Optimizing Spectrum Utilization: The Shared-Access Network

A Farpoint Group Technical Note

Document FPG 2007-279.1
June 2007

The upcoming auction of the very-desirable 700-MHz. spectrum by the FCC creates an important and in fact unique opportunity to rethink a number of key assumptions about both spectrum policy and the nature of wireless network architectures. We expect the demand for the various bands at 700 MHz. to be very heavy primarily because the radio propagation characteristics of these frequencies allow excellent coverage in urban, suburban, and rural areas, and even indoors as well. Both commercial and government interests are excited about the possibilities here, and that brings up an interesting question indeed: is it feasible to deploy a single network infrastructure in this spectrum, based on a common architecture, which can serve the needs of both of these constituencies?

Traditionally, licensed spectrum has been reserved for individual licensees. This has always been the case of government - primarily public safety and emergency/first-responder services - because, well, that's the way it's always been, and, of course, the nature of the fundamentally analog communications historically used in public-safety applications is poorly suited to any form of spectrum sharing. But modern, digital networking and communications technologies, primarily in the form of an all-Internet Protocol (IP), mobile, wireless, broadband network with full support for prioritized and time-bounded traffic, instead constitute an ideal platform for a *shared-access* networks meeting the needs of perhaps *many* simultaneous and distinct services, constituencies, and applications – public-sector and commercial alike. Note here that we are talking about *network architecture* based on IP, but *not* about any specific radio technology. One of the core benefits of this approach is that it is in fact *entirely independent* of any specific radio implementation, and, in fact, could work well with a multi-radio converged strategy – another trend that we believe will become essential in future wireless networks.

The purpose of this Tech Note is to explore the key elements of shared-access wireless networks, and why this strategy will become the preferred - if not *dominant* - approach in future network deployments, both public-safety and commercial, at any frequency, and particularly in the 700 MHz. bands.

Understanding Shared-Access Networks

IP has become, over the past 20 years, the only network protocol that matters. Part of the reason for this is of course the success of the Internet, but also the fact that the IP protocol stack has benefited from continual improvements and additions to support essentially any class of service, from low-bandwidth, high-latency traffic to quite the opposite, broadband, telephony and streaming video. One could argue, of course that they key to success for the Internet was a fundamentally cooperative implementation essentially based on the concept of *over-provisioning*. With the supply of bandwidth exceeding demand, there's less need for clever protocol-based solutions implementing quality of service (QoS) and class of service (CoS) capabilities. But these protocols have nonetheless appeared in IP over the years, making it suitable to essentially any type of traffic and supporting essentially any network-based application. Both raw bandwidth and the management of this bandwidth via protocols will continue to be core requirements, especially as networks see more traffic and occasionally become congested.

Assuming a single network capable of such service, the opportunity for *open-access* networks is realized. Open access, for purposes of this document, means that any authorized user/device/application combination can be supported along with many others, simultaneously, on a single network infrastructure. For example, it is possible to mix both time-bounded (real-time) traffic and traffic with a greater tolerance for latency in a single network. By implication, then, it should also be possible to mix traffic with a broad range of not just prioritization requirements but also security needs, traffic-volume demands, and other factors simultaneously as well, relying upon the provisioning of sufficient capacity and the implementation of appropriate network and traffic-management protocols to yield the desired levels of service. Farpoint Group believes that open-access networks will become the norm in the not-too-distant future, with political considerations relating to spectrum regulation more of a concern than the technology required to bring this vision to fruition. After all, as was noted above, the technology required already exists and is in operation on IP-based networks on a global basis today.

Indeed, as we noted above, current wireless public-safety communications systems (the term "network" is not always appropriate here today) have traditionally been implemented on spectrum reserved just for them. This isn't necessarily a bad idea when the traffic is analog and primarily of a push-to-talk voice nature. But public safety agencies today are increasingly in need of data networks capable of supporting IP-based applications, including access to graphical and video-based information - in other words, multi-media networks. The question then becomes, given the possibilities inherent in shared-access network architectures, why would it not be feasible to mix public-safety and commercial traffic in a single network, based on IP? The interoperability inherent in IP would have an important additional benefit here, giving public-safety officials access to a greater range of subscriber units, at lower prices than would be the case with specialized devices operating on a specialized network.

One question we have been asked is whether commercial IP-based wireless networks would have sufficient security to meet the needs of the public sector. The answer to this question is a resounding yes, again using capabilities already in place today. End-to-end encryption can be provisioned via virtual private networks (VPNs), using, for example, IPSec and/or SSL, with additional airlink security provided by the specific radio technology in use. Strong authentication is available via the IEEE 802.1X standard and the Extensible Authentication Protocol (EAP). EAP can provide essentially any authentication mechanism desired, from username/password, to biometric, hardware-token, and digital-certificate solutions. Security keys can be customized to individual sessions, users, or devices. Authentication can be applied to both users and devices, and can also be used to drive traffic prioritization decisions.

What we are describing here is what Farpoint Group has been calling *4G* networks. The term 4G remains imprecise, to be sure; some are using it in conjunction, for example, with 100 Mbps service or some other arbitrary throughput number. We prefer to use 4G to describe multi-service, shared-access networks with support for traffic prioritization and capable of essentially any set of missions simultaneously, independent of any specific radio technology. Moreover, given the scarcity and high cost of radio spectrum, it makes sense to share access among services so as to make the best use of a scarce resource. Spectrum reserved for specific applications will of necessity lie fallow much of the time. This problem is eliminated via the use of prioritized access, an inherent feature of 4G networks required to implement time-bounded service like voice, but also directly

applicable to class-of-service as well. This means that an instantaneous demand for capacity by a public-safety application will be prioritized ahead of any commercial traffic when required.

We can think of no technical reason why a 4G architecture could not support essentially *any* mix of users, traffic and applications, subject of course to provisioning enough raw bandwidth for the traffic demand present at any given moment in time. And we can also think of one other reason why public-safety users should demand such a solution – *interoperability*. As we learned during 9/11, there are a huge number of incompatible public-safety communications systems in use today, and this problem must be addressed as soon as possible.

Key Public-Safety Application Support Requirements

Thus far, we have demonstrated that the facilities required to implement shared-access 4G networks exist today. The technical risk inherent in deploying these networks is, then, quite low. But there are in fact a few additional requirements imposed on shared-access networks in order to fully support public-safety applications, as follows:

- *Lawful Intercept and CALEA* − Commercial communications network operators are obligated under federal law (known as the *Communications Assistance for Law Enforcement Act*, or *CALEA*) to provide a mechanism for intercepting traffic under carefully proscribed conditions. Support for CALEA in open-access networks is conceptually simple, involving the copying of packets in streams identified as being of interest, for recording, interpretation, or re-direction. There is no reason, then, why an open-access network could not provide these required services.

- *Support for E911* − Enhanced 911 (E911) is a set of extensions to wireless networks that allow for location information to be captured and communicated along with other emergency-related information. The FCC does not specify a particular technology for implementing E911, and several are in use today, including time difference of arrival (*TDOA*, a form of terrestrial triangulation), angle of arrival (*AOA*), and the use of the Global Positioning System (*GPS*), which is satellite-based. Because urban areas do not always have a clear view of the sky, a terrestrial component is often added to E911 implementations otherwise based on GPS. This is referred to as Assisted GPS (A-GPS). Regardless of the specific approach chosen to implement E911, an open-access network can easily forward location information like any other data.

- *Network Integrity* − As we noted above, security mechanisms appropriate to public-safety (and also more than useful in commercial) applications are already in place. An even more interesting question involves overall network *integrity*, the ability of a given solution to tolerate some degree of interruption to portions of the network. As it turns out, IP was in fact designed with exactly this challenge in mind. Failure in any given part of the network, or even multiple simultaneous failures, simply results in the re-routing of packets in response. Such actions can be taken with respect to the airlink (the failure of a cell simply forces the association of a given mobile unit with another cell) and the rest of the network value chain as well.

An example illustrating how all of these pieces fit together in a shared-access solution can be seen in Figure 1.

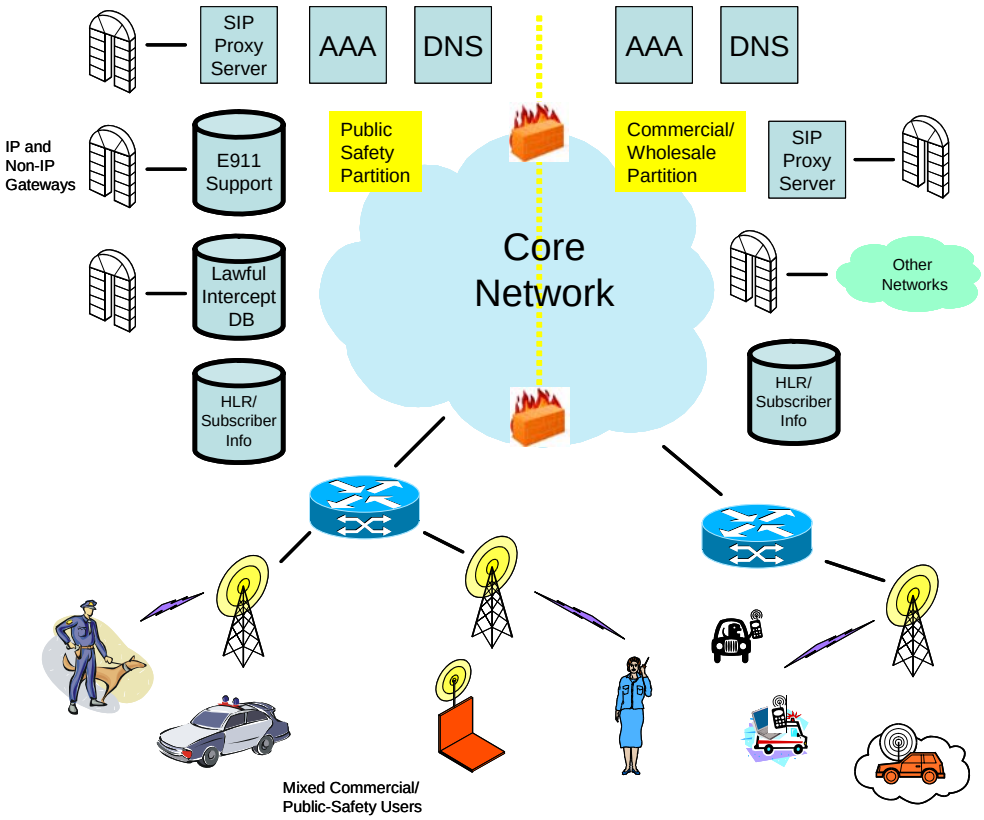

Figure 1 - A block diagram of a potential shared-access network, as proposed by Frontline Wireless. Note that any authorized client can access the network, and that the physical and logical separation of different classes of service can be performed in the core of the network (represented by the firewalls between the "commercial" service to the right, and the public-safety service on the left). Gateways are used to provision connectivity to external networks and legacy services. *Source:* Frontline Wireless.

A Note on Business Models

As we have demonstrated above, there are no technical roadblocks to the deployment of large-scale shared-access networks services with the possibility of a very broad variety of classes of service. These networks can have the security, integrity, traffic prioritization, and flexibility essential to any application or service, and can also support all other key requirements essential in public-safety communications solutions today.

One proposal for deploying a shared-access network in the 700 MHz. bands involves the use of a wholesale/retail model, with a wholesaler owning and operating the network, supporting multiple retail customers offering public, commercial, mixed, or other services. Such is, of course, independent of any specific network implementation, but there is no conflict whatsoever between this business model (which is likely best suited to supporting multiple missions regardless) and the fundamental technological nature of shared access.

It is also important to point out that the shared-access strategy is completely independent of any underlying radio technology – or, more likely, technologies. As can be seen in Figure 2, the layer natured of the IP stack allows common services to be provisioned across an essentially unlimited number of physical layers (PHYs), both wired and wireless. Perhaps even more importantly, individual connections can be moved across a number of PHYs, or even provisioned across several simultaneously. This is the essence of *Fixed/Mobile* and *Mobile/Mobile Convergence (FMC/MMC)*, a key requirement going forward. After all, no radio technology can do it all, and a combination of wide-area systems and Wi-Fi may become the most desirable alternative. The real beauty of the shared-access approach is that it maintains independence from any particular radio, and equally importantly, any particular spectral band. The flexibility of the shared-access approach is unmatched in any other strategy.

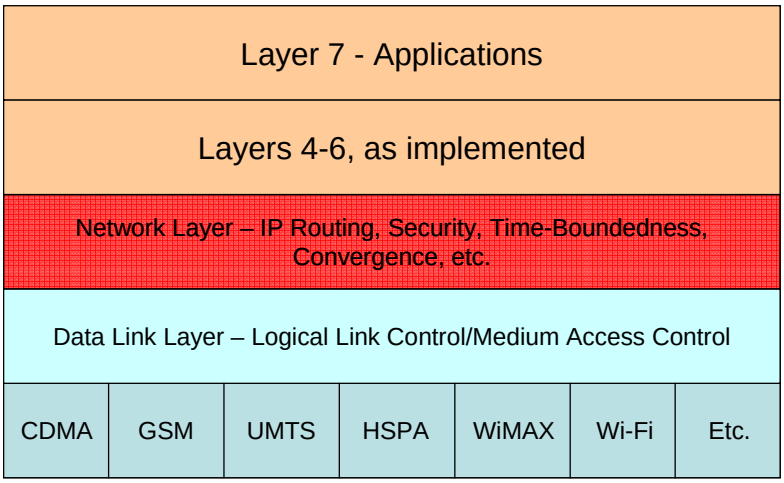

Figure 2 - Conceptual model of the IP protocol stack. Open-access architectures can support multiple physical layers (PHYs) in addition to multiple classes of service, as well as handoffs across these PHYs. *Source:* Farpoint Group

Conclusion – The Best Solution for Mobile Networks

It is very clear, we believe, that shared-access networks are the future of wide-area wireless communication for all applications and multiple, simultaneous constituencies. There is no reason that a broad variety of public-safety and commercial services cannot be served by a single shared-access network, and we believe that such an approach provides all necessary services while making the best use of the radio spectrum in a cost-effective and interoperable manner. This concept is perhaps the most broadly-influential trend in networking today, and we expect to see such systems in use as the deployment of 4G networks proceeds over the next few years.

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