Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**NRR Draft Report**
Date Submitted	**Resubmitted 2010-03-17 (Originally submitted 2009-07-15)**
Source(s)	Matthew Sherman BAE Systems GRIDMAN SG Chair Voice: +1 973-633-6344 E-mail: matthew.sherman@baesystems.com *<http://standards.ieee.org/faqs/affiliationFAQ.html>
Re:	802.16 Working Group Ad Hoc Committee on Network Robustness and Reliability
Abstract	This document is a resubmission of the document C802.16nrr-08/004r3 originally developed by the NRR Ad Hoc Committee.
Purpose	Reference for GRIDMAN Study Group
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

NRR Draft Report

Authors: Arnaud Tonnerre (THALES), Stephen Skipp (Plextek), Sheng Sun, Mo-Han Fong (NORTEL), Ranga Reddy (US Army), DJ Shyy (MITRE), Frank L Whetten (BOEING), Djamal-Eddine Meddour (France Telecom), Arthur Wang (LinQuest), Yi-Hsueh Tsai, Chih-Hsun Chou (III)

Table of content

1 Scope

The NRR Ad Hoc Committee has been created at session #58. The main objectives of this activity are to promote discussion and to carry out studies on network robustness and reliability. The Committee will also analyze the potential interest for standardizing an advanced air interface that would enable mission-critical communications. Thus the purpose of the initiative is to provide supplementary functionalities for fixed and mobile 802.16 systems, to be deployed in civil and professional applications.

This Working Group Ad Hoc Committee has been created to study specific issues that are not addressed in the other IEEE 802.16 standards or Task Group activities. Indeed, in particular, the primary focus of 802.16m is to "*meet the cellular layer requirements of IMT-Advanced next generation mobile networks*" [5]. The 802.16m standard is intended to be a candidate for consideration in the IMT-Advanced evaluation process, which binds the project to follow a strict timeline in relation to the ITU planning. Therefore the consideration of additional requirements and features for specific applications would be inappropriate in this activity.

The target applications are not only Land/Private Mobile Radios (LMR or PMR), which are used by a wide range of customers such as public safety, transportation and utilities industry, but also Surveillance, Airport/Harbor Communication, Disaster Responder and Replacement, and Quick-Deployable Backhauling. All those applications have common high requirements for resilience, reliability and security.

The work conducted in between sessions #58 and session #59, has allowed defining the scope of the NRR Ad Hoc Committee. The objective is to tackle robustness and reliability aspects, as well as supplementary topics that have been identified as important requirements for the target applications. The NRR Ad Hoc Committee is therefore focused on the following items:

- High resilience and robustness,
- Increased reliability level,
- High security, protection and assurance,
- Spectrum analyzes,
- Reliable network topology,
- Very high speed mobility,
- Dynamic group management,
- Increased range,
- Mobile base stations,
- Enhanced relay operations,
- Coexistence with DSRC systems.

2 References

[1] IEEE Std. 802.16-2004: IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems, June 2004

[2] IEEE Std. 802.16e-2005, IEEE Standard for Local and metropolitan area networks, – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, – Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, and IEEE Std. 802.16-2004/Cor1-2005, Corrigendum 1, December 2005

[3] Call for interest on Network Robustness and Reliability, Arnaud Tonnerre, Matthew Sherman, November 2008, http://www.wirelessman.org/docs/08/C80216-08_028.ppt

[4] Land Mobile Radio evolution to Broadband, C80216nrr-08_002, Arnaud Tonnerre, December 2008

[5] IEEE 802.16m Project Authorization Request (PAR), December 2006, http://standards.ieee.org/board/nes/projects/802-16m.pdf

[6] White paper on C-band bandwidth requirements for future Airport Communication Systems, ACP-WGF15/WP23, International Civil Aviation Organization, May 2006

[7] "TETRA and WiMAX: Complementary or competing?", Marco Morresi, Enrico Donnini, www.tetramou.com

[8] "The market positioning of TETRA", Devdarsh Jain, www.tetramou.com

[9] "WiMAX, what is it and what can it offer to the mission critical business case?", Pierre Force, TETRA Association members Workshop, 4 November 2008

[10] "Broadband wide-coverage, emergency mobile communication", Dr. M. Nouri (Chairman of ETSI TC-TETRA WG4), ICWMMN, October 2008, Beijing, China

[11] SMART-Net project, under the Future Internet Research and Experimentation (FIRE) initiative, ICT-223937, deliverable D2.1 "Requirements and specifications of SMART-Net targeted scenarios", April 2009.

[12] SAFECOM program, "Statement of Requirements for public safety wireless communications and interoperability", April 2004.

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

AOC	Airline Operational Communication
APCO	Association of Public safety Communications Officials
BS	Base Station
DSRC	Dedicated Short Range Communication
ETSI	European Telecommunication Standard Institute
IMT	International Mobile Telecommunications
ITU	International Telecommunication Union
LMR	Land Mobile Radio
LOS	Line-Of-Sight
NLOS	Non-Line-Of-Sight
NRR	Network Robustness and Reliability
PAR	Project Authorization Request
PMR	Private Mobile Radio
SS	Subscriber Station
TEDS	Tetra Enhanced Data Service
TETRA	TErrestrial Trunked RAdio
TIA	Telecommunication Industry Association

4 Applications

4.1 Description of the usage models

The following usage models depict selective NRR applicable use cases. The initial purposes are:

- Clarifying the scope of targeted technical objectives,
- Establishing some common understanding of the uniqueness,
- Demonstrating the need of Resilience and Robustness,
- Facilitating the following discussion of requirements and issues.

It shall be noted that usage models are introduced to help identify areas of requirements. Not all requirements will be supported by NRR, the filtering process is pending on future work.

4.1.1 Land mobile radio applications

Land Mobile Radio (LMR) systems denote wireless communication means providing mobile radio services for coordination of people and material, safety, security and emergency responses. LMR systems are used by a wide range of users such as companies, public safety organizations, public transportation and utilities industry. Therefore those systems have been designed especially for mission-critical communications and then LMR wireless networks shall be:

- *Accessible*, this means that the coverage area shall be large enough for providing services at the required location (spectrum issues in Sub-GHz bands).
- *Available*, denoting a high level of resilience and robustness. Indeed the service shall be available whenever the users need it.
- *Secure*, with high requirements for authentication, integrity and confidentiality services.
- *Predictable*, involving high-reliability of the transmissions.

Several digital standards have been established for such applications, in particular by the TIA in United States (e.g. APCO) and the ETSI in Europe (e.g. TETRA). Those systems are robust, secure, highly reliable and specified for low frequencies, which make them cost effective. Indeed the use of sub-GHz frequency bands provide large coverage operations for each Base Station and then less BS are required to cover a certain area. However, in conventional LMR standards, there is very limited provision of data services. Currently the bandwidth allocated to data services is quite low, usually less than 10kbps. Some works have been carried out to provide Wideband capabilities with up to 500kbps data rate (e.g. TETRA2 TEDS), but it is not sufficient for offering new services such as video streaming.

Consequently Broadband solutions, such as 802.16, shall be introduced in LMR systems for provisioning new services enabling in particular faster emergency responses for public safety organizations. The current and short term approach seems to be the deployments of Broadband networks as hotspots in specific areas. The logical evolution afterwards will be an integrated LMR/Broadband solution with multi-mode stations and fully operational interworking between these two technologies. The most likely long-term vision is convergence between LMR and Broadband solutions, in which 802.16 may play an important role since it is a good basis for developing a Broadband LMR system. To this end, 802.16 shall specify the enhancements that are needed to meet the related specific requirements.

It shall be noted that the TETRA community is currently analyzing potential technologies for developing such a Broadband solution. Indeed Dr. Nouri, chairman of TC-TETRA Working Group 4 (TETRA high speed data), states in [10] that "*TETRA requires addition of a broadband capability to cater for today's* *sophisticated multimedia applications*" and he also explains that WG4 will define the broadband solution in the coming years. 802.16 is foreseen to be one candidate [7] [8] [9] [10], however the current standards would require enhancements in security, reliability, resiliency and group management [7][8] [9].

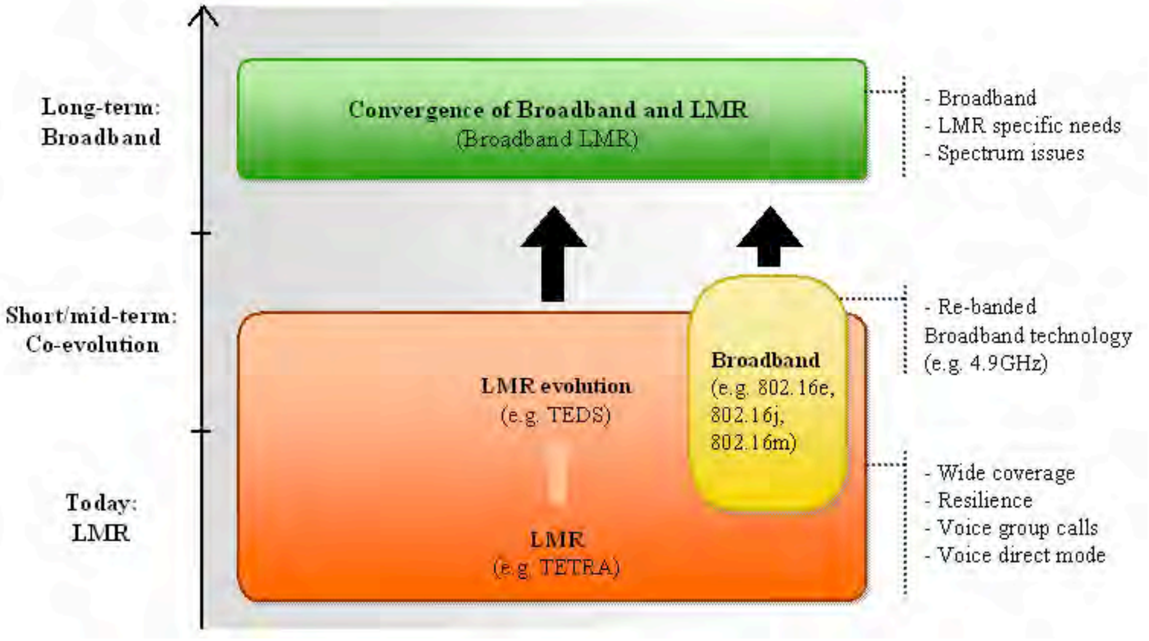


Figure 1: Envisaged LMR evolution to broadband

4.1.2 Surveillance scenarios

4.1.2.1 Air-Ground Scenario

The scenario is for UAV with 802.16 communications payload conducts surveillance. If UAV assumes the role of a BS, the associated subscriber stations would be on the ground. The design considerations include increased Doppler shift and different channel models than the ground-based systems.

The communication payload on the UAV can be in the form of a base station, a relay or a subscriber station. A requirement with mobile base station and mobile relay would be highly desirable.

4.1.2.2 Government Surveillance Use Cases

Majority of commercial surveillance applications focus only on high profile dwellings such as banks, retailer stores, or storage facility. These applications expose less difficulty by adopting existing wireless communication standards. However, for boarder petrol, coast guard, or military personnel, their interest may extend to support:

- Wireless connectivity in extremely long range, wide area, or non-line-of-sight terrain,
- Operation in interfering/jamming/hostile situations,
- Collecting information only by protective (highly secure) communications,
- Deploying surveillance network in self-healing geographical topology and with high availability.

These applications surface a need to modify the standards to consider a reliable frequency band, stronger encryption, tighter access control, link-interruption recovery or heterogeneous network topology.

4.1.2.3 High Altitude Platform Imaging

A very similar scenario to UAV surveillance is Disaster Imaging which offer needed situational awareness for rescue mission. In most disaster management, the term UAV could be generalized to any “high altitude long endurance” platform that could be achieved by fuel efficient UAV circling around the target area, an unmanned high altitude stationary platform (Balloon), or a pilot based long duration aeronautical vehicle.

Depending on the capability of the platform, disaster imaging either operates in a extreme weather (low altitude) or in necessity to penetrate through rain clouds (high altitude). The challenges are summarized as:

- Difficult channel estimation impacted by carrier phase detection and calibration,
- Long range wireless link (>15 km in some cases) to avoid storm,
- Higher speed (>200km/h) in some cases,
- Broadband (for video/imaging).

4.1.3 Aviation usage models

The aviation usage models for 802.16 corresponds to Airport Communications and intra-airplane wireless transmissions. Moreover the use of 802.16 systems at the Airport shall be divided into two different applications; Airport Surface Communication and Extended Airport Communication.

The main services for these applications are listed hereafter:

- Surveillance,
- Weather data transmission,
- Navigation,
- Automation,
- Electronic Flight Bag,
- Airline Operational Communication (AOC): voice and data services.

4.1.3.1 General requirements for aviation usage models

Aviation has use cases for a deterministic, robust, relatively low-power protocol stack.

- Real-Time applications: A number of real-time applications exist in aviation, beyond the initial obvious cases of voice and video streaming. Examples include engine monitors and systems controls, which are real-time, and high-bandwidth.

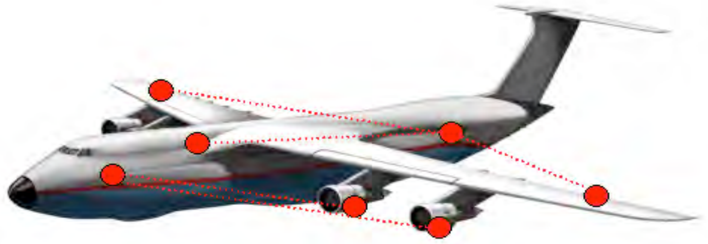


Figure 2: Example of intra-airplane wireless communications

- High-robustness applications: Aviation has far more stringent performance requirements than most systems designs. While it is unlikely that 802.16nrr will qualify for aviation applications in a COTS form, considerations of aviation applications early in development process could result in suitable COTS hardware that is amenable to aviation applications with minimal modification of the firmware.

- Potential architectures: Several different architectures are likely to coexist.
    - Peer-to-peer: many network nodes may be categorized as cable replacement in environments hostile to cable bundles – for example on landing gear. A wireless link may replace a large number of cables, requiring fairly high bandwidth capacity, and highly robust network connectivity and throughput.
    - Fixed point-to-multipoint: In this scenario numerous subscriber stations would communicate with an infrastructure base station which provides backhaul to the remainder of the airplane systems.
    - Mobility: There are several mobility use cases, including air crew communications systems as they move about the airplane, and airplane communications with the airport infrastructure as the plane moves about an airport.
- Security: Any wireless systems in aviation must be able to assure message security, integrity, availability, and other standard security metrics. Additionally, the protocol stack should be able to detect a denial of service attack, whether protocol- or jamming-based; and provide robust avoidance and recovery methods.

4.1.3.2 Airport Surface Communication

Aviation experiences rapid growth and then it is foreseen that the airport infrastructure will be enhanced significantly to meet future demand. In particular, regions such as the United States and Europe need a fundamentally new Airport Traffic Management system if they are to accommodate the expected doubling of traffic by the end of the next decade. This transformation requires better communications linking airborne and ground-based elements.

Therefore EUROCONTROL and the FAA (Federal Aviation Administration) have initiated a joint study to identify potential future communication technologies. One of the main results of this work was the recommendation of 802.16 technology for the provision of dedicated aeronautical communication services at the airport surface. It is expected that such system will operate in the aeronautical C-band frequency allocation, between 5091 and 5150 MHz.

The Airport Surface Operation includes communication involving ground-based elements and transmissions between infrastructure and airplanes when they are on the ground at airport (parked or taxing along the runways). Typical coverage for such an application corresponds to the whole airport surface, namely up to 6 km and the path loss model varies from Line-Of-Sight to Non-Line-Of-Sight. The maximum speed for a vehicle moving around the airport is 100km/h. Moreover the use of wireless networks for certain safety critical applications (e.g. surveillance, weather data) requires high security and reliability levels.

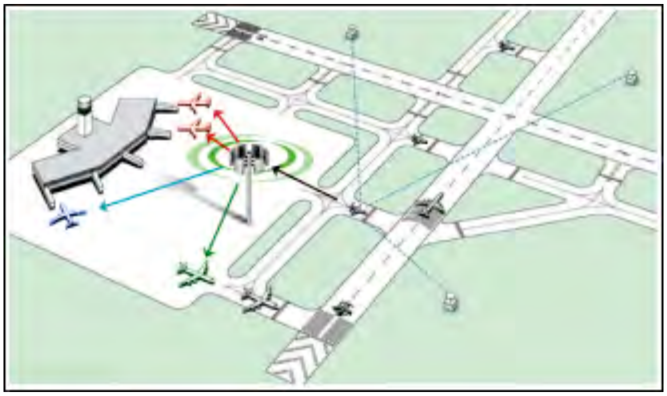


Figure 3: Illustration of Airport Surface Communication

4.1.3.3 Extended Airport Communication

The Airport Operation Communication may be expanded to a wider area. Extended Airport Communications are performed between the ground-based infrastructure and airplanes flying near the Airport. They may be either approaching the airport for landing, or taking off. The radio coverage may vary between 10 and 30 km with a LOS path loss model. The speed of the airplanes in this area may reach 400 or 500 km/h.

4.1.4 Secured and reconfigurable backhauling

The demand of fixed and mobile wireless broadband access networks is rapidly growing. All these access networks have as characteristic that the base stations possess a cabled connection to the backbone network (backhaul) or are connected in a more general way to the internet. Classical solutions for the backhaul links use optical fiber, E1/T1 lines, xDSL technologies, microwave point-to-point links, satellite links or passed through a third party network. The big drawback of the current solutions is the very high OPEX and high initial CAPEX. Furthermore, rapidly increasing traffic in the access network needs an upgrade of the backhaul link which nowadays either cannot be done easily and leads in anyway again to a high investment (CAPEX) [11].

Actually, Operators are interesting in rapid and easy deployable and low CAPEX/OPEX solutions to face the increasing demand of broadband accesses. In particular in areas where they don't held any fixed infrastructure. Therefore, proposing alternative and cost-effective solutions is essential.

The wireless secure and reconfigurable backhaul is intending to provide wireless access to the fixed network infrastructure for any kind of access network in a transparent way. It could be also deployed to increase the current capacity of the existing fixed infrastructure.

4.1.5 Disaster First Responder & Recovery

Post a major disaster, the ground based communication infrastructure may suffer a complete destruction. Disaster recovery force often wrestles with the information and communication vacuum that exists during the first 24 hours. Life hinges on the first responder gain access to critical information and provide early communication replacement. High altitude and long endurance communication solution has shown great interest to worldwide governments due to the following reasons:

- Early ground based rescue mission is prohibited by weather or crew safety constraint,

- Emergency calls may rely only on the residual battery life of a cellular phone in standby (<12 hours),
- Major disaster could wipe out all communication solutions and create an information vacuum, don't know where to start from,
- Broadband communication capacity is required to replace the ground communication infrastructure.

The following usage model is a collection of use cases bellowing to emergency disaster recovery.

4.1.5.1 Automatic and Seamless Base Station Profile Transition

During the first 24~72 hours of an approaching hurricane, it is important to anticipate the worst case and prevent the complete lose of critical information access. Two areas in particular are required to enhance a 802.16 system:

- The capability to smoothly transition of critical information from the victim base stations to back up base stations in order to provide seamless base station profile transition. The failover concept of inter-base station profile transition is new to 802.16. This feature is required to support system operating at non-nominal condition. The transition can be intentional or unintentional, human-involved or automatic.
- The capability to minimize the impact to service continuity due to base station transition. Many people may view it as the capability as "set-before-break" connection. From NRR point of view, the issue may become how to achieve the functionality of "set" and how to minimize "break".

4.1.5.2 Critical Information Access

The other important aspect for Disaster First Responder is the capability to access critical information. The system may need to have capability of policy based resource allocation assuming resource contention is going to happen. The first responder is supposed to offer the most critical connections and is not "fairness" or "service class" based. The policy is decided by the desire of disaster management authority.

4.1.5.3 E-9111

The last area of Disaster First Responder is Emergency 9111. The system may carry dual services: one for emergency communication, the other is local E-9111 compatible services. Many life-and-death situations depend on the possibility of maintaining E-9111 service before the victim's handset ran out of battery. In this case, the speed of offering replacing access connection is equally important as the compatibility with regional cellular services.

Note: since cross-standard issue is discussed in other 802 WGs, it might not be appropriate in the scope of NRR.

4.1.6 Flexible Infrastructure Platform

For a system offering high reliability and robustness may require flexibility in chosen flexible infrastructure platform. In the other words, the system may have a fixed primary base station/relay while the failover/backup platform may not be fixed. The following paragraphs intends to establish the usage case why a heterogeneous topology may be needed. Further discussion is offered below from 3 different levels of maneuvering speed.

4.1.6.1 Transportable (Nomadic) Base/Relay Stations

Transportable/nomadic base station assumes a vehicle-mounted platform which can be quickly relocated and deployed while the platform, at this temporal location is operated in a stationary condition.

The transportable/nomadic base station is often required for emergency event response or frequent mission update. The challenges are:

- Prompt bandwidth adjustment through wired or wireless solutions,
- Intelligent path selection balancing resource allocation and topology,
- Multi-homing issues by redundant coverage or paths.

4.1.6.2 Semi-Nomadic Semi-Mobile Base/Relay Stations

Public security enforcement or rescue mission may demand a flexible wireless network that can be quickly reconfigured and replace existing infrastructure. One possible solution is an airborne base/relay station. This platform, despite is in high-speed motion, may not impose complexity for frequent base station hand over. From physical layer point of view, it is “mobile” but from network layer point of view, it is stationary.

4.1.6.3 Full Mobile Base/Relay Stations

The most challenging situation of resume mission is “full” mobility. This use case covers the situations that law enforcement/military mission simply can not pre-coordinate the locations of the base/relay stations.

The network is dynamically changing the topology, and path selections at layer 1, 2, or even 3, are consistent updated. Such dynamically uncorrelated maneuver impose a large difficulty in path/link selection (We try to avoid the term route selections to differentiate the issue associated with “router”).

The combination of fixed, transportable, and mobile platforms form a heterogeneous network. It often adds unique complexity to the problem space.

5 Requirements and related issues

5.1 General requirements

5.1.1 Minimum to None Physical Layer Parameter Modification

Initially NRR would like to minimize the change made to existing PHY standard (modulation, codec, or multiplexing). The focus is enhancing the capability of prompt adjustment upon different environmental/operational situation. For example, 802.16e PHY standard offers a powerful carrier selection, which could be extended from channel fading recovery to interference/jamming avoidance.

Discussion by NRR teleconference has also reached a conclusion that spectral efficiency might not be the top priority of reliability and robustness. In a nut-shell, efficiency in any layer might be a sacrificed as a trade-off factor in exchange for high level protection (e.g. spread spectrum, interference avoidance, or redundant payload).

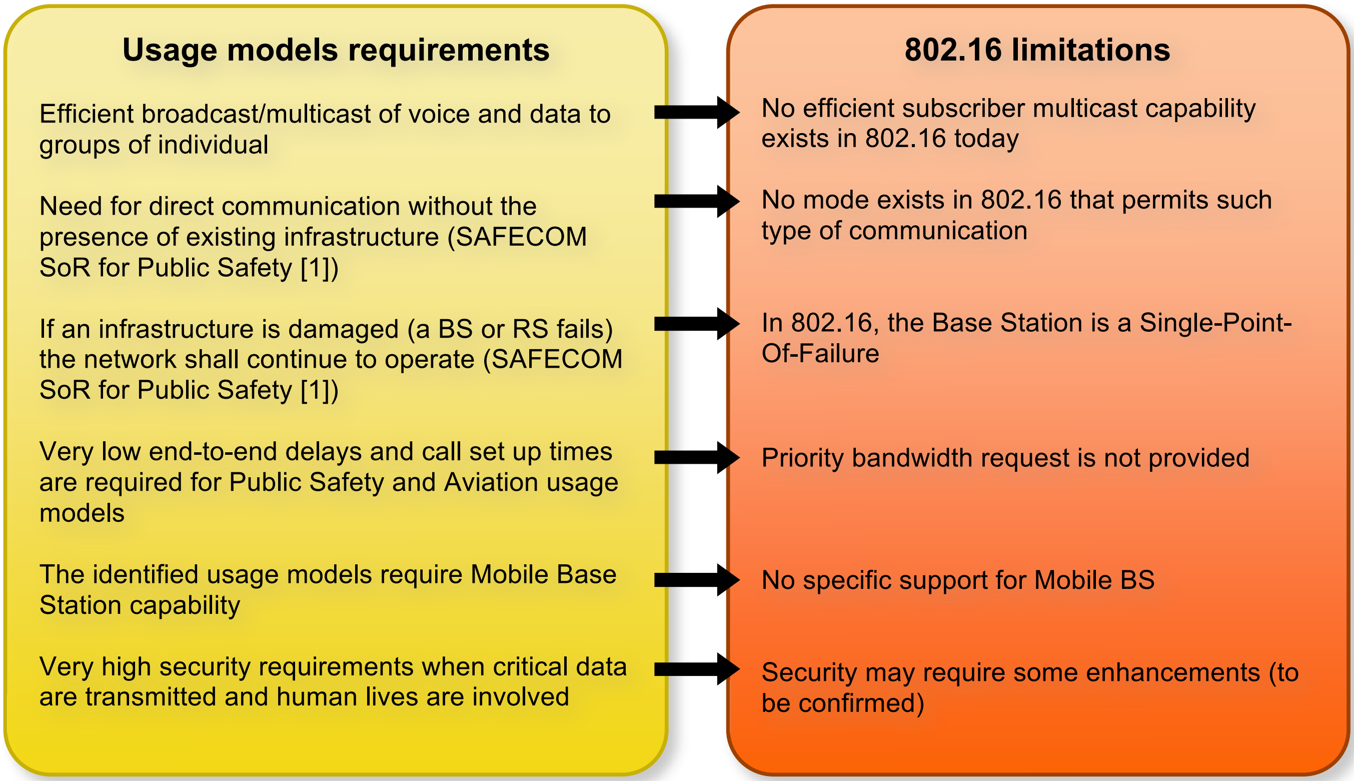
5.1.2 Medium Backward Compatibility

802.16j based MAC layer has offered a jump-start for the requirement of NRR. It is needed to mention that 802.16j is an good example for backward compatible PHY standard. NRR may follow the patter of 802.16j and offer further modification at MAC to achieve advanced relay.

Through the teleconference, it is recommended that fixed radio station is not very practical to support UAV based relay or airborne disaster recovery use cases. The group is exploring areas to be improved, beyond the existing 802.16 standard.

5.2 Preliminary set of requirements

The following figure presents a summary of the preliminary set of requirements and the associated limitations that have been identified in the 802.16 standards.



Usage models requirements

Efficient broadcast/multicast of voice and data to groups of individual

Need for direct communication without the presence of existing infrastructure (SAFECOM SoR for Public Safety [1])

If an infrastructure is damaged (a BS or RS fails) the network shall continue to operate (SAFECOM SoR for Public Safety [1])

Very low end-to-end delays and call set up times are required for Public Safety and Aviation usage models

The identified usage models require Mobile Base Station capability

Very high security requirements when critical data are transmitted and human lives are involved

802.16 limitations

No efficient subscriber multicast capability exists in 802.16 today

No mode exists in 802.16 that permits such type of communication

In 802.16, the Base Station is a Single-Point-Of-Failure

Priority bandwidth request is not provided

No specific support for Mobile BS

Security may require some enhancements (to be confirmed)

Figure 4: Preliminary set of requirements

5.3 Analyzed requirements

5.3.1 Resilience and Robustness

The objectives of (Network) Resilience and Robustness can be generalized throughout the whole document as the title of this WG ad hoc Committee. Here we attempt a definition applicable to 802.16 compatible systems.

In a commonly used term, Network Resilience and Robustness is a measurement of network fault tolerance. However, the term “fault” often leads to confusion. In a 802.16 like system (i.e. Metropolitan Area Fixed and Mobile Access Network), the following measurable are considered:

Physical Layer:

- Support control plane response to a sudden RF characteristics change (beyond typical channel fading due to multi-path/delay spread),
- Protection against RF interference, (intentional jammer or unintentional intra-system interference due to topology change),
- Prompt adjustment of physical layer parameters upon sudden mission or operation scenario modification.

MAC/Convergence Layer:

- Support higher-layer functionality to respond to a sudden node removal (intentional or unintentional),
- Support the capability of topology self-healing,
- Reconfigurability requirement for role reversal between stations,
- Protection against identification attack.

Management Plane:

- Support advanced access control (policy or attribute based authentication),
- Support higher security level including stronger identification protection and datagram encryption,
- Support promptly adjustment of protection level upon mission or operational scenario modification.

5.3.2 Reliability

Reliability is equal to high functionality availability. It is often achieved through the selections of least troublesome technology, hardware, or software. In 802.16-like applications, we consider reliability is achieved when:

From Service Offering Point of View:

- Enhance Quality of Service (QoS) (e.g. burst borrowing, flow management). In a packet network, reliability can be interpreted as the capability to maintain delay/jitter/loss per flow sustainable to provide meaningful connectivity or to maintain prior established service level agreement.
- Adjust QoS policy to distribute resource in an way to protect critical services.
- Avoid “single point failure”.

From Implementation Point of View:

- Allow the choice of operational frequency with RF characteristics easier to penetrate, less sensitive to dwelling/terrain blockage, and less sensitive to weather.
- Allow the choice of mature technology, component, or software.
- Provide high measurement in overall functional availability. (system-wide reliability is achieved by combining the reliability across all layers, any weak layer will jeopardize top level reliability measurement).
- Minimize the necessity of hard-to-find, hard-to-build, or hard-to-maintained component.
- Select technology with stronger tolerance to extreme environmental conditions (e.g. lower or higher temperature).
- Select technology with performance consistency over wider operational conditions (e.g. higher speed, longer range, or higher RF noise floor).

In summary, other than mean-time-between-failure (MTBF), reliability is difficult to measure by a quantitative approach. We offer the above qualitative design constraints for the ad-hoc WG to consider.

5.3.3 Security

The security functions must be able to provide subscribers and devices with assured privacy, authentication, and confidentiality within the 802.16nrr network. The intended protection should be for traffic and signaling/management messages.

The security architecture should specify the critical security components that can satisfy the following general security requirements:

- Encryption and Integrity Protection

  - Traffic encryption
  - Signaling/management message digital signature protection with encryption options
  - Cryptographic specifications for encryption
  - Cryptographic specifications for integrity protection
  - Key management and control

- Authentication and authorization management
- Subscriber and device authentication mechanism
  - Security Association(SA) establishment and management
  - Privacy Key Management (PKM) protocol control
  - User/device Identity Protection

It's also imperative to specify the enhanced security requirements that are practically applicable to the 802.16nrr systems that provide LMR-like features such as:

- Protection from PHY attack (Scrambling and Jamming)
- Signaling/management message (encryption) protection (encryption and integrity protection)
- MAC header protection (encryption and integrity protection)
- Group key management enhancement with secure and efficient key establishments and distribution
- Early authentication without possessing the credentials that can protect the association processes

The best practices of the security mechanism outlined here should be in accordance with the security specifications developed in both 802.16rev2 and 802.16m. The security architectures and authentication managements are both compatible with both standards in order to achieve the interoperability.

5.3.4 Spectrum

The bands of interest include: 4.4 – 5GHz, 5.091 – 5.15GHz, 5.2 – 5.4GHz, 5.4 – 5.7GHz, 5.7 – 5.8GHz, and 700 – 800MHz.

The consideration of government applications would lead to the following requirements:

- Extend frequency band consideration to government owned spectrum (e.g. the ISM bands) in addition to cellular services occupied licensed based
- Extend frequency bands consideration to sub-GHz spectrum (e.g. VHF or UHF) to support reliable RF characteristics with advantages in dwelling penetration and terrain following.
- Extend frequency bands consideration to both digitally modulated or non-licensed spectrum as licensed spectrum often have incumbent specific waveform specification excluding the possibility of considering 802.16e-like carrier.

In particular, for the NRR usage models sub-1GHz frequencies are desired for the following reasons:

- Better propagation in foliated and urban environments,
- Wider coverage,
- Lower power,
- More resistant to Doppler, i.e. higher mobility possible,
- More resistant to fading,
- Lower complexity RF Hardware.

FCC 08-230 covers the recent ruling with regard to spectrum set aside for public safety (see the following figure).

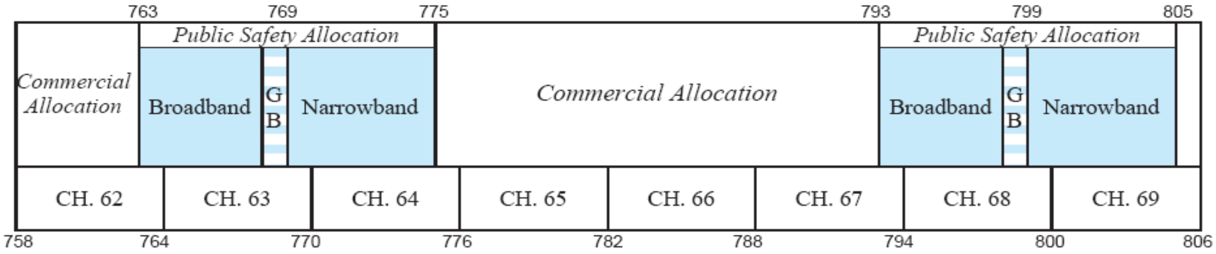


Figure 5: 758 – 806MHz frequency allocation in US

In FCC 08-230, the frequency band plan breaks the spectrum into 2 Lower Bands for broadband use (763-768 & 793-798 MHz) as well 2 Upper Bands for narrowband use (769-775 & 799-805). 802.16nrr should target technology for the Lower Bands of the 700Mhz.

In addition to the Lower Bands, there is a commercial allocation from 775-793 MHz. FCC 08-230 states that 10MHz from the 2 Lower Bands and up to 10 MHz in the commercial allocation can be "pooled" together to form one (logical) 20MHz.

To date, there are no owners of this commercial allocation. FCC 08-230 (paragraph 86) classifies seven types of incidents in which, up to 14% of the 20MHz block must be shared with public safety.

For the commercial allocation, the FCC also states (paragraphs 231-248 of 08-230) that "dynamic spectrum management" techniques can be used. The cognitive capabilities being developed with 802.16h or possibly 802.22 could be used.

In the 700MHz public safety bands, FCC is expecting that technology can support the following:

- 1Mbps DL/600kbps UL through put on average
- minimum 256 Kbps to cell-edge for urban users
- minimum 128 Kbps to cell-edge for rural users
- minimum 64 Kbps for nodes on the move
- be up 99.6% of the time

In the ruling, 08-230, the FCC expects that technologies like 802.16 can be used to meet those needs. The FCC has also ruled on 4.9GHz bands for public safety, FCC 02-47. FCC 02-47 is an older document that does not consider 802.16 technology.

Operation in public safety bands could be met without significant MAC or PHY modifications. This requires that profiles for 700 MHz or 4.9GHz hardware. Currently, no such profiles are under development.

5.3.5 Very high speed mobility

In the usage model of border surveillance the radio link will be required to support fixed and mobile ground based communications linking in to unmanned aerial vehicles with cameras and other sensor payloads. Direct UAV to UAV communications will also be required to provide such things as data sharing and range extension to ground based users. The radio link must therefore operate with the maximum likely UAV closing speed which is believed to be in the range of 400 km/h to 1400 km/h.

5.3.6 Support for dynamic group management

To provide the service similar to LMR group call, 802.16 needs to have a) push to talk with encryption capability, b) multicast and broadcast service with encryption option, and c) priority and pre-emption.

5.3.7 Increased Range

Several public safety use cases (e.g. border patrol and surveillance for a large area with low density of users) require the 802.16 communication range to be larger than the typical range.

The system needs to have ranges in excess of 200 km to support air to air and air to ground operations.

5.3.8 Mobile Base Stations

The UAV surveillance scenario and Public Safety applications require the 802.16 communication to support mobile base stations.

The high-level technical issues for mobile base station include: the mobile base stations must coordinate with each other (in a secure way) such that there is no gap on the coverage, interference is properly managed and handoff region is properly maintained.

5.3.9 Enhanced Relay Operation

In addition to the features provided by IEEE 802.16j, the following enhancements are required:

- Enable redundant routes from the BS and subscribers using relays.
- Relays can be on the move (using vehicle, UAV, or manpack), on the halt or stationary. For relay mobility, the handover between relays needs to be supported.
- The system needs to support direct communications between relays for direct forwarding, that is to say, mobile can communicate with another mobile via relays for data communications (without going through the BS); however, signaling would still need to go through the BS.
- Enable dynamic role reversal between subscriber and relay.
- The system should allow remote configuration of all relays and over the air keying/re-keying.

Focusing on the local forwarding aspect, the following enhancements are required:

- Relay should coexist with the DSRC device,
- Enable ad-hoc connections between vehicle and vehicle.
- Enable redundant connections for vehicles with the DSRC devices,
- Relays should guaranty any vehicle-to-infrastructure-to-vehicle safety message relaying,
- Relays should minimize vehicle-to-infrastructure-to-vehicle safety message relaying,
- Relays should be capable to handle mass vehicles communications (e.g. in the road intersection of a urban area).

5.3.10 Coexistence with DSRC

DSRC (Dedicated Short Range Communication) are one-way or two-way short-to-medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards. It offers communication between the vehicle and roadside equipment. IEEE 802.11p will be used as the groundwork for DSRC.

The IEEE 802.16 system should coexist with the DSRC devices. Possible applications for combing 802.16 and DSRC (such as IEEE 802.11p) technologies are:

- Emergency warning system for vehicles,
- Cooperative Adaptive Cruise Control,
- Cooperative Forward Collision Warning,

- Intersection collision avoidance,
- Approaching emergency vehicle warning,
- Vehicle safety inspection,
- Transit or emergency vehicle signal priority,
- Electronic parking payments,
- Commercial vehicle clearance and safety inspections,
- In-vehicle signing,
- Rollover warning,
- Probe data collection,
- Highway-rail intersection warning,
- Road condition warning,
- Imminent collision warning,
- Green light – optimal speed advisory.

5.4 Identified requirements of interest

At the 802.16 session #60, the NRR ad hoc Committee has identified the following requirements of interest for further studies. They are associated with a priority levels, 1 being the higher priority and 2 the least priority.

- Enhanced relay operation (Level 1),
- Direct communication mode (Level 1),
- Priority bandwidth request (Level 1),
- Non-standard channel behaviors (Level 1),
- Enhanced security (Level 2),
- Dynamic reconfigurability (Level 2),
- Mobile BS (Level 2),
- Group management (Level 2).

6 Proposed Project Requirements

The NRR Ad-Hoc committee has agreed to study the following Project Requirements:

- **Ability to operate without an attached infrastructure,**
- **Local forwarding by relay stations (MS-RS-MS),**
- **Capability of dynamic self reconfiguration,**
- **End-to-end path redundancy,**
- **Enhancement to Mobile Relay Station,**
- **Security enhancement as required by above features**

6.1 Smart Relay technical approach

A Smart Relay Station (SRS) is a feature enhanced relay station (RS) which has supplementary functions, allowing the system to be more resilient and more reliable. In this context a Smart Relay station may provide the following features in addition to those already provided by 802.16j.

----------- Future text added here pending on continuing work of 80216nrr-09_028r2.doc and discussion of 80216nrr-09_029.ppt ------.

7 Conclusion