IEEE 802.16 Working Group on Broadband Wireless Access
http://WirelessMAN.org

Roger B. Marks
Chair, IEEE 802.16 Working Group
r.b.marks@ieee.org
21 March 2013

To: IETF LMAP Mailing List
        IETF Ops Area
            Benoit Claise
            Joel Jaeggli

cc: IPPM Working Group

        Walter Johnston, Chief, Electromagnetic Compatibility Division, FCC
        James Miller, Office of Engineering and Technology, FCC
        Henning Schulzrinne, Chief Technologist, FCC

        David Allan, Co-chair, Broadband Forum End to End Architecture Group
        Christophe Alter, Broadband Forum Technical Committee Chair
        Paul Nikolich, Chair, IEEE 802 Executive Committee

Subj: Requesting LMAP perspectives of IEEE Project P802.16.3 Architecture and Privacy

The IEEE 802.16 Working Group (WG) on Broadband Wireless Access is seeking the views of the LMAP community, particularly in relation to Project P802.16.3 on *Mobile Broadband Network Performance Measurements*. This inquiry follows reports of 19 November 2012 (IEEE 802.16-12-0680) and 17 January 2013 (IEEE 802.16-13-0041).

The P802.16.3 perspective is currently reflected in working document IEEE 802.16-12-0682-01 on "[Draft] IEEE 802.16.3 Architecture and Requirements for Mobile Broadband Network Performance Measurements." Note that our project is targeted directly at mobile users (independent of air interface technology) and, at the core, the needs of those users for performance data about their networks. The needs of additional stakeholders, such as network operators and public administrators, are also itemized and addressed.

Project P802.16.3 has reviewed the draft minutes of the Large-Scale Measurement of Broadband Performance (LMAP) BOF of 13 March <http://www.ietf.org/proceedings/86/minutes/minutes-86-lmap> and would like to forward some of our thoughts and questions:

(1) The LMAP BOF draft minutes indicate some concerns about issues of "gaming the system", including "identification of test traffic and giving it preferred treatment," noting that "many integrity issues cannot be engineered beyond the realm of the possible." In this regard, we wonder if the LMAP discussions have considered the use of both public and private Measurement Servers, as indicated in the draft P802.16.3 architectural model. In our view, the public Measurement Server is useful for public measurement campaigns, but the private Measurement Server, which is specified under the control of the Client, serves a different purpose. The private Measurement Server allows a private user to conduct measurements with respect to a

specific network location. That location may represent a point in the network to which the user is particularly interested in connectivity; for example, to a user's primary place of business. The P802.16.3 model endeavors to support the user in making such private measurements at will. To our understanding, it would be difficult for an operator to provide preferred treatment for such a case; if so, the provider would need to prioritize not by IP address but by packet inspection to detect the presence of measurement activities. We wonder whether LMAP has considered introducing private as well as public measurement servers and look forward to critical comments on our approach.

(2) The LMAP BOF draft minutes include minimal discussion of Security and Privacy; these are noted as "TBD." From our perspective, privacy is a core issue and helped to motivate our architecture at the most basic level. When LMAP considers these issues, we would like to request comments regarding our stipulation of separate Public and Private Data Collector entities in the architectural reference model. In our view, large-scale consumer measurement campaigns do require a public Data Collector, and perhaps that is the sole focus of LMAP. However, this results in a privacy dilemma. Since public users will be hesitant to volunteer for public data collection that potentially exposes their private information, it will be essential to ensure that collected public data is suitably anonymized. On the other hand, if the data is anonymous, it will not be of value to the individual users for analysis. To our understanding, the availability of such personalized data is the main incentive for the individual to participate in the campaign. Because we are presuming mobile users, our view is that the cost of participating in a public campaign may be quite high for the private user, probably prohibitively high unless the private user receives private benefit from the information. The use of separate public and private Data Collectors provides an opportunity to resolve the dilemma. Professional or enterprise users, or any who wish to store data privately, are given the opportunity to do so. Note that the private Data Collector entity might be located direct in the mobile device itself, but we are also planning to support network-based private Data Collectors that provide more storage and more flexibility of access. For example, an enterprise may be interested in analyzed results collected from a large employee pool collected into a single database.

Note also that the P802.16.3 architectural model, while placing the private user measurements at the focus, does not neglect the needs of large-scale public measurement campaigns. The model accounts for the ability of the private entities to contribute data (suitably anonymized) to the public Data Collector. Since the anonymization and communication are handled by the network entities, the work is offloaded from the local device, requiring fewer mobile resources (battery power and over-the-air communications).

One key factor that we have not fully analyzed is the degree to which the public system will value the private-reported data and trust its authenticity. We hope that IETF participants may have expertise that would guide us in understanding those issues. At the current time, we do not see that the use of the public/private diversity significantly increases the susceptibility of the public system to falsified data reports. We are open to other views.

Please keep us informed regarding progress in the LMAP activity, including chartering proposals when they become available for review. We also welcome further input and encourage comments regarding our Architecture and Requirements draft. We draw attention to the relevant Call for Contributions IEEE 802.16-13-0060. Our next opportunity to discuss new inputs will occur at IEEE 802.16 Session #85 (13-16 May 2013 in Waikoloa, HI, USA). For information on our future meeting schedules, see http://ieee802.org/16/calendar.html.

Sincerely,

Roger B. Marks
Chair, IEEE 802.16 Working Group on Broadband Wireless Access