

# PSTN Transition Issues

## 1. Copper Retirement

- What services remain dependent upon the existing twisted-pair copper plant? What services may no longer be available if twisted pair copper is no longer offered from customer premises to the wire center? What non-voice services and features will not work without modification in an all IP-based network?
- What substitutes exist for services that may not be able to transition from the analog circuit-switched network? What is the cost or technological impact of the substitute?
- As landline voice service decreases, what fraction of copper loops is left idle, rather than serving as DSL loops or being put to other use? How is non-voice demand for copper loops expected to change over 5-10 years?
- Are there practical uses of abandoned copper and if so, what are the uses, and what are the costs (or cost drivers) and technological impediments to putting such copper to use?

## 2. PSTN Users

- What technologies might encourage or ease transitions to IP-based networks for consumers, especially those who might otherwise find a transition disruptive?
- For consumers who only want to pay for a fixed voice connection, are there cost-effective mechanisms for supplying that connection if there is no circuit-switched last mile, such as standalone managed VoIP service over DSL or fixed wireless service? What are potential issues when running VoIP over (fixed) LTE, whitespace wireless, or other fixed wireless access solutions?



# PSTN Transition Issues

## 1. Interconnection Group A

- What methods have evolved for the exchange of traffic in the hybrid IP-based/circuit-switched network? How will those methods transition as the network shifts to being wholly IP-based?
- How might interconnection requirements and provisioning evolve as consumers adopt new communications technologies, such as HD voice or video?

## 2. Database Transition Group A

- What legacy databases will need to transition to a future all-IP environment?
- How will databases that are essential to the operations of the PSTN need to evolve to operate in an IP-based network?



# PSTN Successor Infrastructure

## 1. Interconnection Group B

- Do technological interconnection issues exist at higher protocol levels, e.g., SIP?
- What architectures might evolve to support VoIP interconnection and interconnection of advanced communications services? How would architectures function at different network layers (e.g., MPLS, IP, SIP)?
- Develop a detailed matrix of technical issues that need to be worked out for an IP interconnection framework, the entities who would need to be involved in each aspect, and preliminary thoughts on possible technical solutions.

## 2. Numbering Group B

- What changes might be expected in a numbering plan optimized for IP-based communications services? (For example, current numbering systems are tied to physical resources, such as lines, and are often service specific, e.g., SMS short codes.)
  - What are the obstacles to assigning numbers to users, analogous to how domain names are assigned, rather than to service providers?
  - Should number assignment need to retain a geographic component? For example, do numbers still need to be assigned to specific rate centers in an all-IP world?
  - How can the receiver of a call validate that the caller is authorized to use the number or other identifier (“caller ID validation”)?
  - What role is ENUM going to play as a number mapping service as the numbering system evolves? Is there a need for additional or alternate solutions?
- How might technological changes drive signaling requirements and number translation capabilities?



# PSTN Successor Infrastructure

## 3. Database Transition Group B

- What new databases or database architectures will be necessary or helpful in an all-IP network?
- To what extent are these new databases already developing? Who is developing them? What challenges does their development face?

## 4. Quality of Service

- How will the use of end-to-end IP connectivity impact QoS? Is there a need for defined call quality metrics? How can we properly measure and assess the difference in QoS in IP service relative to circuit-switched service? What are the complexities associated with measuring IP QoS?
- What entity or entities can best perform reliable, unbiased and comprehensive QoS testing? Can this be done by industry and/or government groups or labs and if so, do such groups/labs exist already?
- Can end-to-end QoS be provided across service providers? What models seem possible (e.g., DiffServ, resource reservation, separate physical, or L2 networks)?
- How would the use of multiple media (high-quality audio, video) impact QoS considerations?

# PSTN Successor Infrastructure

## 5. Robustness and Public Safety

- How will the transition affect network robustness?
- What will robustness likely improve or degrade in the transition?
- What technologies can improve network survivability? How effective are these technologies likely to be compared to existing PSTN survivability?
  - Wireless
    - Backup power at base station and handsets?
    - Capacity vs. footprint tradeoffs
  - Wireline
    - Backup power for both the network and home or small business environments?
- What, if any, additional capabilities are needed from the underlying broadband network to enable 911 or other emergency services functionality that is at least equivalent to that offered by the existing system?



# Receivers and Spectrum

1. What resources are available on the performance of receivers, particularly relative to adjacent channel rejection?
2. What are the gaps in what is known about receiver performance, particularly relative to particular services that rely on reception of weak signals such as radar and satellite services?
3. What work should be undertaken to close these gaps?
4. Who should perform this work and what role should the FCC play relative to closing the knowledge gaps relative to receiver performance?
5. How can information about receiver performance be made more transparent to prospective users of spectrum that is a candidate for repurposing?
6. To what extent is it important to have access to such information for federal systems?



# Receivers and Spectrum

7. To what extent do national security concerns come into play in making information available about receiver performance for both federal systems and non-federal public safety and critical infrastructure systems?
8. What particular parts of the spectrum are of greatest priority for study of receiver performance and how it might affect access to spectrum for new services?
9. How might the FCC best approach receiver performance from both a technical and policy perspective?
10. If performance metrics were established for receivers, what parameters should be subject to these metrics and how should criteria for performance be derived?
11. What approaches should be taken relative to receivers that do not conform to the metrics?
12. How should the Commission address situations where there is a significant issue relative to legacy equipment? For example, should the FCC establish transition periods based on the full expected life of most legacy equipment or take steps to enable faster deployment of new services?



# Multi-band/Multi-mode Devices

1. What are the challenges that face commercial wireless service providers and equipment manufacturers in providing service across multiple frequency bands and multiple mode of operation?
2. How are they approaching these challenges? For example, are the carriers and equipment manufacturers forced to choose which bands they will cover in any particular area or device based on technical limitations? How is interoperability managed for multiple-mode of operation?
3. How will these challenges become more difficult or easier in the near term and long term future?
4. What are the challenges relative to filter technology both from a transmitter and receiver standpoint?
5. What are the challenges relative to antenna technology?



# Multi-band/Multi-mode Devices

6. How do these various factors affect performance and quality of service? For example, does the need to operate across multiple bands necessarily lead to compromises in the ability to receive weak signals or reject interference?
7. Are challenges mostly on hardware? Any firmware challenges such as preferred system acquisition?
8. What is the impact on battery life?
9. What are the limitations today on the frequency range that can be covered by a multi-band device? How might they change in the future?
10. How would the availability of frequency bands above 3 GHz for small cell deployment such as the 3550 – 3650 MHz band or the 5 GHz Wi-Fi bands affect the availability and use of multi-band devices covering these frequency ranges?



# Multi-band/Multi-mode Devices

11. How will the availability of new spectrum in the 600 MHz range recovered through a voluntary incentive auction affect the design and availability of multi-band devices?
12. What is the process of Multi-band/Multi-mode device certification and type approval process? Is there a room for improvement?



# Wireless Apps and Services

1. What is the experience thus far in the development of wireless apps and services?
2. What obstacles have been encountered by carriers, innovators and users in the introduction of these services?
3. What are the current friction points relative to the availability of wireless apps and devices for health care? For energy? For education? Public safety?
4. What specific steps can be taken to reduce or remove these friction points?
5. What are the principal M2M applications today?
6. What impact are those M2M applications having on the networks?
7. What is the projected growth of M2M applications and what impact are they expected to have on the networks in the future?



# Wireless Apps and Services

8. Are particular M2M data hungry applications such as video surveillance and monitoring anticipated to have a particular impact on the networks? If so, how will they be dealt with?
9. How does the current industry process work for approval of new apps and M2M services & devices?
10. Do the carriers have any pre-defined boundaries or parameters necessary to obtain approval of wireless apps, services and devices?
11. Are there things the industry can do to improve this process?
12. What can the FCC and other federal agencies do to improve the availability of new wireless apps, services and devices?
13. What privacy issues exist in the introduction and operation of wireless apps and services? What existing regulations affect such issues? How should industry standards and practices be developed to ensure that the rights of users are protected?
14. What capabilities exist in the design of standard application platforms such as IOS, Android, and Windows 8 to ensure appropriate privacy of end user data?



# Wireless Security and Privacy

1. What are the chief areas of concern relative to the security of commercial wireless networks, and how would you prioritize them and why?
2. Recognizing that today's mobile communication devices house multiple transceivers operating on multiple bands – each operating independently from one another – what are the security vulnerabilities associated with each of those RF transceivers?
3. What are the most significant privacy issues from a wireless technology point of view, and how should the Commission begin to address them?
4. Is the air interface the most appropriate area in which to focus? If not, what areas are most appropriate?
5. What are the security features of today's wireless networks?
6. What are the security features that will be introduced for the next generation of wireless technology?
7. What is the scope of potential vulnerabilities? For example, could security vulnerabilities lead to service outages? Hacks of private information?



# Wireless Security and Privacy

8. How does the industry identify breaches in security?
9. What response systems are in place for dealing immediately with security attacks?
10. Are different levels of security available to users depending upon the type of application? For example, can public safety or critical infrastructure applications be provided with greater security than an ordinary smart phone?
11. To what extent is jamming a concern and what has the experience been thus far? What is and can be done about this?
12. To what extent is theft of service a concern and have there been instances where this has occurred already? What can and is being done about this?
13. To what extent is the industry addressing concerns about privacy?
14. What roles should the FCC and other federal agencies play in this area?

