over time. And, most importantly, as metro-scale Wi-Fi deployments proliferate, their nodal densities will also increase. We thus have the potential for an every-increasing blanket of radiation across potentially large geographic areas in the unlicensed bands serving as a source of interference for enterprise and residential Wi-Fi systems.

A Problem, or Not?

As we noted above, we have to date conducted no empirical studies of interference to or from metro-scale Wi-Fi meshes. We did, however, interview senior executives from a number of Wi-Fi mesh equipment vendors regarding the potential for both types of interference noted above. With respect to interference from external Wi-Fi networks to the mesh, all of the vendors told us that this is not a significant problem for them, nor is it expected to be. Meshes will reconfigure, changing channels, modulation rates, and transmit power levels, and re-route traffic, using mesh routing protocols, automatically. Meshes can and do adjust the sensitivity of their radio receivers when faced with significant interfering signals. A number of vendors reported that signals originating from a nearby by indoor source would likely be too weak to cause any serious problems for them, and we must agree that this is likely going to be the case, especially considering that meshes will also be using higher transmit power than nearby enterprise and residential nodes. Finally, some mesh vendors are now deploying “customer premises equipment” (CPE), which is subscriber equipment that actually forms the edge of the mesh via equipment installed in a subscriber’s home or office. These CPE boxes replace potentially-interfering access points and wireless routers, and allow a much greater degree of traffic control and reliability than would be possible with subscriber devices like notebook computers communicating through walls and windows.

But this brings us back to the other, and much more significant, question: will metro-scale Wi-Fi meshes cause interference to residential and enterprise WLAN deployments? While we have no direct evidence that such is major problem today, the parameters that we have outlined in this Tech Note certainly lead us to the conclusion that such interference is very likely to become a challenge in urban areas over the next few years. This means that operators of especially enterprise Wi-Fi systems need to be on the lookout for the symptoms of interference, and then use Spectrum Assurance (SA) tools to identify the sources. Reconfiguration of the enterprise WLAN, in terms of adjusting transmit power and even the location of APs, may also be necessary, and we believe this functionality will benefit from increasing automation as SA tools are integrated into wireless LAN systems themselves, as Cisco, for example, is currently doing with their WCS 4.2 release.

As of this point, our advice is to monitor for interference from metro-scale meshes in the same manner as any other potential interferer, using Spectrum Assurance tools. As we discussed in our White Paper FPG-2006.321.2, *The Invisible Threat: Interference and Wireless LANs*, tools such as Cisco’s *Spectrum Expert* [http://www.cisco.com/en/US/products/ps9393/index.html], which we use at Farpoint Group and highly recommend, can be used to monitor for and identify specific forms of interference easily and automatically. As we have also noted before, interference will most likely show up as reduced throughput in the WLAN, and, without the proper tools, identifying the reason for this reduction can be and will remain very difficult indeed.

The bottom line for now is that the potential for interference from metro-scale wireless LANs needs to be managed as any other, and the tools to address this challenge exist today. We will continue to monitor this issue as deployments (*proliferation* might be a better term) of metro-scale Wi-Fi services continue.

Farpoint Group
Ashland MA 01721
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

The information and analysis contained in this document are based upon publicly-available information sources and are believed to be correct as of the date of publication. Farpoint Group assumes no liability for any inaccuracies which may be present herein. Revisions to this document may be issued, without notice, from time to time.