4.9 GHz Work Group Guidelines

Metropolitan, New York City Area
New York, New Jersey
FCC Region 8 700-MHz
4.9 GHz Work Group

May 2011
## Table of Contents

1. **OVERVIEW OF FCC REGION 8 4.9-GHZ REGIONAL GUIDELINES** ................................................. 1

2. **REGION 8 4.9GHZ WORK GROUP COMMITTEE** ........................................................................ 2

3. **FCC REGIONAL PLANNING COMMITTEE (RPC) REGION 8 4.9-GHZ REGIONAL DESCRIPTION** ... 3

   3.1 New York ........................................................................................................................................ 3

   3.2 New Jersey ...................................................................................................................................... 5

4. **WORK GROUP MEETINGS – AND NOTIFICATION PROCESS** ................................................... 8

5. **INTEROPERABILITY PROCEDURES AND REQUIREMENTS** ....................................................... 9

   5.1 Introduction ................................................................................................................................. 9

   5.2 Broadband Operations Pyramid ............................................................................................... 10

   5.3 Broadband Interoperability Requirements .............................................................................. 12

      5.3.1 Broadband and Wideband Interoperability Applications ................................................. 12

      5.3.2 Avenues for Achieving Operations-Level Interoperability ................................................... 13

      5.3.3 Avenues for Achieving Mutual Municipal and Regional Operations Interoperability ........... 13

      5.3.4 Avenues for Achieving Disaster and National Mutual Aid Operations Interoperability ....... 13

6. **DATA APPLICATIONS** ............................................................................................................. 15

    6.1 Introduction ............................................................................................................................... 15

    6.2 Region 8’s 4.9-GHZ APPLICATIONS & APPLICATION SECURITY ............................................. 15

       6.2.1 GHz Public Safety Applications ......................................................................................... 15

       6.2.2 Wireless Application Security .......................................................................................... 18

7. **PROCEDURES ON DEALING WITH ADJACENT AND OVERLAPPING JURISDICTIONS** ...... 26

    7.1 Adjacent Regional Coordination ............................................................................................ 26

    7.2 Dispute Resolution .................................................................................................................. 27

    7.3 Incident Commanders ............................................................................................................. 27

    7.4 Procedure for Regional Frequency Coordination ..................................................................... 28

    7.5 Interference Avoidance ............................................................................................................ 29

    7.6 Protection of Incumbent Adjacent and Co-Channel Users ...................................................... 29

       7.6.1 US Navy ............................................................................................................................ 29

       7.6.2 Radio Astronomy .............................................................................................................. 30

       7.6.3 Aviation (Requires an FCC Waiver) ................................................................................ 31

8. **REGIONAL SPECTRUM UTILIZATION** ..................................................................................... 33

**APPENDIX A, 4.9-GHZ WORK GROUP MEMBERS** ................................................................. 1

**APPENDIX B, RELEVANT STANDARDS AND TECHNOLOGY IN THE 4.9-GHZ BAND FOR PUBLIC SAFETY USE** .............................................................................................................. 1

Overview .............................................................................................................................................. 1

Introduction, The 4.9-GHZ Licensed Spectrum for Public Safety ..................................................... 1

The 4.9-GHz Spectrum Parameters ..................................................................................................... 2

   Power Levels ...................................................................................................................................... 2

   Channelization ................................................................................................................................... 2

Possible Coverage Scenarios ................................................................................................................ 8

Air Interface Standards ....................................................................................................................... 11

IEEE 802.11 – 802.20, Wireless Access Standards Suite .................................................................. 11

   Comparison of Characteristics Specified within the IEEE 802.11 Suite ......................................... 13
4.9-GHz Work Group Guidelines

IEEE 802. 15 -22 Standards, Spectrum, Throughput, Licensing, Availability ................................................................. 14
IEEE 802.11 Standard (aka ISO/IEC 8802-11-1999) ........................................................................................................ 15
802.11a ........................................................................................................................................................................ 15
802.11b ........................................................................................................................................................................ 15
802.11g ........................................................................................................................................................................ 15
802.11i ........................................................................................................................................................................ 16
802.11j ........................................................................................................................................................................ 16
802.11n ........................................................................................................................................................................ 16
802.11p, Wireless Access in Vehicular Environment WAVE (DSRC) ........................................................................ 17
802.11T - Wireless Performance Prediction (Recommended Practice) ...................................................................... 17
802.15 ........................................................................................................................................................................ 17
802.16 ........................................................................................................................................................................ 18
802.18 ........................................................................................................................................................................ 18
802.19 ........................................................................................................................................................................ 18
802.20 ........................................................................................................................................................................ 18
802.21, Handoff/Interoperability Between Networks ................................................................................................... 19
802.22, Cognitive Wireless Regional Area Networks .................................................................................................. 19
ISO/IEC WIRELESS JPEG 2000 (JPWL, JPEG WIRELESS) .......................................................................................... 20
4.9 GHZ, CCTV TECHNOLOGY APPLICATION ......................................................................................................... 20
POTENTIAL VENDORS CAPABILITIES FOR 4.9 GHZ ................................................................................................. 21
Motorola’s line of point-to-point (PTP) and point-to-multipoint (PMP) operate in the 4.9 GHz, in a line-of-site
and non-line-of-sight environments, over long distances, and across water and open terrain. The radios
overcome the key degrading factors in all radio environments – signal attenuation, fading, dispersion and
polarization taking advantage of the following radio technologies to maintain link reliability: ................................................................................................. 21
Antennas type example for 4.9 GHz ............................................................................................................................. 22
APPENDIX C ACRONYMS .................................................................................................................................. 25

List of Figures

Figure 1, Map of Region 8 Counties (New York and New Jersey) .................................................................................. 3
Figure 2, New York Counties in the 700-MHz 4.9-GHz Coverage Area (from U.S. 2000 Census) ........................................ 5
Figure 3, New Jersey Counties in the 700-MHz 4.9-GHz Coverage Area (from U.S. 2000 Census) .................................... 7
Figure 4, Operations Pyramid ...................................................................................................................................... 12
Figure 5, 4.9-GHz L and M Masks ............................................................................................................................... 7
Figure 7, Channelization Coverage from Two Adjacent APS, both with 10 MHz Channels, 2 5-MHz Channels,
and 10 2-MHz Channels, and 10 1-MHz Channels .................................................................................................. 10
List of Tables

Table 1, Counties Listed by Population in New York (based on U.S. 2000 Census) ................................................... 4
Table 2, Counties Listed by Population in New Jersey (based on U.S. 2000 Census) ................................................. 6
Table 3, Application Priority Levels for Use in the 4.9-GHz Band................................................................. 16
Table 4, Applications Matrix......................................................................................................................... 17
Table 5, Security Methods to be Employed ................................................................................................. 24
Table 6, Security Levels and Associated Controls .................................................................................. 25
Table 7, Possible Channel Allocations for Region .................................................................................... 33
Table 8, List of FCC Region 8 700-MHz 4.9-GHZ Work Group Members ................................................................. 1
Table 9, IEEE 802.11 Standards, Spectrum, Throughput, Licensing, and Availability ............................ 11
Table 10, Characteristics Specified within the IEEE 802.11 Suite ............................................................... 13
Table 11, IEEE 802.15 -.22 Standards, Spectrum, Throughput, Licensing, and Availability ..................... 14
Table 12, 5-GHz Band Characteristics ...................................................................................................... 21
1. OVERVIEW OF FCC REGION 8 4.9-GHZ REGIONAL GUIDELINES

The Region 8 700-MHz Regional Planning Committee chartered its 4.9-GHz Work Group to meet the FCC’s request for a regionally created set of 4.9-GHz Regional Guidelines. From the 2003 Memorandum Opinion and Order (MO&O) of WTB Docket 00-32:

Within twelve months of the effective date of the rules adopted herein, each Regional Planning Committee (RPC) shall provide the FCC with a copy of its plan. The plan should identify coordination procedures for both fixed and mobile operations, including but not limited to, mechanisms for incident management protocols, interference avoidance and interoperability. We envision that such plan could be done either on a regional basis or on a national basis through industry formulation of a best practices coordination plan. We also believe that any coordination plan for the 4.9 GHz band should contain express procedures affording specific flexibility to accommodate dynamic spectrum utilization in response to immediate public safety communications needs.

We believe that the combination of our frequency utilization plan and use of the RPCs as described above will facilitate effective coordination of operations in the band. We note that planning committees may do very well in urban areas where there are numerous public safety jurisdictions within a given area, whereas in rural areas, where there is further distance between public safety jurisdictions, less formal procedures may accomplish the same coordination goals. Additionally, with regard to emergency and incident scenes, we expect that RPCs will establish procedures to allow an incident commander to take control of emergency operations, including communications issues, consistent with procedures established by adjacent and overlapping jurisdictions.

This document represents the revisions necessary to reflect recent FCC rule changes and apply lessons learned from various regional deployments. However, as the 4.9-GHz band is still relatively a new allocation, and broadband data utilization is being looked at more and more for public safety use, we expect that these Guidelines will continue to be a living document, one that will periodically change and evolve as more deployments are made in the 4.9GHz band.

This document is arranged into 8 sections and three appendices. Section 1 gives an outline of the 4.9-GHz Regional Guidelines. Section 2 re-introduces the Committee and captures changes made to its membership. Section 3 describes the geography and demographics of the Region. Section 4 describes the Work Group’s meetings, participation, and notification processes. Section 5 describes the Region’s Interoperability Procedures and Requirements. Section 6 addresses and documents the Region’s identified data applications, along with their security, operational, and deployment parameters. Section 7 addresses regional spectrum management and interference mitigation procedures, including guidelines for dealing with overlapping and adjacent jurisdictions. Finally, Section 8 presents guidelines for regional spectrum utilization, including the definition of a regional band plan.

Additional information is provided in Appendices, including, in Appendix A, the list of the 4.9GHz Work Group members and, in Appendix B, documentation of the Work Group’s examination of technologies that may prove to be suitable for 4.9GHz operations support. Appendix C defines acronyms used in this document.
2. **REGION 8 4.9GHz WORK GROUP COMMITTEE**

The FCC Region 8 700-MHz 4.9-GHz Work Group Committee covers the following counties in New York: Bronx, Dutchess, Kings, Nassau, New York, Orange, Putnam, Queens, Richmond, Rockland, Suffolk, Sullivan, Ulster, and Westchester Counties. In New Jersey, it covers the following counties: Bergen, Essex, Hudson, Hunterdon, Mercer, Middlesex, Monmouth, Morris, Passaic, Somerset, Sussex, Union, and Warren.

The FCC Regional Planning Committee (RPC) Region 8 founded the 4.9-GHz Work Group on September 10, 2003. The FCC Regional Planning Committee (RPC) Region 8 4.9-GHz Work Group Committee is comprised of Local, State, Tribal, and Municipal representatives. Private industries also are represented on the Committee. The 4.9-GHz Work Group’s chairperson was elected on September 10, 2003. The 4.9-GHz Work Group Committee Officers are:

- **Chairperson**  Felix Melendez  
  Director  
  Citywide Radio Network Operations and FCC Licensing Support  
  City of New York  
  Dept. of Information Technology and Telecommunications  
  Telephone: (718) 403-8278  
  Fax: (718) 403-8220  
  Email: FMelendez@doitt.nyc.gov

- **Vice-Chairperson**  Vacant

- **Secretary**  Vacant

The FCC RPC Region 8 700-MHz 4.9-GHz Work Group Committee membership list appears in Table 8 in Appendix A.
3. **FCC REGIONAL PLANNING COMMITTEE (RPC) REGION 8 4.9-GHZ REGIONAL DESCRIPTION**

A geographical region is a specified district or territory. The FCC Regional Planning Committee (RPC) Region 8 4.9-GHz Work Group region covers counties in New York and New Jersey. Figure 1 shows the FCC Region 8 counties.

![Figure 1, Map of Region 8 Counties (New York and New Jersey)](image)

### 3.1 New York

The FCC Regional Planning Committee (RPC) 700-MHz 4.9-GHz Work Group covers areas in New Jersey and New York. The areas covered in New York include the following counties: Bronx, Dutchess, Kings, Nassau, New York, Orange, Putnam, Queens, Richmond, Rockland, Suffolk, Sullivan, Ulster, and Westchester Counties.

Table 1 lists the populations of the counties based on U.S. census for 2000. Figure 2 shows the percentages of the total Region 8 portion of New York State population by New York State counties. The total population of New York is listed as 18,976,457. The total population of the counties in Region 8 is 12,941,380. The percentages are calculated based on the counties in Region 8.
### Table 1, Counties Listed by Population in New York (based on U.S. 2000 Census)

<table>
<thead>
<tr>
<th>Geographic area</th>
<th>Population</th>
<th>Area in square miles</th>
<th>Density per square mile of land area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>Water</td>
</tr>
<tr>
<td>New York</td>
<td>18,976,457</td>
<td>54,556.00</td>
<td>7,342.22</td>
</tr>
<tr>
<td>Region 8 Counties</td>
<td>12,941,380</td>
<td>8,062.24</td>
<td>2,007.58</td>
</tr>
<tr>
<td>Counties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bronx County</td>
<td>1,332,650</td>
<td>57.43</td>
<td>15.4</td>
</tr>
<tr>
<td>Dutchess County</td>
<td>280,150</td>
<td>825.38</td>
<td>23.78</td>
</tr>
<tr>
<td>Kings County</td>
<td>2,465,326</td>
<td>96.90</td>
<td>26.29</td>
</tr>
<tr>
<td>Nassau County</td>
<td>1,334,544</td>
<td>453.08</td>
<td>166.39</td>
</tr>
<tr>
<td>New York County</td>
<td>1,537,195</td>
<td>33.77</td>
<td>10.81</td>
</tr>
<tr>
<td>Orange County</td>
<td>341,367</td>
<td>838.55</td>
<td>22.21</td>
</tr>
<tr>
<td>Putnam County</td>
<td>95,745</td>
<td>246.25</td>
<td>14.97</td>
</tr>
<tr>
<td>Queens County</td>
<td>2,229,379</td>
<td>178.28</td>
<td>69.04</td>
</tr>
<tr>
<td>Richmond County</td>
<td>443,728</td>
<td>102.5</td>
<td>44.02</td>
</tr>
<tr>
<td>Rockland County</td>
<td>286,753</td>
<td>199.34</td>
<td>25.12</td>
</tr>
<tr>
<td>Suffolk County</td>
<td>1,419,369</td>
<td>2,373.07</td>
<td>1,460.87</td>
</tr>
<tr>
<td>Sullivan County</td>
<td>73,966</td>
<td>996.85</td>
<td>27.14</td>
</tr>
<tr>
<td>Ulster County</td>
<td>177,749</td>
<td>1,160.76</td>
<td>34.28</td>
</tr>
<tr>
<td>Westchester County</td>
<td>923,459</td>
<td>500.08</td>
<td>67.26</td>
</tr>
</tbody>
</table>

[http://factfinder.census.gov/servlet/GCTTable?_bm=y&-geo_id=04000US36&-_box_head_nbr=GCT-PH1&-ds_name=DEC_2000_SF1_U&-format=ST-2](http://factfinder.census.gov/servlet/GCTTable?_bm=y&-geo_id=04000US36&-_box_head_nbr=GCT-PH1&-ds_name=DEC_2000_SF1_U&-format=ST-2)
Figure 2 shows New York Counties listed by name, population, and the corresponding percentages of the total population in the Region 8 portion of New York State.

Figure 2, New York Counties in the 700-MHz 4.9-GHz Coverage Area (from U.S. 2000 Census)

3.2 New Jersey

The FCC Regional Planning Committee (RPC) 700-MHz 4.9-GHz Work Group covers areas in New Jersey and New York. The areas covered in New Jersey include the following counties: Bergen, Essex, Hudson, Hunterdon, Mercer, Middlesex, Monmouth, Morris, Passaic, Somerset, Sussex, Union, and Warren.

Table 2 lists the populations of the counties based on U.S. census for 2000. Figure 3 shows the percentages of the total Region 8 portion of New Jersey State population by New Jersey counties.
Counties. The total population of New Jersey is listed as 8,414,350. The total population of counties in Region 8 is 6,150,834. The percentages are calculated based on counties in Region 8.

Table 2, Counties Listed by Population in New Jersey (based on U.S. 2000 Census)

<table>
<thead>
<tr>
<th>County</th>
<th>Population</th>
<th>Area in square miles</th>
<th>Density per square mile of land area</th>
<th>Housing Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>Water</td>
<td>Land</td>
</tr>
<tr>
<td>New Jersey</td>
<td>8414350</td>
<td>8721.3</td>
<td>1303.96</td>
<td>7417.34</td>
</tr>
<tr>
<td>Region 8</td>
<td>6150834</td>
<td>4080.61</td>
<td>294.56</td>
<td>3786.05</td>
</tr>
<tr>
<td>Bergen County</td>
<td>884118</td>
<td>246.8</td>
<td>12.63</td>
<td>234.17</td>
</tr>
<tr>
<td>Essex County</td>
<td>793633</td>
<td>129.56</td>
<td>3.29</td>
<td>126.27</td>
</tr>
<tr>
<td>Hudson County</td>
<td>608975</td>
<td>62.43</td>
<td>15.74</td>
<td>46.69</td>
</tr>
<tr>
<td>Hunterdon County</td>
<td>121989</td>
<td>437.76</td>
<td>7.82</td>
<td>429.94</td>
</tr>
<tr>
<td>Mercer County</td>
<td>350761</td>
<td>228.84</td>
<td>2.91</td>
<td>225.93</td>
</tr>
<tr>
<td>Middlesex County</td>
<td>750162</td>
<td>322.51</td>
<td>12.79</td>
<td>309.72</td>
</tr>
<tr>
<td>Monmouth County</td>
<td>615301</td>
<td>665.12</td>
<td>193.18</td>
<td>471.94</td>
</tr>
<tr>
<td>Morris County</td>
<td>470212</td>
<td>481.29</td>
<td>12.29</td>
<td>468.99</td>
</tr>
<tr>
<td>Passaic County</td>
<td>489049</td>
<td>197.05</td>
<td>11.76</td>
<td>185.29</td>
</tr>
<tr>
<td>Somerset County</td>
<td>297490</td>
<td>305.05</td>
<td>0.36</td>
<td>304.69</td>
</tr>
<tr>
<td>Sussex County</td>
<td>144166</td>
<td>535.99</td>
<td>14.73</td>
<td>521.26</td>
</tr>
<tr>
<td>Union County</td>
<td>522541</td>
<td>105.46</td>
<td>2.17</td>
<td>103.29</td>
</tr>
<tr>
<td>Warren County</td>
<td>102437</td>
<td>362.75</td>
<td>4.89</td>
<td>357.87</td>
</tr>
</tbody>
</table>

http://factfinder.census.gov/servlet/GCTTable?_bm=y&-geo_id=04000US34&-_box_head_nbr=GCT-PH1&_ds_name=DEC_2000_SF1_U&-redoLog=false&_mt_name=DEC_2000_SF1_U_GCTPH1_ST2&_format=ST-2
Figure 3, New Jersey Counties in the 700-MHz 4.9-GHz Coverage Area (from U.S. 2000 Census)
4. **Work Group Meetings – and Notification Process**

Meetings of the FCC Region 8 700-MHz 4.9-GHz Work Group are limited to the work group and are not opened to the public. However, the 4.9-GHz Work Group presents all the findings or conclusions of its meetings to the ‘parent’ Regional Planning Committee (RPC) Region 8 700-MHz, which is open to the public.

The FCC Region 8 700-MHz 4.9-GHz Work Group members receive meeting notifications via e-mails. Meeting dates are tentatively scheduled at the end of the meeting. If there is a scheduling conflict, members are notified of the change via e-mail or via telephone.

All the 4.9-GHz Work Group meeting minutes are recorded, and they include comments from participants. The meeting minutes are provided to members at the beginning of the next meeting to verify that the information provided is accurate and reflects the general themes that were covered at the previous meeting. Members have to vote to accept the meeting minutes, and vote to amend the meeting minutes, if appropriate.

The 4.9-GHz Work Group has held more than 15 meetings/teleconferences between December 2003 and May 2005 with the group members in the process of developing these guidelines. All agendas and meeting minutes are available upon request.
5. **INTEROPERABILITY PROCEDURES AND REQUIREMENTS**

5.1 **Introduction**

The purpose of this document is to illustrate the wideband and broadband interoperability needs of Public Safety Agencies comprising the FCC Region 8 — the Metropolitan New York City area. Here wideband refers to effective data rates between 50 kbps and 1Mbps, and broadband refers to rates at greater than 1Mbps. Within this document, they are treated together in terms of user applications and requirements.

This document also presents a high-level view of how these wideband/broadband interoperability needs can be addressed within the Region. The Region’s definition of Data Interoperability is as specified in the box that follows.

<table>
<thead>
<tr>
<th>Definition of Data Interoperability:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Interoperability is <em>the ability to communicate specific data information with whom you need to and when you need to</em> — <em>not</em> the ability to communicate “all” information with everyone all the time.</td>
</tr>
</tbody>
</table>

Note that interoperability encompasses many areas of communications, and is best implemented through a comprehensive plan. This plan shall identify who needs to communicate with whom, what information is to be communicated, and how the communications will occur. With respect to data communications, the “how” must address both how the actual communications channel is created, as well as how the data that is communicated is translated into useful information for all of the involved parties.

Through the examination of the Region’s wideband/broadband interoperability needs, some high-level observations have been made.

Across the country, data interoperability requirements may not be consistent with our definition. Our Committee has worked diligently on identifying and characterizing our broadband applications — in our view, few if any, require interoperability that cannot be achieved at a network level.

A mandated interoperability mode in every 4.9-GHz radio will increase the cost of equipment — especially if such a standard deviates from existing global standards, as TIA appears to be doing. Furthermore, we clearly do not know enough about these types of operations to make a decision to constrain all 4.9-GHz equipment. It is also clear that, across the country, nearly all of public safety’s 4.9-GHz requirements change due to operational, geographic, demographic, and financial considerations. With such anisotropic needs, a “one size fits all” approach is ludicrous. It is far more effective to have an effective interoperability plan, one that is both tailored for and trained to, and one designed with regards to each Region’s specific needs.

Physical layer (PHY) standardization as a means to achieve interoperability is an ancient approach and one whose benefits for data are not even well understood. A more modern and practical technique would be to approach interoperability at the network and applications layers. This type of approach is what has led to the massive growth of the Internet — the largest interoperable network in the world, which does not rely on PHY standards whatsoever.
4.9-GHz Work Group Guidelines

No interoperability can ever be achieved unless applications are interoperable and the relevant IT networks are connected. Starting at the applications layer and working down to an IP connection can provide complete interoperability. Starting at the PHY and working up only provides data interoperability once the applications themselves are standardized.

An example of this is the Project 25 voice standard. The common air interface defined in this suite only provides voice interoperability because the voice application (the Vocoder) itself is standardized. When you target data, there are many, many interoperability applications that will need to be standardized, and at this point, none of them is even defined.

5.2 Broadband Operations Pyramid

In order to balance priority and quality of service metrics, Region 8 has expended considerable effort to define the broadband/wideband applications that will be utilized within the Region. Through this process, it was found that most broadband applications are for the support of day-to-day agency operations — not for interoperability. The Region believes that, with respect to wideband/broadband data, it is counterproductive to place a heavy emphasis upon interoperability, since it is clear that the advanced-technology capabilities and force-multiplier aspects of broadband are becoming more important to mission support. Transferring data to and from the field is likely to prove to be the most effective communications tool for homeland security, and to support the primary mission (protection of life and property).

This is not to say that data interoperability is not important. It simply implies that the main interoperability application is voice, which is mostly irrelevant to data communications. This is mainly due to first responders being most effective at performing their duties when they do not have to take their eyes off the mission objectives. Therefore, for the vast majority of first responders, aural cues and voice communications are the most effective means to convey information in an incident that requires interoperability. There is a subset of first responders that will require data interoperability at an incident, but mainly the incident commanders, who require the high information levels in order to provide direction, command, and control of the incident scene. With regards to voice and data interoperability, it is simply a matter of selecting the best tool for the job.

Fig 4 illustrates the Region’s consensus regarding the relative magnitudes of the various categories of operations involving data communications and data interoperability. In the lower portion of the pyramid in this figure, it is shown that the “Operations” level holds the vast majority of data applications, and its benefits apply to day-to-day operational support. At this level, the mobile data applications provide support for the primary mission: protection of life and property. This represents most of the cases and benefits of wideband/broadband data. It offers an immediate force-multiplier effect, and opens access to high-rate bidirectional data flow to and from the field. We feel that it is in these day-to-day operations that the most effective homeland security support operations occur.

Higher up in the pyramid in Figure 4 is the “Mutual Operations” layer. It is in this layer that a very small fraction (<1%) of data applications and cases require direct agency-to-agency transfer of data. In order to produce an effect on his communications interoperability, it will be necessary to have interoperable IT networks, as well as end-user applications to translate the data transferred. It does not necessarily require direct physical-layer interoperability, and can be easily accommodated through network and IP interconnections.
The highest level in the pyramid, the “Disaster” layer, represents the smallest number of cases and applications. This represents applications necessary to support operations at an incident affecting or threatening large-scale loss of property and life. In these scenarios, the Region recognizes the need to maintain an incident command and control structure, and that this will require not only broadband/wideband data transfer between incident commanders on scene, but also command and control of the wideband/broadband spectrum resources at the scene. With respect to 4.9 GHz, Interoperability should be effectively implemented through a detailed planning process and its associated training. The utilization of the broadband/wideband spectrum at the scene should be limited to the applications supporting the critical-incident command and control communications structure. Seamless roaming of “interoperable” wideband units may actually hinder the ability of the first responders and incident commanders to perform their duties at the scene. Again, in order to provide this communications interoperability, it will be necessary to have interoperable IT networks, as well as end-user applications to translate the data transferred. It will not necessarily require direct physical-layer interoperability, and in nearly all cases can be accommodated through network and IP interconnections.

When operating directly on-scene of a Disaster-level incident, the Region Prefer to keep operational control of Wireless and IT systems; and to let agency commanders assign appropriate equipment, authentication/passwords, etc. to the appropriate individuals. The region has documented few if any cases in which direct-mode off-network data transfer between the incident commanders (or first responders) on scene is required. In such instances, the Region feels that a cache of data devices with known authentication parameters and MAC address should be retained to distribute to the appropriate on-scene personnel. This will enable the Region to react to an infusion of outside assistance in such situations, while maintaining a secure and spectrally pure command and control-operating environment.

---

1 This is consistent with the Region’s efforts to define relative Quality-of-Service (QoS) metrics for broadband/wideband applications in order to develop bandwidth applications/priority guidelines.
5.3 Broadband Interoperability Requirements

This section will introduce the Region’s broadband and data interoperability requirements, as well as discuss and detail avenues for achieving and supporting these requirements.

5.3.1 Broadband and Wideband Interoperability Applications

In column 5 of the Regional Data Applications Matrix Table (Table 4), three possible levels of the highest level of required Interoperability/Operations are specified for all significant data applications that were identified. They are as follows:

O: “Operations-Layer” holds the vast majority of data applications, and its benefits apply to day-to-day operational support. Technology application here brings substantial force-multiplier effects. As indicated previously, most public safety and homeland security operations fall within this category (~ 99% of operations).

M: “Mutual Operations” layer, in which a very small fraction (<1%) of data applications and cases require direct agency-to-agency transfer of data.

An “M” in this category also implies that most operations are at “O”, with a very small percentage at “M”.

Figure 4, Operations Pyramid

- ~0.01%
- <1%
- ~99%
4.9-GHz Work Group Guidelines

D: “Disaster” layer represents the smallest number of cases and applications. This represents applications necessary to support operations at an incident affecting or threatening large-scale loss of property and life. In these scenarios, the Region recognizes the need to maintain an incident command and control structure, and that this will require not only broadband/wideband data transfer between incident commanders on scene, but also command and control of the wideband/broadband spectrum resources at the scene.

A “D” in this category also implies that most operations are at “O”, with a very small percentage at “M”, and even smaller percentage at “D”.

5.3.2 Avenues for Achieving Operations-Level Interoperability

Public safety Operations Level applications require no stressing interoperability configuration, as users will either fall on the same system, or on another IP-interconnected system. However, any effective data interchange between users will require that data applications are interoperable, or have a defined transcending interpreter. Operations typically involve data communications between users from same agency.

There are many ways to achieve Operations Level Interoperability within the Region, and all that is really required are a connection to the mobile IT/IP networks and data applications that can effectively inter-work. PHY-level standardization is not even required, as data consumers and providers can connect to the mobile IT/IP network through any wireless or wired connection points, e.g. Ethernet, 700 MHz, 2.4 GHz, 4.9 GHz, UNIII, and 5.9 GHz DSRC (Dedicated Short-Range Communications).

5.3.3 Avenues for Achieving Mutual Municipal and Regional Operations Interoperability

Public safety Mutual Municipal and Regional Operations Interoperability Level applications also require no stressing interoperability configuration, as users will either fall on the same system or be on another IP-interconnected system. Again, any effective data interchange between users will require that data applications are interoperable, or have a defined transcending interpreter. Operations typically involve data communications between users from different agencies, with the actual data transferred being a small subset of each individual agency’s Operations-level data.

There are many ways to achieve Mutual Municipal and Regional Operations Level Interoperability within the Region, and again all that is required are a connection to the mobile IT/IP networks and data applications that can effectively inter-work. PHY-level standardization is not even required, as data consumers and providers can connect to the mobile IT/IP network through any wireless or wired connection points, e.g. Ethernet, 700 MHz, 2.4 GHz, 4.9 GHz, UNIII and 5.9 GHz DSRC. In this case, however, there must be also network IT/IP interconnectivity to each agency’s network systems in order to authenticate users and share data objects.

5.3.4 Avenues for Achieving Disaster and National Mutual Aid Operations Interoperability

The Region’s public safety Disaster and National Mutual Aid Operations Interoperability Level applications also require no stressing interoperability configuration, as users will either fall on the same system or on another IP-interconnected system. Again, any effective data interchange between users will require that data applications are interoperable, or have a defined
transcending interpreter. Operations typically involve data communications between commanders from different agencies, with the actual data transferred being a small subset of each individual agency’s Operations and Mutual Aid level data.

There are many ways to achieve Disaster and National Mutual Aid Operations Level Interoperability within the Region, and again all that is really required are a connection to the mobile IT/IP networks and data applications that can effectively inter-work. PHY-level standardization is not required, as data consumers and providers can connect to the mobile IT/IP network through any wireless or wired connection points, e.g. Ethernet, 700 MHz, 2.4 GHz, 4.9 GHz, UNIIIII and 5.9 GHz DSRC. In this case, there must again be also network IT/IP interconnectivity to each agency’s network systems in order to authenticate users and share data objects.

When operating directly on-scene of a Disaster-level incident, the Region Prefers to keep operational control of Wireless and IT systems; and to let agency commanders assign appropriate equipment, authentication/passwords, etc. to the appropriate individuals. The region has documented few if any cases in which direct-mode off-network data transfer between the incident commanders (or first responders) on scene is required. In such instances, the Region feels that a cache of data devices with known authentication parameters and MAC address should be retained to distribute to the appropriate on-scene personnel. This will enable the Region to react to an infusion of outside assistance in such situations, while maintaining a secure and spectrally pure command and control-operating environment.
6. DATA APPLICATIONS

6.1 Introduction
The FCC docket WT-00-32 has allocated the 4.9-GHz spectrum for Public Safety wireless broadband use. This document focuses on providing a list of 4.9-GHz spectrum applications that 4.9-GHz Work Group members have compiled and reviewed. The list of applications have been placed in a matrix, which provides a high-level description of the applications, provides information relating to the application’s type per FCC order, the security levels required, the mission, and the priority.

The allocated 4.9-GHz spectrum is intended to accommodate a variety of applications for mobile and fixed Wi-Fi (MO) on a primary basis. The deployed devices shall support encryption for applications requiring data integrity. It also supports fixed point-to-point broadband operations on a primary basis (FXB), and fixed point-to-point narrowband operations on a secondary basis (FXO). In addition, it is planned that the technology adopted will support the formation of an ad-hoc wireless network connecting users within the same or multiple agencies at a scene of an incident or emergency.

Contributors to Data Applications document were:

MTA Police Department,
NYSTEC,
NYC Police Department,
NY State Office of Emergency Management,
NYC Transit Authority,
NYC Dept of Information Technology and Telecommunications,
New York State – Statewide Wireless Network, and
Syracuse Research Corporation.

6.2 Region 8’s 4.9-GHz applications & Application Security
This subsection presents the applications matrix (starting on the page that follows), along with a discussion on wireless security concerns. Specifically, subsection 6.2.1 contains the applications matrix and definitions for the columns — e.g., security level, priority level, mission critical, etc. — used in the matrix. A reader of this document, based on the application, will be able to refer to the Application Matrix, and determine the applications type, priority, and security levels of 4.9-GHz applications. Subsection 6.2.2 presents wireless security concerns, and presents the means to mitigate security concerns by assigning the security controls needed for each application, as denoted in the Security Level column in the applications matrix.

6.2.1 GHz Public Safety Applications
The applications identified by the 4.9-GHz Work Group members are presented, starting on the foldout page, as Table 4. The column headings in this applications matrix are explained in bullets that precede and follow that matrix.

Security Level - Indicates the level of security required for the application. The column contains two values: the first value, denoting the security level required for the application,
4.9-GHz Work Group Guidelines

ranges from I (lowest security level) to V (highest security level); the second value indicates the connection type — ST denotes a session termination is needed and (P) indicated that the connection is permanent.

**Priority** - Indicates the priority level of the application, as described in Table 3. The application’s priority level can change depending on the incident type. The application ranges from 4 (the lowest priority level) to 1 (the highest priority level).

### Table 3, Application Priority Levels for Use in the 4.9-GHz Band

<table>
<thead>
<tr>
<th>Priority</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Protection of Human Life</td>
<td>Prevents/minimizes the expected loss of life (fire/water/earthquake/WMD rescue, riot/hostage situations, bomb disposal in crowded areas, cardiac/severe trauma EMS response, etc.). Prevents/minimizes expected permanent disabilities (serious diseases, trauma, stroke, etc.). Prevents/minimizes expected recoverable injury/disease, reduce pain and suffering.</td>
</tr>
<tr>
<td>Level 2: Protection of Human Needs</td>
<td>Reduces/prevents the loss of critical infrastructure (water, sewer, electricity, gas mains, emergency communications, etc.). Reduces/prevents the loss of food, clothing, and shelter, or provides emergency replacements. Reduces/prevents the loss of economically critical property (places of business/employment, transportation, machinery, office equipment, public and private records, live stock, etc.).</td>
</tr>
<tr>
<td>Level 3: Protection of the Quality of Life</td>
<td>Reduces/prevents the loss of personal belongings, pets, recreational equipment, and personal communications. Reduces/prevents the loss of places for the performing arts, public parks, wilderness areas, protection of wildlife, etc. (police/fire/environmental actions). Provides public information to Information Officers or from them to media (prevent panic, shelter information, etc.).</td>
</tr>
<tr>
<td>Level 4: Administration</td>
<td>All non-emergency Public Safety tasks, such as records keeping/transfer, recovery cost accounting, etc.</td>
</tr>
</tbody>
</table>

---

2 As defined in Table 6 in subsection 6.2.2.3.
### 4.9-GHz Work Group Guidelines

#### Table 4, Applications Matrix

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Security Level (1 to V)</th>
<th>Priority (1-4)</th>
<th>Mission Critical</th>
<th>Inter-Operability (O, M, D)</th>
<th>Point to Point (PP) or Point to Multi-Point (PMP)</th>
<th>Interactive (I) or Broadcast (B)</th>
<th>App. Layer Data Rate (in Mbps)</th>
<th>Typical Range (in meters)</th>
<th>Mobile to Mobile</th>
<th>Fixed to Mobile</th>
<th>Fixed-to-Fixed Broadcast Band</th>
<th>Itinerate</th>
<th>Fixed-to-Fixed Narrow band</th>
<th>Backhaul Narrow band</th>
<th>Other Bands for Consideration (ISM-916, ISM-2.4, U-NII)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Signaling: Vehicular Traffic light control for emergency vehicles.</td>
<td>V, P</td>
<td>1</td>
<td>X</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Telemetry of patient vital signs: from in-subway or street-level locations to receiving EMS vehicles and hospitals.</td>
<td>V, ST</td>
<td>1</td>
<td>X</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Transmission of voice from Fire and Police emergency call boxes at fixed street-level locations or in subway; real-time report of suspicious activities.</td>
<td>I, P</td>
<td>1</td>
<td>X</td>
<td>M</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Formation of street-level or below-ground (e.g., subway) ad-hoc self-forming networks for sharing of on-scene incident broadband information via an incident-management or command system.</td>
<td>III, ST</td>
<td>2</td>
<td>D</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Visual Intelligence systems</td>
<td>V, ST</td>
<td>1</td>
<td>X</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Signaling: Communications-based Train Traffic Control for above-ground and underground railways (subways).</td>
<td>V, P</td>
<td>2</td>
<td>X</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Video APB (All Points Bulletin)</td>
<td>I, V, ST</td>
<td>2</td>
<td>O</td>
<td>PP</td>
<td>I, B</td>
<td>0.384-2.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Image transfer (send pictures, fingerprints, and descriptions of suspects)</td>
<td>V, ST</td>
<td>2</td>
<td>O</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Use 4.9-GHz network as a backup for existing data systems (Backhaul for ISM).</td>
<td>I, V ST</td>
<td>2</td>
<td>X</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>500-5000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Ad-hoc networking of vehicles while on-scene.</td>
<td>II, ST</td>
<td>2</td>
<td>D</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Hazard Materials information [and Mapping]</td>
<td>II &amp; III, ST</td>
<td>2</td>
<td>X</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Simultaneous transmission of large database files: for use by an Incident Commander providing real-time access to federal, state, and local databases.</td>
<td>V, ST</td>
<td>2</td>
<td>D</td>
<td>PP</td>
<td>I</td>
<td>1</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Remote sensor monitoring for water quality and detection of chemical, biological, radiological or other hazards.</td>
<td>V, P</td>
<td>3</td>
<td>X</td>
<td>O</td>
<td>PP</td>
<td>B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Multiple site transmission of full motion streaming video (30 frames per second) operationally continuous or ad-hoc from inside the subway tunnels, cars, tracks, and stations or from ground or airborne feeds.</td>
<td>III, ST</td>
<td>3</td>
<td>D</td>
<td>PP</td>
<td>I, B</td>
<td>0.384-2</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Video and GIS map download response to inquiries.</td>
<td>I, P</td>
<td>3</td>
<td>X</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Police Record Management Application</td>
<td>V, ST</td>
<td>3</td>
<td>O</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. White board capability</td>
<td>I, ST</td>
<td>3</td>
<td>O</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. Access to building facility drawings (CAD)</td>
<td>II, ST</td>
<td>3</td>
<td>O</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Signaling: Updating messaging on roadways.</td>
<td>V, P</td>
<td>4</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. AVL: Automatic vehicle location information transmission.</td>
<td>I, P</td>
<td>4</td>
<td>M</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Climate Telemetry: Temperature and weather conditions for outdoor facilities monitoring.</td>
<td>I, P</td>
<td>4</td>
<td>O</td>
<td>PP</td>
<td>I</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22. Non-Critical Telemetry: Monitoring and control of remote equipment (e.g. switch heaters).</td>
<td>I, P</td>
<td>4</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23. Access to internet/intranet applications: e.g., schedules, special operational events.</td>
<td>V, ST</td>
<td>4</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24. E-mail</td>
<td>III, ST</td>
<td>4</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 1.0</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25. Instant messaging [SMS]</td>
<td>II, ST</td>
<td>4</td>
<td>M</td>
<td>PP</td>
<td>I</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26. Radio frequency identification (RFID) Tags</td>
<td>II, ST</td>
<td>4</td>
<td>O</td>
<td>PP, PMP</td>
<td>I, B</td>
<td>&lt; 0.1</td>
<td>5-1000</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.9-GHz Work Group Guidelines

Mission Critical - Indicates whether the application is mission critical to public safety or not. A mission critical application cannot suffer from an undue delay in getting the message through which could result in a high probability for loss of life/property.

Interoperability - Indicates the type of interoperability (Operations, Mutual Operations, and Disaster) required of the application. The terms Operations, Mutual Operations, and Disaster are defined in Section 5.

Point-to-Point (PP)/Point-to-Multi-Point (PMP) - Indicates whether the application is point-to-point or point-to-multi-point.

Interactive or Broadcast - Indicates whether the application transmissions are interactive (the sender and the receiver communicate with each other) or broadcast (the sender sends and the receiver just receives the information).

Application Layer Data Rate - Indicates the typical data rate — in Megabits per second (Mbps) — required by the application.

Typical Range - Indicates the typical radio range in meters required by the application.

Application Type (per FCC order) - This set of columns denotes the application type according per FCC order, regardless of whether the application is Primary or Secondary.

Primary are those that are licensed for mobile or fixed broadband use in the area. If Primary, it is Mobile-to-Mobile (MO), Fixed-to-Mobile (MO), or Fixed-to-Fixed Broadband (FXB). Although mobile and fixed broadband applications share primary status, they do not share common technical parameters. MO devices, typically access points and station terminals, can use antennas with up to 9dBi gain without reducing the transmit output power. FXB devices such as point-to-point and point-to-multipoint radios can use antennas with up to 26dBi gain without reducing the transmit output power. MO devices provide access signal within a small area (about 100 meters), and FXB devices provide connectivity between remote locations (several kilometers apart). Secondary applies to those that are not licensed for use in the area or are licensed for fixed narrowband use in the area. If the application use has secondary status, further detailing can be cited for Itinerate use (allowed to roam) or if it is to be used as narrowband Fixed-to-Fixed or narrowband Back Haul operations.

Other Bands for Consideration - Indicates which other bands (ISM-916, ISM-2.4, and U-NII 5.2) are under consideration for this application.

6.2.2 Wireless Application Security

This section begins by first presenting (in subsection 6.2.2.1) a general overview of 802.11 a/b/g technology evolution and security. This is followed by a discussion of wireless security concerns (in subsection 6.2.2.2). Subsection 6.2.2.3 presents Table 5 and Table 6 showing the security controls needed to mitigate security risks to an acceptable level for the applications presented in the applications matrix (Table 4).

6.2.2.1 802.11 a/b/g Wireless Technology Overview

Over the past several years, the 802.11a and the 802.11b (g)³ standards-based wireless networks have entered the mainstream because they were low-cost, widely available, and highly

---

³ What differentiates 802.1g from 802.11b is at the physical layer, how the information is physically transmitted.
interoperable among different vendors. Organizations are seeing the practical benefits of using wireless technology within the enterprise. Wireless networks allow the enterprise to rapidly deploy networks, to reduce the cost of installing wiring, and to give workers more flexibility in where and when they work.

Over the years, improvements have been made in the wireless security protocols to meet the security needs of enterprises wanting to take advantage of wireless networks without compromising security. The following subsections briefly review wireless network security protocols that have been developed. However, it is important to realize that 802.1x standards describe only the physical layer and layer 2 protocols and do not address security aspects. All security aspects are assumed to be addressed by wired LAN standards developed by the IETF. Therefore any 802.1x system has the same security feature as those used by wired LAN networks. Due to this limitation, the licensed 4.9 GHz band protects users from accessing the network since only licensed devices can access this network (unlike the unlicensed bands of 4.9 GHz or 5 GHz). But beyond this basic protection, other aspects of security remain the same as any other wired network.

In contrast, security aspects specific to wireless networks are addressed in cellular networks where security algorithms are designed as an integral part of physical layer and layer 2. Due to integrated approach, cellular networks have excellent track record in terms of security. However, it is not possible to either import or incorporate modified versions of cellular industry’s security features in a WLAN network. The two networks are fundamentally different in their basic architecture, therefore cellular security schemes or algorithms are not described in this document (not relevant).

6.2.2.1.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the de facto encryption algorithm used in the 802.11a/b/g standard. WEP has been found to be easily breakable with software available on the Internet. WEP, by itself, offers essentially no security protection to the wireless access point (AP).

WEP is derived from the existing provisions in the IETF (Internet Engineering Task Force). The types of security provided by IETF are not comparable to algorithms used by cellular systems today. By introducing these algorithms, which are independent of the wireless technology (TDMA, CDMA, OFDM etc.) used, protection to the wireless access can be provided that will be superior to existing IP network security.4

6.2.2.1.2 802.1x

The 802.1x standard improves WLAN security (based on IETF standards), but is still fallible. The standard provides generic support for authenticating wireless clients using an authentication server (e.g., using RADIUS) before they are allowed to access/use the wireless AP. The 802.1x approach allows standards-based implementations of extensible authentication protocols (EAPs)

---

4 Ref: TIA/EIA IS-778 committee TR-2, also TSB 50, committee 45.3.
to be used in conjunction with network authentication. EAP types include EAP-MD5, EAP/TLS, PEAP, and TTLS, as well as Cisco’s proprietary LEAP authentication protocol.

The 802.1x standard, while doing a good job of only granting access to users who have successfully authenticated to the wireless network, still relies on WEP for data encryption. Even if dynamic WEP keys are used to encrypt the data, it is still possible to circumvent security by taking advantage of the inherent weakness in WEP. Risk to an enterprise using any of the mentioned EAP types includes unauthorized network access, potential for recovering dynamic WEP keys and then decrypting confidential information, and a vulnerability to denial-of-service (DoS) attacks. The protocol is also subject to a “man-in–the-middle” attack as well as to session hijack. Use of an EAP authentication method supporting mutual authentication — along with 1) using the authentication server to assign dynamic WEP keys and 2) periodic re-authentication — minimizes the probability of these two types of attacks. The attacks described are equally applicable to wired networks as well.

6.2.2.1.3 WiFi Protected Access Specification (WPA-1)

WiFi Protected Access Specification (WPA-1) uses a combination of 802.1x for network authentication and a security protocol called the Temporal Key Integrity Protocol (TKIP) to encrypt, validate, and secure the transmission of data over the wireless connection. TKIP includes methods to ensure that no data was improperly transmitted on the network; it uses rotating keys for encrypting data, and it implements a message authenticity check and per-packet key mixing.

TKIP has been designed by the security community to address all the major weaknesses of WEP by including: 1) using a message-integrity protocol to prevent message tampering; 2) changing how the initialization vector (IV) is selected and how the IV is used as a replay counter; 3) changing the encryption key for every frame through Pre-Packet Key Mixing, 4) increasing the IV size to avoid reuse of the same IV, and 5) using a key-management mechanism to distribute and change the keys.

It is important to note that WPA-1 is a compromise security solution developed within the limitations of existing WEP-based wireless systems so as not to invalidate the installed wireless base present within organizations. For example, to meet the processor limitations in installed APs, the Michael algorithm was chosen as the message integrity code (MIC), because the algorithm does not involve multiplications and uses a fairly short check-word. This, however, makes the MIC susceptible to a brute-force attack. As a countermeasure to a brute-force attack on the MIC, the security designers gave Michael a 60-second “blackout period” rule that says something to the effect that, if the AP receives a predetermined number of unauthorized packets within a predetermined period of time, the AP assumes that it is under attack and “shuts down” for a specified period of time (e.g., 60 seconds). The shutdown is meant to thwart a brute-force attack, but could itself become the source of a denial-of-service attack by a hacker who sends vast quantities of unauthorized data, thus triggering an ongoing series of AP “shutdowns.” Also, a fundamental weakness in the first four bytes of the RC4 key stream theoretically can be exploited.

At the writing of this document, WPA-1 security is considered by industry experts to provide acceptable security for deploying wireless networks securely in the enterprise. Security experts hold this opinion because the technology used to implement the security methods is based,
4.9-GHz Work Group Guidelines

wherever possible, on pre-existing and well-tried algorithms. While it seems unlikely at the present time that the security of the WPA-1 can be compromised in some way, experts caution that there is a possibility of it happening — because the WPA-1 is a compromise solution. Thus, security experts recommend that WPA-1 be an interim solution until the 802.11i standard is adopted. Any organization wanting to use WPA-1 should have a migration plan and path to 802.11i when the standard is adopted and equipment becomes available. Many wireless vendor offerings are upgradeable from WPA-1 to 802.11i.

6.2.2.1.4 802.11i (aka WPA-2)

The 802.11i standard introduces the Robust Secure Network (RSN) protocol, the Counter Mode with Cipher-Block-Chaining Message-Authentication-Code Protocol (CCMP), and the Advanced Encryption Standard (AES). CCMP defines a rule set that uses the AES block cipher to enable encryption and protection of 802.11i frames of data. CCMP is considered stronger than TKIP in that it was designed from the ground up to provide security for 802.11. In creating CCMP, designers took a clean sheet of paper, using the best-known security techniques. By contrast, TKIP is a compromise security solution. There is much in common between WPA/TKIP and RSN/CCMP-based systems, with the fundamental difference being in how the data is encrypted and decrypted. The former uses WEP, and the latter AES.

The 802.11i standard supports an AES key using CCMP, which conforms to the FIPS 140-2 specification required by many federal government agencies.

6.2.2.2 Wireless Security Concerns

This section presents the various types of wireless LAN security concerns. In general, these concerns, which follow, apply predominantly to the 802.11a/b/g family of wireless LANs.

1) **Policy** - Without policy, there is no overarching set of guiding principles for securing the organization’s information resources.

2) **Physical Security** - The physical location of the wireless access point (AP).

3) **Rogue Wireless Access Point** - Unauthorized installed wireless access points on an enterprise network bypass all perimeter security and offer backdoors to the enterprise’s wired network.

4) **Denial of Service** - A denial-of-service attack aims to prevent valid wireless clients from reaching the enterprise access point through either of two means: RF jamming attacks or weaknesses in the 802.11 specifications.

5) **Eavesdropping** - Eavesdropping is a passive attack in which the attacker monitors the transmissions between the wireless access point and the wireless client.

6) **Network Topology and Wireless Access Points** - The proper placement of the wireless access point in the network topology can enhance or detract from security.

7) **Impersonation Attacks** - Three similar attacks (Masquerading attack, Man-in-the-Middle attack, and Session-Hijacking attack) involve “spoofing” a legitimate wireless AP or a legitimate wireless client.
8) **AP Configuration Interfaces** - Attackers will attempt to gain access to the AP’s configuration interfaces by compromising the interface’s security.

9) **Secure AP Configuration** - Misconfiguration of the wireless access point and not maintaining the wireless client and the AP at the vendor’s latest patch level can facilitate a successful attack against the WLAN.

10) **The Wireless Client** - An often overlooked risk to a WLAN. Each wireless client contains sensitive information required for authenticating and communicating with APs, which must be safeguarded.

   a. **Physical Loss/Theft of Wireless Clients** - With physical possession of the wireless client, an attacker can either gain access to the WLAN or extract other sensitive information for accessing the organization’s networks and systems.

   b. **Host System Configuration** - Attackers will attempt to compromise the host device in order to gain access the authentication credentials stored there.

   c. **Wireless Client Configuration** - The ability of users to alter the configuration of their wireless device may allow the users to utilize the device in unintended ways.

   d. **Ad-Hoc Mode** - Many newer computers have preinstalled wireless cards, and ad-hoc mode may be enabled by default. This can be done by an attacker, if the AP or wireless client unit is in an easily accessible public area, for example.
6.2.2.3 4.9 GHz Application Security Controls

This section presents the various security controls identified to mitigate the risk to wireless applications identified in the applications matrix. Table 5 presents the six security methods identified for addressing the identified security concerns. Table 6 lists the 5 security levels (I-V) for the identified applications, and denotes the security methods from Table 5 associated with each security level.
<table>
<thead>
<tr>
<th>Security Method</th>
<th>Description</th>
<th>Options</th>
<th>Type</th>
<th>Pre-requisite</th>
<th>Coverage</th>
<th>Time Frame</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Authentication algorithm based</td>
<td>Authenticated physical unit being used - No user intervention at any point. Entirely automated, process-based algorithm.</td>
<td>Channels - limited/Global</td>
<td>Auth - Algorithm based</td>
<td>ESN, MIN, A-key, all pre-registered</td>
<td>Covers all handsets. Based on info in database, further authentication may be needed by some units</td>
<td>Phase I or II</td>
<td>High level of security; not broken or attacked since introduction in 1997. Modified version may be used in WLAN networks (see 6.2.2.1)</td>
</tr>
<tr>
<td>2 Voice Encryption</td>
<td>Encrypts both the uplink and downlink voice; type of vocoder is predetermined; type of encryption is also predetermined.</td>
<td>Voice channels only</td>
<td>Algorithm based</td>
<td>Successful Authentication</td>
<td>Covers handsets with voice capability. Details of implementation in VoIP - TBD</td>
<td>Phase I or II</td>
<td>High level of security; not broken or attacked since introduction in 1997. This may be implemented if VoWiFi is supported (see 6.2.2.1)</td>
</tr>
<tr>
<td>3 PIN-based authentication</td>
<td>User input based. PIN acts as password to authenticate user and provide services.</td>
<td>Only in legacy systems</td>
<td>User name/ unit + PIN input</td>
<td>Only combination of user name + PIN</td>
<td>Allows flexibility to add users in times of urgent need. (Less secure than CAVE algorithm based system).</td>
<td>Initial</td>
<td>In use for over two decades. Known methods of attack and hijack, but success rate is low.</td>
</tr>
<tr>
<td>4 Data Encryption</td>
<td>Encrypts both the uplink and downlink Data - type of encryption is predetermined.</td>
<td>Authentication or PIN</td>
<td>Algorithm based</td>
<td>Successful Authentication</td>
<td>Covers all sessions for the handset. Encryption of individual sessions or streams - TBD.</td>
<td>Initial</td>
<td>In use for about a decade. Handset needs DTMF encryption. Not useful if user inputs PIN in a public area.</td>
</tr>
<tr>
<td>5 Standard 128-key encryption</td>
<td>Encryption based on IP certificates and IETF methods.</td>
<td>Applies to specific web site access</td>
<td>web/ application based</td>
<td>Specific certificate match</td>
<td>Covers intranet and internet sites. No specific schemes for VoIP or voice.</td>
<td>Initial</td>
<td>In use for over one decade. A known method of attack and hijack, but success rate is low.</td>
</tr>
<tr>
<td>6 Unique Challenge</td>
<td>Challenges handset based on a random number generated using the specific SSD-U (Shared Secret Data Update).</td>
<td>Channels - limited/Global</td>
<td>Auth - Algorithm based</td>
<td>Successful Authentication from CAVE</td>
<td>Covers all cellular handsets. Based on info in database. Unique challenge provides the highest level of security in cellular networks.</td>
<td>Phase I or II</td>
<td>Highest level of security; not broken or attacked since 1997. But completion of both authentication and unique challenge may take up to 15 seconds - Cannot be implemented in WLAN networks (6.2.2.1)</td>
</tr>
</tbody>
</table>
### Table 6, Security Levels and Associated Controls

<table>
<thead>
<tr>
<th>Access/Content Protection Type</th>
<th>Access/Content Protection Description</th>
<th>Security Levels (I-V)</th>
<th>Security Methods (from Table 3)</th>
<th>Option Type</th>
<th>Applications - typical</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Physical Device</td>
<td>I</td>
<td>1 only</td>
<td>A</td>
<td>Daily Use</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Device + User (login/ password)</td>
<td>II</td>
<td>1 and 3 (2 as option)</td>
<td>A + B</td>
<td>Guest user but within facility</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Party Authentication (group call, etc.)</td>
<td>III</td>
<td>1,2,3</td>
<td>A + B + C</td>
<td>System users or system to system</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Integrity of Data</td>
<td>IV</td>
<td>1,2,5,6</td>
<td>A+B+C+D</td>
<td>Integrity of Communication</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Encryption of Data</td>
<td>V</td>
<td>1,2,4,6</td>
<td>A + B + C + E</td>
<td>Confidential communication</td>
<td></td>
</tr>
<tr>
<td>ST</td>
<td>Session Termination (user logout or timer based)</td>
<td>N/A</td>
<td>Management function</td>
<td>Management Function</td>
<td>System function</td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>Permanent connection (timer with period of years)</td>
<td>N/A</td>
<td>Connection type</td>
<td>Connection type</td>
<td>System connection for 7 X 24 use</td>
<td>Usage depends on specific applications. Refer to applications matrix for details.</td>
</tr>
</tbody>
</table>
7. PROCEDURES ON DEALING WITH ADJACENT AND OVERLAPPING JURISDICTIONS

7.1 Adjacent Regional Coordination

The 4.9-GHz Work Group shall contact the chairpersons of the adjacent Regions to determine the status of their respective plans. Before submitting Region 8’s 700-MHz 4.9-GHz Work Group Guidelines to the FCC, Region 8 700-MHz 4.9-GHz Work Group members will coordinate its Work Group Guidelines with those of adjacent regions.

The Regions adjacent to Region 8 are Regions 19, 28, and 30. Region 19 is comprised of the New England States; Region 28 is comprised of Eastern Pennsylvania, Delaware, and southern New Jersey; and Region 30 is comprised of the majority of New York State. The contacts for these regions are as follows:

Regional Chairman, Region 19, New England
700-MHz Public Safety Planning Committee
George J. Pohorilak
Office of Statewide Emergency Telecommunications
1111 Country Club Road
Middletown CT 06457-9294
Telephone: (860) 685-8108
FAX: (860) 685-8363
Email: george.pohorilak@po.state.ct.us
Web: www.ner700mhz.org

Regional Chairman, Region 28,
Pennsylvania - Eastern (east of Harrisburg), southern NJ, and DE
700-MHz Public Safety Planning Committee
Mark A. Grubb Director Division of Communications
Department of Safety and Homeland Security
3050 Upper King Road Dover DE 19904-6410
Telephone: (302) 739-4207
FAX: (302) 697-0355
Email: mailto:mark.grubb@state.de.us

Regional Chairman, Region 30,
David Cook
New York State – Central and Northern NYS)
700-MHz Public Safety Planning Committee
New York - Albany
P. O. Box 2062
Albany NY 12220-0062
Telephone: (518) 443-2041
FAX: (518) 443-2787
eFax: (408) 580-8496
Email: David.Cook@oft.state.ny.us
7.2 Dispute Resolution

“(a) Channels in this Band are available on a shared basis only and will not be assigned for the exclusive use of any licensee”

“(b) All licensees shall cooperate in the selection and use of channels in order to reduce interferences and make the most effective use of the authorized facilities. Licensees of stations suffering or causing harmful interference are expected to cooperate and resolve this problem by mutually satisfactory arrangements. If licensees are unable to so, the (FCC) Commission may impose restrictions including specifying the transmitter power, antenna height, or area or hours of operation of the stations concerned. Further, the (FCC) Commission may prohibit the use of any 4.9 GHz channel under a system license at a given geographical location when, in the judgment of the (FCC) Commission, its use in that location, is not in the public interest.”

The 4.9-GHz Work Group members will assist in the dispute-resolution process. If an agency disputes the implementation of the 4.9-GHz Work Group Guidelines after FCC approval, the agency shall notify the Chairperson of the 4.9-GHz Work Group in writing. The 4.9-GHz Work Group will attempt to resolve the dispute on an informal basis.

If a party to the dispute is the employer of the Chairperson, then the Chairperson will recuse himself/herself in the dispute resolution process, and the Vice Chair will serve in his place to lead the dispute resolution process.

If a party to the dispute is the employer of both the Chairperson and the Vice Chair, then both the officers will recuse themselves from the dispute resolution process. The Work Group will appoint a member who has no conflict of interest. Senior members of the 4.9-GHz Work Group will be given the first priority in cases in which the Chairperson and the Vice Chair recuse themselves.

If, after 30 days the dispute is not resolved, the Chair, Vice Chair, or Appointed member will create an ad-hoc Dispute Resolution Committee. The ad-hoc Dispute Resolution Committee will hear input from disputing agencies and any affected agencies and consider the issues in terms of the Regional plan 4.9-GHz Work Group Guidelines.

The Committee will then meet in executive session to prepare recommendations to resolve the dispute. If the recommendation from the executive session meeting is not acceptable to the disputing agency or agencies, the Committee will forward the dispute and all written documentation to the Federal Communication Commission (FCC) for final resolution.

The 4.9-GHz Work Group Chair, Vice Chair, or Work Group Member appointed will inform the Chairperson of Region 8 700-MHz Regional Planning Committee (RPC) of all the dispute resolutions and provide supporting documentation of procedures and recommendations that were used in the dispute-resolution process.

7.3 Incident Commanders

The Incident Commander is an individual representing one or multiple agencies at the incident scene. The Incident Commander at the scene of an incident not only is responsible for the units

---

5 Refer to CFR §90.1209 Policies governing the use of the 4940-4990 MHz Band
of the agencies that he/she represents, but also responsible for other units of other agencies that are operating in support of the incident operations.

Incident Commanders follow the five major management activities: Administration and Finance, Command, Logistics, Operations, and Planning. Administration and Finance monitors cost related to the incident. Command has responsibility at the incident scene, including establishing objectives and priorities based on the type of incident, determining the available resources, and enforcing agency or agencies policies based on prior agreement(s) between agencies. Logistics provides all other resources, including implementing communications functions and coordinating services. Operations develop the tactical organization and direct all resources to carry out the Incident Action Plan. Planning collects and evaluates information, maintains status of assigned resources and functions, and develops the Incident Action Plan to accomplish objectives.

The Incident Commanders shall make reasonable efforts and attempts to coordinate as per guidelines developed with agencies involved in mutual aid. The Incident Commanders shall follow the guidelines established during the pre-planning phase, during which SOPs between agencies are developed.

The Incident Commanders have control and responsibility at the scene. Incident Commanders of licensed operations on record with the Region 8 700-MHz 4.9-GHz Work Group will have the authority to establish user priorities and temporary rules of operation on all 4.9-GHz spectrum usage that might interfere with the incident scene. Incident Commanders will make all reasonable efforts and attempts to coordinate 4.9-GHz frequency usage with other licensed operators that have been approved by the 4.9-GHz Work Group.

7.4 Procedure for Regional Frequency Coordination

Prior to applying for a new license to operate in 4.9-GHz spectrum, eligible entities should contact the Region 8 700-MHz 4.9-GHz Work Group, in writing, to provide it with information regarding their intended operation in the 4.9-GHz spectrum. Licensed operations not already on record with the 4.9-GHz Work Group will be considered as being secondary until such licensee contacts the 4.9-GHz Work Group, in writing, and provides information about existing and intended operations in the 4.9-GHz spectrum.

The 4.9-GHz Work Group highly recommends the sharing of infrastructure and technologies among multiple licensees operating in the same geographic area. Memoranda of Understanding shall be created to allow for the shared use of spectrum if sharing of infrastructure or technologies is not a feasible solution.

The 4.9-GHz Work Group will create and maintain a database for coordinating 4.9-GHz spectrum resources in areas where multiple 4.9-GHz operations are proposed. The 4.9-GHz Work Group will act as a clearinghouse for public safety agencies, providing information and facilitating resource sharing where feasible. Requests for frequency coordination should be submitted to the 4.9-GHz Work Group in writing. The 4.9-GHz Work Group will appoint a frequency coordinator and an alternate coordinator, who will review the request and make a recommendation to the 700-MHz Regional Planning Committee (RPC) Chair within 30 days from the request date.

The RPC Region 8 700-MHz 4.9-GHz Work Group will provide coordination documentation to the application and existing licensees within overlapping jurisdiction of the proposed area of operation upon request.
7.5 Interference Avoidance

The 4.9-GHz Work Group does not guarantee full interference protection within the 4.9-GHz spectrum. Systems should be engineered to facilitate resource sharing where feasible. The 4.9-GHz Work Group recommends the use of 4.9-GHz equipment that has built-in interference-avoidance mechanisms to provide for protection, such as carrier sense, MAC mechanisms.

7.5 Protection of Incumbent Adjacent and Co-Channel Users

7.5.1 US Navy

The US Navy uses spectrum in the band just below 4.9 GHz to conduct Cooperative Engagement Capability (CEC) operations in nine training areas located along the East, West and Gulf Coasts, the entire state of Hawaii, plus military reservations in southern California and New Mexico. Licensees in the lower half of the 4.9 GHz band might receive interference from high power CEC operations within these training areas or, worst case, as far as 245 miles away from high power airborne CEC operations within these training areas. The Navy has the right to expand the training areas. The FCC has not established any specific interference mitigation procedures between 4.9 GHz and Navy CEC operations. As the 4.9 GHz band begins to be deployed, licensees and the FCC may establish approaches to address concerns about CEC interference to 4.9 GHz operations. Appendix C of the Report & Order in WT Docket 00-32 lists the parameters of the nine CEC stations. Maps of the protected areas in affected states follow:

MAPS OF NAVY CEC TRAINING AREAS
7.5.2 Radio Astronomy
Radio Astronomy operates in the 4990-5000 MHz band on a primary basis and in 4950-4990 MHz at 14 specific locations on a secondary basis. 4.9 GHz licensees must protect those
operations as required in Part 2, Table of Frequency Allocations, footnote US311.6 Because public safety transmitters will primarily be operating close to the ground, no interference to radio astronomy observatories is anticipated. The need to protect radio astronomy is the reason behind the prohibition on aeronautical use of the 4.9 GHz on a routine basis. The radio astronomy sites that must be protected and the coordination zones are shown on the following map.

7.5.3 Aviation (Requires an FCC Waiver)

Operation on-board aircraft – helicopter video downlinks for example – is not generally permitted in the 4.9 GHz band because of concern about interference from such operations to radio astronomy operations. Agencies wishing to use the band for airborne operations can seek a waiver to do so. All waiver requests for airborne operations must include the following information:

- All technical parameters of the proposed airborne operation
- Technical showings, using ‘established criteria’ (interference threshold levels contained in ITU-R Recommendation RA. 769-1)7 demonstrating the proposed operation will not cause interference to any radio astronomy operations.
- Demonstrate how the airborne operations will protect other 4.9 GHz band operations.

---


The FCC will coordinate with the National Telecommunications and Information Administration (NTIA) before acting on any waivers requesting airborne operations.
8. REGIONAL SPECTRUM UTILIZATION

Primary Uses

Primary uses of the 4.9 GHz band are for hot spots, point-to-multi-point, base/mobile/portable operations, broadband permanent fixed point-to-point links, and temporary fixed point-to-point. Communications must be related to the protection of life, health or property. Unattended and continuous operation is permitted; voice, data and video operations are permitted. Operation onboard aircraft is prohibited; although the FCC will entertain waivers for such operations (see section on “Uses Requiring Waiver.”)

Broadband permanent (in place for more than one year) fixed point-to-point links, defined as:

- “fixed links that connect 4.9 GHz base and mobile stations that are used to deliver broadband service, as well as other public safety network using spectrum designated for broadband use,” and
- “Stand-alone permanent fixed 4.9 GHz links that are used to deliver broadband service, such as a fixed video surveillance link used to monitor a high-risk target or environment.”

Secondary Uses

Narrowband permanent fixed point-to-point links that are “only used to connect narrowband base stations operating in public safety bands not designated for broadband (i.e. public safety VHF, UHF, narrowband 700 MHz and 800 MHz) to other networks, or serve to backhaul narrowband traffic originating from narrowband base stations are secondary to the primary uses of the band. Fixed point-to-point operations are considered permanent if they are constructed and in place for more than one year. Secondary operations must not cause interference to primary operations and must accept interference from primary operations in the band. Secondary operations must mitigate any interference caused to primary operations up to and including ceasing operations.

Table 7, Possible Channel Allocations for Region

<table>
<thead>
<tr>
<th>4940-4945</th>
<th>4945-4955</th>
<th>4955-4965</th>
<th>4965-4975</th>
<th>4975-4985</th>
<th>4985-4990</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 MHz Block for multiple or aggregate 1 MHz application’s Air Video Link PAN/VLAN* Mesh Ad-Hoc On Scene Fixed Primary or Secondary Point to Point for Backhaul of Multipoint to Point Network Block</td>
<td>10 MHz Network Block for node type application or hotspot</td>
<td>10 MHz Network Block for node type application or hotspot</td>
<td>10 MHz Network Block for node type application or hotspot</td>
<td>10 MHz Network Block for node type application or hotspot</td>
<td>5 MHz Block for multiple or aggregate 1 MHz application’s Air Video Link PLAN/VLAN Mesh Ad-Hoc On Scene Fixed Primary or Secondary Point to Point for Backhaul of Multipoint to Point Network Block</td>
</tr>
</tbody>
</table>
The bullets that follow define the technologies referenced in Table 7.

- **Ad-hoc (or “spontaneous”) Network** - A local-area network or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network. In Latin, *ad hoc* literally means “for this,” further meaning “for this purpose only,” and thus usually temporary. The term has been applied to future office or home networks in which new devices can be quickly added, using, for example, the proposed Bluetooth technology, in which devices communicate with the computer and perhaps other devices using wireless transmission.

- **Application** - In information technology, an application is the use of a technology, system, or product.

- **Backhaul** - In wireless network technology, *backhaul* refers to the process of sending voice and data traffic from a cell site to a switch, from which it can be distributed across the network.

- **Block** - In network communication, a *block* is a group of data bits or bytes that is transferred as a standard unit. The size (or length) of such a block depends on the communications protocol.

- **Fixed** - Refers to the operation of wireless devices or systems in fixed locations. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless, which tend to be battery powered.

- **Hotspot** - A *hotspot* is a wireless LAN (local-area network) node that provides Internet connection and virtual private network (VPN) access from a given location. For example, a business traveler with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet and his/her own company remotely with a secure connection.

- **LAN** - *Local-Area Network*, a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a *wide-area network (WAN).*

- **MAN** - *Metropolitan Area Network*, a data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media.

- **Mesh** - Also called *mesh topology* or a *mesh network*, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.

- **Node** - In a network, a node is a connection point, either a redistribution point or an end for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes.
• **PAN - Area Network**, a wireless communications system intended for use by terrestrial subscribers in vehicles or on foot. Such a system can stand alone, but often it is interconnected with a fixed system. The ideal PLAN provides mobile and portable users with a level of service comparable to that of subscribers in a fixed network. This can be a special challenge in regions where the terrain is irregular, where base station sites are hard to find and maintain and in urban environments where there are numerous obstructions such as buildings, as well as myriad sources of radio-frequency (RF) radiation that can cause noise and interference.

• **Point-to-Multi-Point** - Communication between a point and multiple points using parallel interfaces.

• **Point-to-Point** - Communication between two points using a serial interface.

• **VLAN - Vehicular Local Area Network**, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that, when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.
## APPENDIX A, 4.9-GHZ WORK GROUP MEMBERS

### Table 8, List of FCC Region 8 700-MHz 4.9-GHZ Work Group Members

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Agency</th>
<th>E-Mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bradshaw</td>
<td>Hugh</td>
<td>NYC OEM</td>
<td><a href="mailto:hbradshaw@oem.nyc.gov">hbradshaw@oem.nyc.gov</a></td>
</tr>
<tr>
<td>Delaney</td>
<td>Matthew</td>
<td>New York State Office of Technology</td>
<td><a href="mailto:Matthew.Delaney@dhses.ny.gov">Matthew.Delaney@dhses.ny.gov</a></td>
</tr>
<tr>
<td>Golder</td>
<td>Thomas</td>
<td>NCPD</td>
<td><a href="mailto:tgolder@pdcn.org">tgolder@pdcn.org</a></td>
</tr>
<tr>
<td>Guedko</td>
<td>Larissa</td>
<td>New York State Office of Technology</td>
<td><a href="mailto:LGuedko@dhses.ny.gov">LGuedko@dhses.ny.gov</a></td>
</tr>
<tr>
<td>Horace</td>
<td>Edmund</td>
<td>NCPD</td>
<td><a href="mailto:ehorace@pdcn.org">ehorace@pdcn.org</a></td>
</tr>
<tr>
<td>Jacobowitz</td>
<td>Neli</td>
<td>NYCT</td>
<td><a href="mailto:Neli.jacobowitz@nyct.com">Neli.jacobowitz@nyct.com</a></td>
</tr>
<tr>
<td>Johnson</td>
<td>Chris</td>
<td>New York State Office of Technology</td>
<td><a href="mailto:Christopher.Johnson@dhses.ny.gov">Christopher.Johnson@dhses.ny.gov</a></td>
</tr>
<tr>
<td>Krishnamurthy</td>
<td>Raghunandan</td>
<td>NYCT</td>
<td><a href="mailto:krishnamurthy.raghunandan@nyct.com">krishnamurthy.raghunandan@nyct.com</a></td>
</tr>
<tr>
<td>Lieberman</td>
<td>Chris</td>
<td>Westchester County</td>
<td><a href="mailto:Cal4@westchestergov.com">Cal4@westchestergov.com</a></td>
</tr>
<tr>
<td>Link</td>
<td>Kenneth J.</td>
<td>NJ-TF1 USAR</td>
<td><a href="mailto:kc2klw@comcast.net">kc2klw@comcast.net</a></td>
</tr>
<tr>
<td>Louit</td>
<td>Gerard</td>
<td>NYCT</td>
<td><a href="mailto:gerard.louit@nyct.com">gerard.louit@nyct.com</a></td>
</tr>
<tr>
<td>Manion</td>
<td>Robert</td>
<td>NYSTEC</td>
<td><a href="mailto:manion@nystec.com">manion@nystec.com</a></td>
</tr>
<tr>
<td>Melendez</td>
<td>Felix</td>
<td>NYC-DOITT</td>
<td><a href="mailto:fmelendez@doitt.nyc.gov">fmelendez@doitt.nyc.gov</a></td>
</tr>
<tr>
<td>Melia</td>
<td>Anthony</td>
<td>Essex County Sheriff's Department, Office of the Chief</td>
<td><a href="mailto:meliaa@apco911.org">meliaa@apco911.org</a></td>
</tr>
<tr>
<td>Napolitano</td>
<td>Jerry</td>
<td>Motorola</td>
<td><a href="mailto:napolitano@motorolasolutions.com">napolitano@motorolasolutions.com</a></td>
</tr>
<tr>
<td>Quinn</td>
<td>Myles P.</td>
<td>Suffolk County Fire Rescue</td>
<td><a href="mailto:myles.quinn@co.suffolk.ny.us">myles.quinn@co.suffolk.ny.us</a></td>
</tr>
<tr>
<td>Stiles</td>
<td>Vincent</td>
<td>NYS Office for Technology</td>
<td><a href="mailto:Vincent.Stile@dhses.ny.gov">Vincent.Stile@dhses.ny.gov</a></td>
</tr>
<tr>
<td>Yurman</td>
<td>Joseph</td>
<td>Wireless Communications &amp; Frequency Coordination, NYC Transit Authority</td>
<td><a href="mailto:joseph.yurman@nyct.com">joseph.yurman@nyct.com</a></td>
</tr>
</tbody>
</table>
APPENDIX B, RELEVANT STANDARDS AND TECHNOLOGY IN THE 4.9-GHZ BAND FOR PUBLIC SAFETY USE

A compendium of Standards and Technology relevant to the RPC 8 700-MHz Planning Committee, 4.9-GHz Work Group

Warning:
The information contained herein represents a snapshot in time (September 2010) of the state of the art in standards and technology suited to be considered in light of the 4.9 GHz Work Group endeavor. It is not to be construed as an authority or an exact representation of any current Industry products. For updates on any standards group’s activities and for manufacturer products, please refer to the latest information from their respective web sites.

Overview
The report points to the various wireless IEEE standards activities as well as the current technologies relevant to the 4.9-GHz Band Transferred from Federal Government Use for Public Safety. The report summarizes the 4.9-GHz specific Parameters as described in the FCC Memorandum Opinion and Order and 3rd Report and Order, dated May 2, 2003, and updated by: 1/ FCC 07-85 WP docket No: 07-100 NPRM Released May 14,2007; 2/ FCC 09-29 WP Docket 07-100 RO & Further NPRM Released April 9, 2009, and, 3/ FCC DA 09-2530 – PS and HSB new station classic code and licensing instructions for PPFS in the 4940-4990 MHz Band.

Introduction, The 4.9-GHz Licensed Spectrum for Public Safety
The 4.9-GHz spectrum offers 50 MHz of bandwidth for Public Safety. The band is to be used and shared by regional Public Safety Agencies according to rules of the Federal Communications Commission (FCC) Memorandum Opinion and Order (MO&O) and the 3rd Report and Order, FCC Doc. # 03-99. The FCC Doc #03-99 delegates to the regional committees the task to specify the sharing of the 4.9-GHz bandwidth among agencies operation in RPC Region 8 areas.

The FCC imposes no Standard to apply to this spectrum.

However, the Telecommunications Industry Association (TIA) TR-8.8 Working Group was established by TIA to address interoperability standards for Broadband Data Systems in the 4.9-GHz Public Safety band.

The NPSTC Regional Planning Committee and Broadband Working Groups considered the uniform extension of the 802.11 suite of Institute of Electrical and Electronic Engineers (IEEE) standards in the 5.1, 5.3, 5.7 and 5.9 GHz bands to use in the 4.9-GHz band; NPSTC is

---

8 FCC 03-99; WT Docket No. 00-32, 18 FCC Rcd 9152 (2003 (Third R&O))
9 Another subcommittee is also created to address SDR (Software-Defined Radio)
10 National Public Safety Telecommunications Council.
developing a Statement of Requirements. to renegotiate from the FCC the mask definition adopted from Motorola to match the 802.11 profile.

The 4.9-GHz Spectrum Parameters

Power Levels
- Power limit: PSD of 20 dBm/MHz,
- Maximum total power output: 33dBm (2W) per channel
- Maximum antenna limit Gain: 9 dBi.
- Maximum antenna limit Gain: 26dBi
- Maximum EIRP: 42 dBm.

Channelization
- 1+1+1+1+5+5+5+5+5+5+5+5+5+1+1+1+1
- Aggregation possible to 5, 10, 15 and 20 channels.

4.9 GHz Band Plan
The following channel center frequencies are permitted, per FCC rules (90.1213), to be aggregated to channel bandwidths of 5, 10, 15, or 20 MHz. The maximum bandwidth of a 4.9 GHz channel is 20 MHz.

<table>
<thead>
<tr>
<th>Center Frequency (MHz)</th>
<th>Channel Nos.</th>
<th>Channel Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>4940.5</td>
<td>1</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4941.5</td>
<td>2</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4942.5</td>
<td>3</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4943.5</td>
<td>4</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4944.5</td>
<td>5</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4947.5</td>
<td>6</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4952.5</td>
<td>7</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4957.5</td>
<td>8</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4962.5</td>
<td>9</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4967.5</td>
<td>10</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4972.5</td>
<td>11</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4977.5</td>
<td>12</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4982.5</td>
<td>13</td>
<td>5 MHz</td>
</tr>
<tr>
<td>4985.5</td>
<td>14</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4986.5</td>
<td>15</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4987.5</td>
<td>16</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4988.5</td>
<td>17</td>
<td>1 MHz</td>
</tr>
<tr>
<td>4989.5</td>
<td>18</td>
<td>1 MHz</td>
</tr>
</tbody>
</table>
**Technical Requirements**

**Emission Mask**

The emission masks for 4.9 GHz are listed in 90.210. In November 2004, the FCC defined two masks for use in the 4.9 GHz band: the DSRC-A mask (identical to the mask defined in the 802.11 standards) for a low power devices, and the DSRC-C mask, with better adjacent channel protection, for higher power devices. The low-to-high power breakpoint varies by channel bandwidth: 20 dBm (100 milliwatts) for 20 MHz channels, 17 dBm for 10 MHz channels, 14 dBm for 5 MHz channels and 7 dBm for 1 MHz channels. Public Safety users requested the looser mask for low power devices such that existing 5 GHz commercial-off-the-shelf (COTS) equipment could be easily modified to operate in the 4.9 GHz band, thereby bringing down the costs and reducing initial time to market. The two masks “L” and “M”, defined by the FCC, are displayed in figure 5.

The power limits of stations operating in the 4.9 GHz band are outlined in Rule Section 90.1215. Maximum transmitter power increases according to the amount of bandwidth used. High power devices are limited to a peak power spectral density of 21 dBm within any 1 MHz of bandwidth as long as they do not exceed the peak transmit power over the entire channel bandwidth defined in table 90.1215(a). Likewise, low power devices are limited to a peak power spectral density of 8 dBm within any 1 MHz of bandwidth.

The peak transmit power should not exceed:

<table>
<thead>
<tr>
<th>Channel Bandwidth (MHz)</th>
<th>Low power peak transmitter power (dBm)</th>
<th>High power peak transmitter power (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>27</td>
</tr>
<tr>
<td>10</td>
<td>17</td>
<td>30</td>
</tr>
<tr>
<td>15</td>
<td>18.8</td>
<td>31.8</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>33</td>
</tr>
</tbody>
</table>

All devices can use omni or directional antenna gains up to 9 dBi at maximum transmit power output. Directional antenna gain may exceed 9 dBi, if both power transmit power and power spectral density are reduced dB-per-dB by the amount that directional antenna gain exceeds 9 dBi.
High power devices used for point-to-point or point-to-multipoint operation (fixed or temporary) may use transmit antennas with a directional gain up to 26 dBi at maximum transmit power output. Directional antenna gain may exceed 26 dBi, if both power transmit power and power spectral density are reduced dB-per-dB by the amount that directional antenna gain exceeds 26 dBi.

Eligibility
Public Safety services as defined under Part 90 rule section 90.523 are eligible to hold a 4.9 GHz license. All state or local governmental entities (including municipal transit authorities and municipal utilities qualifying for public safety service) are eligible to hold 4.9 GHz licenses. Entities not eligible to hold a license, but which perform operations in support of public safety, (such as private critical infrastructure industries) can negotiate sharing agreements with 4.9 GHz public safety licensees. The federal government is not eligible to hold 4.9 GHz licenses but can share state and local public safety systems. Sharing of systems must be by written agreement between the licensee and the party sharing the system and all communications by the non-licensee must be in support of public safety, related to the protection of life, health or property.

Types of Uses
The 4.9 GHz band has been allocated to public safety for broadband technologies. Communications must be related to the protection of life, health or property. Examples of types of uses are:
- Wireless LANS for incident scene management
- Mobile data
- Video security
- VoIP
- PDA connectivity
- Hotspots
- T1 line replacement (permanent fixed point-to-point operations are secondary to base mobile and temporary fixed operations)

Filing for a 4.9 GHz License
Frequency coordination is not required at 4.9 GHz, so eligible entities can apply for a 4.9 GHz license using the FCC’s on-line application system, the Universal Licensing System (ULS).

Eligible entities interested in obtaining 4.9 GHz licenses can either use the filing guide provided in Appendix A of this document, or contact one of the many FCC licensing preparation firms for assistance.

How to File for a 4.9 GHz License
Eligibility for a 4.9 GHz license is limited to public safety entities and communications on the band must be limited to the protection of life, health or property. Cities, towns, counties, states, municipal utilities are all eligible to hold 4.9 GHz licenses.
Each 4.9 GHz license is granted for the entire 50 MHz available in the band and all primary licensees share the band equally – there are no exclusive assignments. Licenses in the 4.9 GHz band are granted to cover the licensee’s legal jurisdiction – e.g. citywide, countywide, statewide. Each transmitter site need not be licensed unless it affects an Environmentally Protected Area, is within a Quiet Zone or would require international coordination. Then the site must be licensed separately.

If the applicant is licensing a permanent fixed point-to-point system (which operations are secondary to other operations in the band), then each permanent fixed site must be listed individually on the license application giving complete information about the site.

License applications for operations at 4.9 GHz are filed using the FCC’s Universal Licensing System (ULS). At any time during the electronic filing process, if you do something wrong, or fail to complete a required field, an error message will appear explaining what was completed incorrectly or what information is missing. The system will not let you advance to a new screen until the current screen is completed successfully.

Log onto the FCC’s Universal Licensing System at http://wireless.fcc.gov/uls/.

- Click on “On-Line Filing.”
- Enter your FCC Registration Number (FRN) and your password
- Click ‘Submit’
- A screen will appear that says “My Applications” – Application at a Glance
- Click on the “Apply for New License” link on the left hand side of this page
- A screen will appear that says “License Manager”
- Use the drop-down box to select the radio service code “PA”
- Click “Continue”
- The Form 601 will appear
- When filling out a Form 601 on-line, certain fields will not require completion – these fields appear faint or faded on the screen.
- First item you will need to respond to is “Will this application require a waiver of the Commissions rules?”
- Select ‘No”
- Click ‘No” to the question ‘Are attachments filed with this application?”
- Next question is: “Interconnected Service?”
- Answer yes or no
- Next field is “Fee Status”
- Governmental entities are exempt from fees
- Click “Next page.”
- On the drop down screen in the field “The licensee is” select ‘Governmental Entity’
- Complete all the blank fields (name, address, etc.)

---

11 If you do not have an FCC Registration Number (FRN) you will have to register your Taxpayer Identification Number (TIN) with the FCC following the on-screen prompts using “CORES”. CORES is available on-line on the ULS homepage.
12 Operation on-board aircraft requires a waiver. See text of 4.9 GHz Overview for details.
13 If you have requested a waiver, you will need to answer ‘yes’ to this question because the waiver will be attached to the application.
• Click “Next Page.”
• Ownership Questions/Qualifications
• Answer each of the questions using the drop-down boxes
• Click “Next Page.”
• Type the name of the party authorized to sign the application in the box
• Click “Next Page.”
• The control point section comes up
• Click on ‘add a control point.’ And fill in the control point information, address, telephone number.
• Click on ‘Save’
• Click on “Next Page.”
• The Eligibility screen will appear. Enter rule section 90.1203. Describe your activity just as always – e.g. applicant is a governmental entity, etc.
• Click on “Next Page.”
• The Location Page comes up
• Click on “Add”
• Using the drop down box on Location Description Click on “T – Temporary Fixed.”
• Using the drop down box on Area of operation code, choose the area of operation that corresponds with your legal jurisdiction – Countywide, Statewide, or ‘Other” (for Citywide operations), or kmra around a center point, or box rectangular”
  o A dialogue box will open up after you select the Area of Operation. If you choose:
  ▪ “Other” indicate “within the legal jurisdiction of (city),”
  ▪ “kmra around a set of coordinates,” enter the coordinates, city and state.
  ▪ “County”, enter the county
  ▪ “State”, enter the state
• The last two questions on the page are whether or not the sites would result in an Environmental Effect or are located within a Quiet Zone. Answer these questions using the drop down boxes.
• Click on “Next Page.”
• This is the antenna page, no information is needed, unless you are filing for permanent fixed point-to-point operations. Click on “Next Page.”
• This is the frequency page. You do not need to enter anything in this section because the Universal Licensing System automatically fills in the frequency range for 4.9 GHz.
• At the bottom of the page, select ‘submit’ to file the application with the FCC.
• The FCC assigns your application a file number so that you can track it if necessary. You should receive a granted license within a short period of time. Some grant literally overnight.

14 Temporary Fixed operations are primary. If you propose to operate permanent fixed point-to-point stations, you must select that option from the drop down menu and each permanent fixed site must be listed separately on the application. You must provide coordinates, ground elevation, antenna height, HAAT, etc. for each site.
Figure 5, 4.9-GHz L and M Masks
POSSIBLE COVERAGE SCENARIOS

Various examples of Throughput Capacity Scenarios for On-Scene 4.9-GHz Infrastructure Resources\textsuperscript{15} appear in subsections that follow.

Coverage from Two Adjacent APs

Both APs have 1 X 10-MHz channel, 2 x 5-MHz channels, and 10 x 2-MHz channels.

\begin{itemize}
\item (2) Incident Video Feeds Direct to Infrastructure [2 Mbps]
\item (6) Tactical EMS Feeds to Vehicles [3 Mbps]
\item (8) Vehicle EMS WLAN Feeds to Infrastructure [4 Mbps]
\item (4) Police Tactical WLAN Feeds to Vehicles [0.4 Mbps]
\item (4) Police WLAN Feeds to Infrastructure [0.4 Mbps]
\item (2) Fire Video Feeds to Incident Commander/Vehicle [2 Mbps]
\item (4) Fire Vehicle WLAN Feeds to Infrastructure [4 Mbps]
\item (2) NYCT Video Feeds to Incident Commander/Vehicle [2 Mbps]
\item (2) NYCT Vehicle Feeds to Infrastructure [2 Mbps]
\item (2) NYCT/MTA NYCT FSDB Feeds to ICS [2 Mbps]
\item (2) Guests Feeds/Access [2Mbps]
\end{itemize}

Total 19.6 Mbps, 11.8 to Applications, 7.8 Tactical.

Total Available 40 Mbps, 20 at AP, 20 TAC Margin for PER (Channel and Interference) and OH/Contention %ge, Probability of ACI%ge, with AFS and DFC.

Coverage from Two Adjacent APs

Adjacent APs have 1 10-MHz channel, 2 5-MHz channels, and 10 2-MHz channels.

\begin{itemize}
\item (2) Incident Video Feeds Direct to Infrastructure [2 Mbps]
\item (6) Tactical EMS Feeds to Vehicles [3 Mbps]
\item (8) Vehicle EMS WLAN Feeds to Infrastructure [4 Mbps]
\item (4) Police Tactical WLAN Feeds to Vehicles [0.4 Mbps]
\item (4) Police WLAN Feeds to Infrastructure [0.4 Mbps]
\item (2) Fire Tact. Video to Incident Commander/Vehicle [2 Mbps]
\item (4) Fire Vehicle WLAN Feeds to Infrastructure [4 Mbps]
\item (2) NYCT Video Feeds to Incident Commander/Vehicle [2 Mbps]
\item (2) NYCT Vehicle Feeds to Infrastructure [8 Mbps]
\end{itemize}

\textsuperscript{15} Source: S. O’Hara  SRC
(2) NYCT/MTA NYCT FSDB Feeds to ICS [10 Mbps]
(2) Guests Feeds/Access [2 Mbps]
Total Available 40 Mbps, 20 at AP, 20 TAC Margin for PER (Channel and Interference) and OH/Contention%ge, Probability of ACI%ge, with AFS and DFC.

Coverage from Two Adjacent APs
Both adjacent APs have 20-MH channels.

4.9 GHz Capacity Needs
(2) Incident Video Feeds Direct to Infrastructure [2 Mb/s]
(10) Tactical EMS Feeds to Vehicles [5 Mb/s]
(10) Vehicle EMS WLAN Feeds to Infrastructure [5 Mb/s]
(8) Police Tactical WLAN Feeds to Vehicles [0.8 Mb/s]
(8) Police WLAN Feeds to Infrastructure [0.8 Mb/s]
(2) Fire Video Feeds to Incident Commander/Vehicle [2 Mb/s]
(4) Fire Vehicle WLAN Feeds to Infrastructure [4 Mb/s]
Total 19.6 Mb/s; Total Available 40 MB/s
Margin for PER (Channel and Interference) and OH/Contention, 50%. Probability of ACI, Medium.
Figure 6, Channelization Coverage from Two Adjacent APS, both with 1 10-MHz Channels, 2 5-MHz Channels, and 10 2-MHz Channels, and 10 1-MHz Channels
Air interface standards

The IEEE standards explained below are for informational purposes only and does not infer that the 4.9 GHz band be required to use these standards. Presently the 4.9 GHz public safety band does not have a common air interface that all equipment would need to conform to. There is no guarantee equipment will interoperate with different equipment manufacturers. For example: a PCMCIA air card or subscriber module manufactured by “Vendor B” may not communicate with an access point manufactured by “Vendor A”. Though some manufacture may claim that they are abiding by a particular IEEE standard such as 802.16 WiMax it is not possible to receive interoperable equipment certification from The WiMAX Forum (WiMAX standards organization) since the 4.9 GHz public safety band is not a recognized band of the WiMAX Forum. The only bands that are supported for interoperability by the WiMAX Forum are 2.5 GHz and 3.5 GHz. For more information on products that have received WiMAX interoperability certifications visit: Certified WiMAX products.

IEEE 802.11 – 802.20, Wireless Access Standards Suite

The IEEE 802.11 – 802.20 set of standards addresses the Air Interface specifications governing various configurations of wireless access, e.g. WirelessPAN, WirelessLAN, WirelessMAN, and WirelessRAN. These specifications are of interest and value for the 4.9-GHz Public Safety spectrum. Table 9 summarizes the major features of these standards.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Summary</th>
<th>Band (in GHz)</th>
<th>Bandwidth (in MHz)</th>
<th>Throughput (in Mbps)</th>
<th>Licensing</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>IEEE WLAN Standards, MAC (supported by WiFi)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>OFDM Physical Layer and MAC</td>
<td>5-6</td>
<td>20</td>
<td>6 – 54</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>B</td>
<td>DS-SS, FH-SSPhysical and MAC Layer</td>
<td>2.4</td>
<td>20</td>
<td>11*</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>C</td>
<td>Bridge Operations</td>
<td>All</td>
<td>N/A</td>
<td></td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>D</td>
<td>New Regulatory Domains</td>
<td>All</td>
<td>N/A</td>
<td></td>
<td>Various</td>
<td>Available Now</td>
</tr>
<tr>
<td>E</td>
<td>MAC Improvements – QoS</td>
<td>All</td>
<td>N/A</td>
<td>N/A</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>F</td>
<td>Inter-Access Point Protocol</td>
<td>All</td>
<td>N/A</td>
<td></td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>G</td>
<td>OFDM Physical Layer</td>
<td>2.4</td>
<td>20</td>
<td>54</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>H</td>
<td>Power Control and Dynamic Channel Selection</td>
<td>All</td>
<td>N/A</td>
<td></td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>I</td>
<td>Enhanced Security Mechanisms</td>
<td>All</td>
<td>N/A</td>
<td>N/A</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
</tbody>
</table>

16 Source: 95% SRC.
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Frequency</th>
<th>Bandwidth</th>
<th>Maximum</th>
<th>Status</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td>Japanese Version of X.a PHY</td>
<td>4.9-5</td>
<td>10 and 20</td>
<td>108</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>K</td>
<td>Radio Resource Management</td>
<td>All</td>
<td>N/A</td>
<td>N/A</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>N</td>
<td>High Throughput and MIMO</td>
<td>All</td>
<td>N/A</td>
<td>&gt; 100</td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>P</td>
<td>WAVE/DSRC Physical and MAC Layer</td>
<td>5.9</td>
<td>10</td>
<td></td>
<td>Licensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>R</td>
<td>Fast Roaming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Available Now</td>
</tr>
<tr>
<td>S</td>
<td>ESS MESH</td>
<td>All</td>
<td>N/A</td>
<td></td>
<td>Unlicensed</td>
<td>Available Now</td>
</tr>
<tr>
<td>T</td>
<td>Wireless Performance Prediction</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Comparison of Characteristics Specified within the IEEE 802.11 Suite\textsuperscript{17}

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>802.11</th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Wireless data networking</td>
<td>Broadband LAN Access</td>
<td>Wireless data networking</td>
<td>Broadband LAN Access</td>
</tr>
<tr>
<td>Spectrum Band</td>
<td>2.4-GHz UNII</td>
<td>5 GHz UNII</td>
<td>Unlicensed 2.4 GHz ISM</td>
<td>Unlicensed 2.4-GHz ISM</td>
</tr>
<tr>
<td>Modulation Scheme</td>
<td>FHSS or DSSS</td>
<td>OFDM</td>
<td>DSSS</td>
<td>OFDM or DSSS</td>
</tr>
<tr>
<td>Number of Channels</td>
<td>79 channels with FHSS; 3 or 6 channels with DSSS</td>
<td>12</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Maximum Data Rates (in Mbps)</td>
<td>2</td>
<td>54</td>
<td>11</td>
<td>54</td>
</tr>
<tr>
<td>Range (in meters)</td>
<td>100</td>
<td>50</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Date established (Market Ready)</td>
<td>July 1997</td>
<td>September 1999</td>
<td>September 1999</td>
<td>Commercially available since January 2004</td>
</tr>
<tr>
<td>Compatibility</td>
<td>802.11 only</td>
<td>802.11a only</td>
<td>802.11g</td>
<td>802.11b</td>
</tr>
<tr>
<td>Operability</td>
<td>NA,E,A</td>
<td>NA,E,A</td>
<td>NA,E,A</td>
<td>NA,E,A</td>
</tr>
</tbody>
</table>

Source: PSWN May 2003

\textsuperscript{17} See list of current 802.11 activities at http://www.ieee802.org/11/Reports/802.11_Timelines.htm
### Table 11, IEEE 802.15-22 Standards, Spectrum, Throughput, Licensing, and Availability

<table>
<thead>
<tr>
<th>Technology</th>
<th>Summary</th>
<th>Band (in GHz)</th>
<th>Bandwidth</th>
<th>Throughput (in Mbps)</th>
<th>Licensing</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15</td>
<td>Wireless Personal Access Network – PAN</td>
<td></td>
<td>&gt;100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.15.1</td>
<td>Bluetooth PAN, FHSS PHY</td>
<td>5-6</td>
<td>5-6 GHz</td>
<td>100</td>
<td>Unlicensed</td>
<td>Now</td>
</tr>
<tr>
<td>802.15.3a</td>
<td>Ultra Wideband (UWB – MBOA, DSS)</td>
<td>5-6</td>
<td>5-6 GHz</td>
<td>100</td>
<td>Unlicensed</td>
<td>Now</td>
</tr>
<tr>
<td>802.15.4</td>
<td>ZigBee</td>
<td>5-6</td>
<td>5-6 GHz</td>
<td>0.250</td>
<td>Unlicensed</td>
<td>Now</td>
</tr>
<tr>
<td>802.16</td>
<td>IEEE Fixed point to Multipoint Metropolitan Area Network (MAN) Standards, supported by WiMax</td>
<td>10 - 66</td>
<td>134</td>
<td></td>
<td>2-10 GHz now, above 10 GHz in the future</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>MAN, Fixed Point Communications (OFDM, ARQ, Mesh)</td>
<td>2-11</td>
<td>1.5-20 MHz</td>
<td>134</td>
<td>Both</td>
<td>Now</td>
</tr>
<tr>
<td>B</td>
<td>MAN, Fixed Point Communications (HiSpeed, OFDM, ARQ, Mesh)</td>
<td>5-6</td>
<td>134</td>
<td>Unlicensed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Same as above plus Mobility, OFDM, OFDM-A, WiMAX</td>
<td>2-6</td>
<td>1.5-20 MHz</td>
<td>134</td>
<td>Licensed</td>
<td>2Q05</td>
</tr>
<tr>
<td>802.17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.18</td>
<td>Radio Regulatory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.19</td>
<td>Coexistence Assurance</td>
<td></td>
<td>1/F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.20</td>
<td>Mobile Broadband Wireless Access (MBWA)</td>
<td>&lt; 3.5</td>
<td>1.25 to 40 MHz</td>
<td>1/user</td>
<td>Licensed</td>
<td>1Q05</td>
</tr>
<tr>
<td>802.21</td>
<td>Handoff/Interoperability Between Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.22</td>
<td>Cognitive Wireless Regional Area Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canopy</td>
<td>Motorola Proprietary MAN, BFSK PHY</td>
<td>5-6</td>
<td>20 MHz</td>
<td></td>
<td>Unlicensed</td>
<td>Now</td>
</tr>
</tbody>
</table>

---

18 Source: SRC.
IEEE 802.11 Standard (aka ISO/IEC 8802-11-1999)

**Title:** IEEE Standard for Information Technology-Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium. Access Control (MAC) and Physical Layer (PHY) specifications.

**802.11a**

**Title:** Supplement to IEEE Standard for Information Technology-Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-Speed Physical Layer in the 5 U-NII GHz Band.

**Scope:** FEC was added to the specification to improve the reliability and utilization of the channel: this improves performance by reducing recoverable frame loss. It uses OFDM modulation and subdivides the spectrum in 8 non-overlapping 20-MHz-wide channels. Each channel is further subdivided into 52 subcarriers (each ~300-kHz wide). OFDM enables sending data symbols on different sub-carriers in parallel; hence, a maximum data rate of 54 Mbps is achievable. The range is ~ 3km.

**Schedule:** Completed. Good candidate for fixed-point backhaul.

**802.11b**

**Title:** Supplement to IEEE Standard for Information Technology-Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4-GHz ISM Band.

**Scope:** This standard uses DSSS, offering 11 Mbps whenever possible, or dropping to 5.5, 2, and 1 Mbps if signal strength or interferences disrupt the transmission. Uses a CCK (code) to decode the transmission, even with substantial noise and multipath interference. Short range: 300 meters (open area), 122 meters (closed area).

**Schedule:** completed.

**802.11g**

**Title:** Supplement to IEEE Standard for Information Technology-Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4-GHz ISM Band, up to 54 Mbps.

**Scope:** Backward compatible with 802.11b, adapts OFDM from 802.11a, with max throughput of 54 Mbps; not as scalable as 802.11a (3 non-overlapping channels); ranges up to 3 km.

**Schedule:** completed

---

802.11i

**Title:** Supplement to IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhanced Security Mechanisms.

**Schedule:** completed.

802.11j

**Title:** Supplement to IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: 4.9 GHz – 5 GHz Operation in Japan.

**Scope:** Amendment (Annex J) to extend the clause 17 OFDM PHY specification for operation in the 4.9-5 GHz band in Japan: Japan out-of-band spurious emission limits, upper limit of spurious emission, transmit power levels, transmit spectrum mask, with 10 and 20 MHz channelization.

802.11n

**Title:** Supplement to IEEE standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification Enhancements for Higher Throughput.

**Scope:** It addresses wireless LAN with higher throughput than provided by 802.11a, 802.11b, and 802.11g. The goal is to increase the overall system throughput by considering both PHY and MAC layer enhancements.

The scope of the MAC and PHY enhancements assume a baseline specification defined by 802.11 and its amendments and anticipated amendments a, b, d, e, g, h, i, and j. The enhancements shall be to support higher throughput. The amendment shall not redefine mechanisms in the baseline that do not pertain to higher throughput.

Some of the modes of operation defined in the HT amendment shall be backwards compatible and interoperable with 802.11a and/or 802.11g.

Existing 802.11 standards are typically designated by their peak physical data rates. For example, 802.11a has a peak data rate of 54Mbps. This amendment has chosen to use a performance metric of throughput measured at the MAC data SAP. This amendment seeks to improve the peak throughput to at least 100Mbps, measured at the MAC data SAP. Depending on the scenario, this represents an improvement of at least 4 times the throughput obtainable using existing 802.11 systems.

In order to make efficient use of scarce spectral resources in unlicensed bands, the highest throughput mode defined by the HT amendment shall achieve a spectral efficiency of at least 3 bits per second per Hertz for the PSDU. No other IEEE Wireless LAN standards provide significantly higher throughput than either 802.11a or 802.11g.
The high-throughput standard will be introduced as an amendment to the whole 802.11 specification set.

802.11p, Wireless Access in Vehicular Environment WAVE (DSRC)

The Dedicated Short-Range Communications (DSRC) Band proposes an interoperable structure of the spectrum based upon a vehicle-to-roadside model, national network infrastructure model. It follows the ANSI\textsuperscript{20}-accredited standard ASTM E2213-03 (ASTM-DSRC), which is based on IEEE 802.11a. The DSRC has been officially released on August 3, 2004 in the Federal Register as CFR 47 Parts 0, 1, 2, 90, and 95 for an effective application date of October 4, 2004.

The Orthogonal Frequency Division (OFDM) modulation enables 27-Mbps throughput on 10-MHz channels and 54-Mbps throughput on 20-MHz channels. (This is effectively 2.7bps/Hz.) The FCC has not yet specified the specific modus operandi of the band. Also, OFDM is less susceptible to multipath fading in an indoor environment, compared to other modulations (i.e., Code Division Multiple Access (CDMA), GPSK, or 8PSK).

802.11T - Wireless Performance Prediction (Recommended Practice)

There is a newly approved Work Group as of June 2004.

802.15

\textbf{Title}: IEEE standard for information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks - Specific requirements fall into several parts that follow.

\textbf{Part15.1:} Wireless Medium Access Control (MAC) and Physical Layer Specifications for Wireless Personal Area Networks (WPANs).

\textbf{Scope}: Physical Layer and MAC specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS), in order to achieve interoperability for data transfer between a WPAN device and an IEEE 802.11 device. The POS extends up to a 10-meter-diameter environmental sphere centered on the WPAN device, even in motion.

\textbf{Schedule}: completed

\textbf{Part15.2:} Co-existence of Wireless Personal Area Networks (WPANs) with other Wireless devices operating in Unlicensed Frequency Bands.

\textbf{Scope}: a recommended practice between 802.11b and 1999 DSSS devices at 1, 2, 5.5, and 11 Mbps and 802.15.1 – 2002 WPANs.

\textbf{Part15.3:} Wireless Medium Access Control (MAC) and Physical Layer Specifications for High-Rate Wireless Personal Area Networks (WPANs).

\textbf{Scope}: The high rate is defined to be at least 20 Mbps (e.g., used for file transfer).

\textbf{Schedule}: completed.

\textsuperscript{20} American National Standards Institute.
Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).

**Scope:** The highest rate is defined to be no more than 250 Kbps (e.g., used in toys and sensors).

**802.16**

**Title:** Standard air interface for Fixed Broadband Wireless Access systems.

**Scope:** Specifies the air interface, including the medium access control (MAC) layer and physical layer (PHY) of fixed-point-to-multipoint broadband wireless access systems providing multiple services. MAC can support multiple PHY-level specifications optimized for the frequency bands of the application; PHY includes a particular PHY specification applicable to system operation between 10 and 66 GHz.

**802.18**

**Title:** Regulatory Opportunity for Wireless Regional Access Networks (RANs).

**Scope:** Wireless Regional Area Networks designed to operate in the VHF/UHF TV bands, including mechanisms to protect incumbent licensees from harmful interference.

**802.19**

**Title:** Coexistence Assurance (CA) Methodology (for predicting the impact of mutual interference on network performance).

**Scope:** The proposed IEEE 802.19 Coexistence Assurance (CA) Methodology document will describe several methods for predicting the impact of mutual interference on network performance. Currently IEEE 802 does not have a standardized method for predicting impact of mutual interference on network performance between dissimilar wireless networks. Hence, there is no standardized method for assuring that dissimilar wireless networks coexist. Dissimilar wireless networks are designed according to different standards.

The IEEE 802.19 Wireless Coexistence Technical Advisory Group (TAG) intends to describe in the CA Methodology several modeling and evaluation techniques at several levels of precision. In order to predict the impact of interference, it is necessary to build an interference model. Such models can be built at different levels of precision. Examples of modeling and evaluation techniques that offer increasing levels of details to be discussed include: Analytical Interference Model, Hybrid Analytical/Simulation Model, and Simulation Model.

Interference Testing will also be considered. Simulations using multipath faders with the Nakagami model would be useful for indoor scenarios. Raleigh fading models are specified commonly by the International Telecommunication Union (ITU) for outdoor multipath scenarios. Log-normal models are used for urban outdoor environments.

**802.20**

**Title:** Mobile Broadband Wireless Access (MBWA).

**Target/Goal:** Enable worldwide development of cost-effective, spectrum-efficient, always-on, and interoperable mobile broadband wireless access systems in order to address user needs for:
mobile and ubiquitous internet access, transparent support of internet applications, access to enterprise intranet services, transparent access to infotainment and location services. This performance goal fills the gap between high-data-rate, low-mobility services and the high-mobility cellular networks.

**Scope**: Specification of the PHY and MAC layers of an air interface for interoperable packet-data mobile broadband wireless access systems that operates in licensed frequency bands below 3.5 GHz. Supports peak data rates per user in excess of 1 Mbps; supports vehicular mobility classes up to 250 Km/h; covers cell-size commensurate ubiquitous metropolitan area networks. The strengths of this system are: 1) handoff from one local area network (LAN) to another and 2) support for higher mobility (speed) and higher throughput.

**Schedule**: as shown in Table 13.

802.21, Handoff/Interoperability Between Networks

No information available

802.22, Cognitive Wireless Regional Area Networks

**Title**: Cognitive Wireless Regional Area Networks

**Target/Goal**: The IEEE 802 Executive Committee approved a Project Authorization Request (PAR) at the July 2004 plenary in Portland, Oregon. This PAR is pending approval by the IEEE-SA Standards Board. This proposed new standards project tentatively placed as IEEE P802.22, would address Cognitive Wireless Regional Area Networks designed to operate on an unlicensed, non-interfering basis on unused TV channels, pending the IEEE/NESCOM (New Standard Committee *within IEEE*) decision on the PAR.
ISO/IEC Wireless JPEG 2000 (JPWL, JPEG Wireless)


Title: Wireless JPEG 2000 (JPWL)

Scope:
This International Standard defines, in an extensible manner, syntaxes and methods for the protection against errors that may occur during the transmission of JPEG 2000 codestreams in accordance with their definition in the following parts of ISO/IEC 15444:

In this International Standard, these are referred to as Wireless JPEG 2000 (JPWL), and applications using JPWL are referred to as a JPWL system.

JPWL specifies a set of tools consisting of data added to JPEG 2000 codestreams and of file formats and error-protection techniques, necessary for error correction and signaling. This International Standard includes definitions of the semantics and values to be added, and suggests how these may be used. JPWL also provides guidelines for the use of JPEG 2000 in the context of error-prone environments.

It would be useful to have all future video streams — including closed-circuit television (CCTV) images — conform to this JPWL standard. This can save considerable bandwidth and improve reliability of images.

4.9 GHz, CCTV Technology Application

The data link rate per channel, the throughput\textsuperscript{21}, and the channelization of a band under a specific FCC mandate and standard are parameters that will affect the quality of the video transmission. In addition, standards providing features such as — compression algorithms, error-corrective codes, and error-sensitive code architecture (e.g., Error Sensitivity Table, Data leaving and partitioning, Headers redundancy, residual error signaling) — will contribute to improve the quality of service (QoS) of the transmission. Band channelization — three for 802.11b, eight for 802.11a — affecting frequency re-use and co-channel interference (CCI) will have an impact on the overall efficiency of the cell (station) for CCTV.

The performance capabilities should be further investigated to reveal an optimum use of the 4.9-GHz spectrum.

\textsuperscript{21} The data link rate decreases with distance. The throughput is the actual rate of information that can be transmitted accounting for various overheads, and is a factor of data link rate, PER, packet size, MAC efficiency.
<table>
<thead>
<tr>
<th>Band (in MHz)</th>
<th>Denomination</th>
<th>Bandwidth (in MHz)</th>
<th>Type</th>
<th>Power Limit – SPP-Antenna Gain</th>
<th>02. Std</th>
<th>Datalink Max. Rate (in Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4940-4990</td>
<td>Public Safety</td>
<td>50</td>
<td>Semi: Public Safety</td>
<td>1W - 20dB/1MHz - 9dBi</td>
<td></td>
<td>2-54</td>
</tr>
<tr>
<td>4990-5000</td>
<td>-</td>
<td>10</td>
<td>Radio Astronomy</td>
<td>-</td>
<td>N/A</td>
<td>2-54</td>
</tr>
<tr>
<td>5000-5150</td>
<td>-</td>
<td>150</td>
<td>Aero - Radionavigation</td>
<td>-</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5150-5350</td>
<td>ISM/U-NII.1-2</td>
<td>200</td>
<td>Public - Data</td>
<td>40-250 mW - 6dBi</td>
<td>11a</td>
<td></td>
</tr>
<tr>
<td>5350-5470</td>
<td>-</td>
<td>120</td>
<td>Radio Location</td>
<td>-</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5470-5725</td>
<td>WiFi Broadband</td>
<td>255</td>
<td>Public – WiFi</td>
<td>1W - 30 dBm</td>
<td>11a</td>
<td>20-54</td>
</tr>
<tr>
<td>5725-5825</td>
<td>ISM/U-NII.3</td>
<td>100</td>
<td>Public - Data</td>
<td>1W 30 dBm - 6-23dBi</td>
<td>11a</td>
<td>20-54</td>
</tr>
<tr>
<td>5825-5850</td>
<td>-</td>
<td>25</td>
<td>Radio Location ARRL</td>
<td>-</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5850-5925</td>
<td>WAVE - DSRC</td>
<td>75</td>
<td>ITS – Public Transportation</td>
<td>28.8 dBm,44.8dBm, 6dBi</td>
<td>11a</td>
<td>27-54</td>
</tr>
</tbody>
</table>
Motorola

Motorola’s line of point-to-point (PTP) and point-to-multipoint (PMP) operate in the 4.9 GHz, in a line-of-site and non-line-of-sight environments, over long distances, and across water and open terrain. The radios overcome the key degrading factors in all radio environments – signal attenuation, fading, dispersion and polarization taking advantage of the following radio technologies to maintain link reliability:

- **Multiple-Input Multiple-Output (MIMO)** – minimizes signal fading due to path obstructions or atmospheric disturbances
- **Intelligent Orthogonal Frequency Division Multiplexing (i-OFDM)** – transmits data on multiple frequencies, resulting in higher channel bandwidth and greater resistance to interference and signal fading
- **Advanced Spectrum Management with i-DFS** (Intelligent Dynamic Frequency Selection) – self-selects the frequency over which it can sustain the highest data rate at the highest availability
- **Adaptive Modulation** – continually optimizes modulation to transmit the maximum amount of data across the path while maintaining the highest levels of link quality
- **Spatial Diversity** – combats ducting and multi-path fading via space-diverse antennas at one or both ends of a link
- **Radios** – incorporate super-sensitive receivers delivering the highest possible system gains. Operating at Ethernet data rates up to 300 Mbps, the systems support a wide variety of demanding applications, including:
  - Handling last-mile and heavy-duty backhaul traffic
  - Migrating from an analogue to a digital network
  - Linking separate loops within individual buildings
  - Communicating between buildings
  - Linking networks in a campus setting
  - Quickly deploying emergency services, special operations and events
  - Transmitting across long distances, over water or around obstacles
  - Transmit data reliably over obstructed paths, across expanses of open terrain or water, or in areas with significant interference
- Backhaul more local loops using a single link
- Support bandwidth-intensive IP voice, video and data applications
- Combine E1 /T1 and Ethernet ports in a single radio
- Add capacity and redundancy to 6 GHz networks

**Antennas type example for 4.9 GHz**

Below are examples of PTP & PMP wireless links and their overall performance using different antenna types over a 10km and 20km path. This is a simple example; actual throughputs can only be calculated using a link planning tool such as Motorola’s Link Planner, available on the internet at: [Motorola LINKplanner](https://www.motorola.com/).

The narrowing of the beam increases antenna size and path gain which is a balance of path reliability and throughput vs. what is physically possible to be installed at the location. Increase over path reliability in many cases will reduce interference to adjacent or co-channels as the antenna beam is more directional and focused. The following table shows sample data rates that can be expected over these distances in the 4.9 GHz band, using various antenna options assuming that there is no interference:

<table>
<thead>
<tr>
<th>Sample Antenna Option</th>
<th>10km Link</th>
<th>20km Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.9Ghz PTP 10 MHz link</td>
<td>4.9Ghz PTP 20 MHz link</td>
<td></td>
</tr>
<tr>
<td><strong>Antenna Integrated with radio (23dBi)</strong></td>
<td><strong>2ft Dish (29.2dBi)</strong></td>
<td><strong>2ft Dish (29.2dBi)</strong></td>
</tr>
<tr>
<td><strong>3ft Dish (33.2dBi)</strong></td>
<td><strong>3ft Dish (33.2dBi)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>4ft Dish (34.7dBi)</strong></td>
<td><strong>4ft Dish (34.7dBi)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>6ft Dish (37.5dBi)</strong></td>
<td><strong>6ft Dish (37.5dBi)</strong></td>
<td></td>
</tr>
<tr>
<td>36 Mbps</td>
<td>67 Mbps</td>
<td>96 Mbps</td>
</tr>
<tr>
<td>75 Mbps</td>
<td>145 Mbps</td>
<td>178 Mbps</td>
</tr>
<tr>
<td>17 Mbps</td>
<td>42 Mbps</td>
<td>66 Mbps</td>
</tr>
</tbody>
</table>
Rural deployments are often easier than urban deployments due to there being less overall interference or 4.9 GHz noise this combined with higher gain, narrower beam width, antennas can provide a robust high throughput network.

**Sample Link performance**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Main Street to City Hall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Name</td>
<td>Main Street to City Hall</td>
</tr>
<tr>
<td>Customer Name</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>Link Type</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>Maximum Obstruction Height</td>
<td>0.00 Feet</td>
</tr>
<tr>
<td>Link Distance</td>
<td>9.42 Miles</td>
</tr>
<tr>
<td>Free Space Path Loss</td>
<td>-131.33 dB</td>
</tr>
<tr>
<td>Excess Path Loss</td>
<td>0.00 dB</td>
</tr>
<tr>
<td>User Throughput Expectation</td>
<td>Aggregate 203.18 Mbps</td>
</tr>
<tr>
<td>RF Frequency Band</td>
<td>TBD</td>
</tr>
</tbody>
</table>

**Installation Notes**

- Bearing to REMOTE from LOCAL: 329.6° from True North
- Bearing to LOCAL from REMOTE: 149.5° from True North
- Predicted Receive Power: -34.61 dBm to -44.61 dBm
- Predicted Link Loss: -126.33 dB to -136.33 dB

Perform the following checks during the installation:
1. Check with a GPS that you are installing at the correct location.
2. Check carefully the direction to the other end of the link. Either use a corrected compass or use the GPS waypoint feature about 300 meters from the installation location.
3. Keep directing the antenna until the correct Receive Power is achieved. This should ensure that you are not peaking on a sidelobe of the antenna.
4. An hour after disarming check that the mean value for the link loss is as predicted.

**Local Site**

- Site Name: Main Street
- Hardware Platform: PTP
- Antenna Type: Andrew 3ft Dual-Pol Parabolic, PX3F-52 (33.4dBi)
- Antenna Gain: 33.4 dBi
- Antenna Height: 300 Feet AGL
- Local Site Elevation: 767.7 Feet AMSL
- Feeder Cable: LMR600 (7.3 dB/100 ft)
- Feeder Length: 13.699 Feet
- Feeder Loss: 1 dB
- Spatial Diversity: N/A
- Local Site Location: 34°51' 26.0" N 81°54' 46.5" W

**Remote Site**

- Site Name: City Hall
**Hardware Platform**
- PTP

**Antenna Type**
- Andrew 3ft Dual-Pol Parabolic, PX3F-52 (33.4dBi)

**Antenna Gain**
- 33.4 dBi

**Antenna Height**
- 320 Feet AGL

**Remote Site Elevation**
- 859.6 Feet AMSL

**Feeder Cable**
- LMR600 (7.3 dB/100 ft)

**Feeder Length**
- 13.699 Feet

**Feeder Loss**
- 1 dB

**Spatial Diversity**
- N/A

**Remote Site Location**
- 34°58' 29.0" N 81°59' 50.0" W

### Link Throughput Availability

- **User Throughput Expectation**: Aggregate 203.18 Mbps
- **User Effective Throughput Rate Upstream**: 158.72 Mbps
- **User Effective Throughput Rate Downstream**: 44.46 Mbps
- **Link Symmetry**: Continuously Variable from 80:20 to 20:80
- **Availability**: 99.99998%
- **Outage**: 0.11 Minutes/Year
- **Worst Case Analysis**: Not Selected
- **Link Optimisation**: Optimised for IP Traffic

### Required User Throughput

- **Required User Mux Data Throughput (Mbps)**: 3.67
- **Link Availability for User Mux Data Throughput (%)**: 99.99998%
- **Outage for User Mux Data Throughput Minutes/Year**: 0.11
- **Required User Data Throughput (Mbps)**: 1.00
- **Total User Data Throughput including Mux Data (Mbps)**: 4.67
- **Link Availability for Total User Data Throughput (%)**: 99.99998%
- **Outage for Total User Data Throughput Minutes/Year**: 0.11

<table>
<thead>
<tr>
<th>Modulation</th>
<th>User Throughput(Mbps)</th>
<th>Aggregate Throughput(Mbps)</th>
<th>Fade Margin (dB)</th>
<th>%Time In Mode</th>
<th>Throughput Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>256QAM 0.81 Dual</td>
<td>294.33</td>
<td>4.61</td>
<td>0.00%</td>
<td>0.00000%</td>
<td></td>
</tr>
<tr>
<td>64QAM 0.92 Dual</td>
<td>247.98</td>
<td>-1.71</td>
<td>1.54%</td>
<td>1.53610%</td>
<td></td>
</tr>
<tr>
<td>64QAM 0.75 Dual</td>
<td>202.64</td>
<td>4.39</td>
<td>98.12%</td>
<td>99.66029%</td>
<td></td>
</tr>
<tr>
<td>16QAM 0.87 Dual</td>
<td>157.65</td>
<td>9.29</td>
<td>0.33%</td>
<td>99.98681%</td>
<td></td>
</tr>
<tr>
<td>256QAM 0.81 Single</td>
<td>147.16</td>
<td>0.29</td>
<td>0.00%</td>
<td>99.98681%</td>
<td></td>
</tr>
<tr>
<td>64QAM 0.92 Single</td>
<td>123.99</td>
<td>2.19</td>
<td>0.00%</td>
<td>99.98681%</td>
<td></td>
</tr>
<tr>
<td>16QAM 0.63 Dual</td>
<td>113.33</td>
<td>15.49</td>
<td>0.01%</td>
<td>99.99887%</td>
<td></td>
</tr>
<tr>
<td>64QAM 0.75 Single</td>
<td>101.32</td>
<td>7.99</td>
<td>0.00%</td>
<td>99.99887%</td>
<td></td>
</tr>
<tr>
<td>16QAM 0.87 Single</td>
<td>78.82</td>
<td>13.09</td>
<td>0.00%</td>
<td>99.99887%</td>
<td></td>
</tr>
<tr>
<td>16QAM 0.63 Single</td>
<td>56.66</td>
<td>19.59</td>
<td>0.00%</td>
<td>99.99966%</td>
<td></td>
</tr>
<tr>
<td>QPSK 0.87 Single</td>
<td>39.41</td>
<td>22.89</td>
<td>0.00%</td>
<td>99.99985%</td>
<td></td>
</tr>
<tr>
<td>QPSK 0.63 Single</td>
<td>28.33</td>
<td>26.89</td>
<td>0.00%</td>
<td>99.99994%</td>
<td></td>
</tr>
<tr>
<td>BPSK 0.63 Single</td>
<td>14.16</td>
<td>31.39</td>
<td>0.00%</td>
<td>99.99998%</td>
<td></td>
</tr>
</tbody>
</table>

### Regulatory Conditions
<table>
<thead>
<tr>
<th>Region Code</th>
<th>Region 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max EIRP</td>
<td>57.4 dBm</td>
</tr>
<tr>
<td>Output Power</td>
<td>25 dBm</td>
</tr>
<tr>
<td>In Band Environmental Noise</td>
<td>-80 dBm/30MHz</td>
</tr>
</tbody>
</table>

The calculations for this link estimate were made assuming an output power of 25 dBm in the lowest modulation mode.

---

**APPENDIX C ACRONYMS**

- **ARQ**: Automatic Repeat Request
- **BFSK**: Biphase Shift Keying
- **DSL**: Digital Subscriber Line
- **DSRC**: Dedicated Short Range Communications
- **DSS**: Direct Sequence Modulation
- **DSSS**: Direct Sequence Spread Spectrum
- **EMS**: Emergency Medical Services
- **ECSG**: Executive Committee Study Group
- **ETSI**: European Telecommunications Standards Institute
- **FHSS**: Frequency Hopping Spread Spectrum
- **FXB**: Fixed Broadband class 4.9 GHz license having primary status
- **FXO**: Fixed Narrowband class 4.9 GHz license having secondary status
- **GPSK**: Gaussian Phase Shift Key
- **ITS**: Intelligent Transportation System
- **ITU**: International Telecommunications Union
- **LAN**: Local Area Network
- **MAN**: Metropolitan Area Network
- **MBOA**: The Multiband OFDM Alliance
- **MBWA**: Mobile Broadband Wireless Access
- **MEA**: MeshNetworks Enabled Architecture
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MESA</td>
<td>Project Mobility for Emergency &amp; Safety Applications</td>
</tr>
<tr>
<td>MO</td>
<td>Mobile Operations class 4.9 GHz license having primary status</td>
</tr>
<tr>
<td>NESCOM</td>
<td>New Standard Committee (within IEEE)</td>
</tr>
<tr>
<td>NPSTC</td>
<td>National Public Safety Telecommunications Committee</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Networks</td>
</tr>
<tr>
<td>RANS</td>
<td>Regional Access Networks</td>
</tr>
<tr>
<td>RR_TAG</td>
<td>Radio Regulatory Technical Advisory Group</td>
</tr>
<tr>
<td>SWAN</td>
<td>Structured Wireless-Aware Network</td>
</tr>
<tr>
<td>TIA</td>
<td>Telecommunications Industry Association</td>
</tr>
<tr>
<td>TSACC</td>
<td>Telecommunications Standards Advisory Council of Canada</td>
</tr>
<tr>
<td>TTA</td>
<td>Telecommunications Technology Association (Korea)</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra Wide Band</td>
</tr>
<tr>
<td>VARs</td>
<td>Value Added Resellers</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Networks</td>
</tr>
<tr>
<td>WPANS</td>
<td>Wireless Personal Area Networks</td>
</tr>
</tbody>
</table>