

Technical Advisory Council
 Federal Communications Commission
 Summary of Meeting
 December 4th, 2014

The Technical Advisory Council (TAC) for the FCC was convened for its fifteenth meeting at 1:00 P.M. on December 4th, 2014 in the Commission Meeting Room at the FCC headquarters building in Washington, DC. A full video transcript of the meeting is available at the FCC website at <http://www.fcc.gov/encyclopedia/technology-advisory-council> together with a copy of all materials presented at this meeting. In addition, all materials presented at this meeting are included in electronic form in an Appendix to this document.

In accordance with Public Law 92-463, the entire meeting was open to the public.

Council present:

Shahid Ahmed, Accenture	Russ Gyurek, Cisco Systems
John Barnhill, Genband	Dale Hatfield, Silicon Flatirons Center for Law, Technology, and Entrepreneurship University of Colorado at Boulder
Mark Bayliss, Visual Link Internet, Lc	Theresa Hennesy, Comcast Corporation
Nomi Bergman, Bright House Networks	Kevin Kahn, Intel Corporation
Peter Bloom, General Atlantic	Steve Lanning, Viasat, Inc
Mark Bregman, Neustar	Gregory Lapin, Independent Consultant
Ed Chan, Verizon	Brian Markwalter, Consumer Electronics Association
Greg Chang, YuMe, Inc.	Tom McGarry, Neustar
John Chapin, DARPA	Milo Medin, Google, Inc
Lynn Claudy, National Association of Broadcasters	Ramani Pandurangan , XO Communications
Marty Cooper, Dyna LLC	Jesse Russell, incNetworks
Brian Daly, AT&T	Marvin Sirbu, Carnegie Mellon University
Pierre De Vries, Silicon Flatirons Center for Law, Technology, and Entrepreneurship University of Colorado at Boulder	Kevin Sparks, Alcatel-Lucent
John Dobbins, EarthLink, Inc.	Paul Steinberg, Motorola
Adam Drobot, OpenTechWorks	David Tennenhouse, VMWare
Erik Ekudden, Ericsson North America	Jack Waters, Level 3 Communications LLC

FCC staff attending in addition to Walter Johnston and Julius Knapp included:

Michael Ha
Scott Jordan
Tom Wheeler
David Simpson

NTIA staff attending:

Rangam Subramanian

Meeting Overview

Dennis Roberson, TAC Chairman, began the meeting asking the TAC members to introduce themselves. Each TAC Work Group chairperson next provided a summary of their work activities for the year as well as presenting final recommendations for the 2014th work program.

A copy of all presentations is attached herein.

Technological Advisory Council

12-4-2014



Agenda

- Mobile Device Theft Working Group
- IIT Student Presentation
- Cybersecurity Working Group
- Internet of Things Working Group
- 477 Testing Working Group
- Advanced Sharing and EWG Working Group
- Spectrum and Receiver Performance Working Group
- Supporting the Transition to IP



Technological Advisory Council

Mobile Device Theft Prevention WG

December 4th, 2014



Agenda

- Mission & Working Group Participants
- MDTP Findings
- Top Priority Recommendations
- Additional Recommendations
- Next Steps



MDTP WG Mission

- On June 19, FCC Chairman Tom Wheeler directed the TAC to form a working group to develop industry wide recommendations to mitigate the increasing theft of mobile devices
 - Chairman Wheeler asked for specific actionable recommendations to combat mobile device theft by the end of 2014
- The TAC Mobile Device Theft Prevention Working Group, announced on July 24, quickly organized to fulfill its charge of exploring the problem of mobile device theft and developing recommendations to the FCC to deter and mitigate mobile device theft



WG Participants

- Co-Chairs:
 - Brian Daly, AT&T
 - Rob Kubik, Samsung
- FCC Liaisons:
 - Walter Johnston
 - Charles Mathias
 - Elizabeth Mumaw
- Alan Bersin, DHS
- Asaf Askenazi, Qualcomm
- Ayal Yogev, Lookout
- Ben Katz, Gazelle
- Brad Blanken, CCA
- Chris Bender, Motorola Mobility
- Christian Schorle, FBI
- Craig Boswell, Hobi
- David Strumwasser, Verizon
- Deepti Rohatgi, Lookout
- Dennis Roberson, FCC TAC Chair
- DeWayne Sennett, Editor (AT&T)
- Eric Feldman, ICE/Homeland Security Investigations
- Gary Jones, T-Mobile
- Greg Post, Recipero
- Ian Robertson, Motorola Mobility (Lenovo)
- Irene Liu, Lookout
- Jake Laperruque, Center for Democracy and Technology
- James Moran, GSMA
- Jamie Hastings, SME (CTIA)
- Jason Novak, Apple
- Jay Barbour, Blackberry
- Jeff Brannigan, DHS
- Joe Heaps, National Institute of Justice
- John Foust, Metropolitan Police, Washington, DC
- John Marinho, CTIA
- Kirthika Parmeswaran, iconectiv
- Les Gray, Recipero
- Mark Romer, Asurion
- Matt Rowe, Gazelle
- Mike Rou, eBay
- Maxwell Szabo, City and County of San Francisco
- Nick Tucker, Microsoft
- Ron Schneirson, Sprint
- Samir Vaidya, Verizon
- Samuel Messinger, U.S. Secret Service
- Sang Kim, LG



MDTP Findings

No common national framework for smartphone anti-theft mitigation

No current official national or international smartphone theft statistics

- Industry database has only been operational in the U.S. for the past few years
- Large number of law enforcement agencies makes aggregation of mobile device theft data a significant challenge
- Improved data collection is necessary to understand if measures being implemented are effective

MDTP Working Group obtained preliminary data from 22 police jurisdictions supporting the view that smartphone theft is a major issue in the U.S.

Destination of the millions of stolen smartphones is unknown



MDTP Findings (continued)

Industry groups (e.g., CTIA, GSMA-NA) have developed voluntary commitments and best practices on smartphone theft mitigation

- Major manufacturers and OS providers have committed to providing device-based solutions by July 2015 (CTIA)
- Not all mobile service providers have adopted these commitments
- Best practices need to be enhanced over time

No “silver bullet” that will eliminate smartphone theft

- A complementary suite of technical and operational mitigation techniques must be made available and applied to gain additional impact to mobile device theft
- There is evidence that implementation of specific solutions is impacting criminal activity
- Secure technology solutions are required to ensure unique device identifiers on all smartphones



MDTP Findings (continued)

Law enforcement needs a better understanding of anti-theft tools available to aid theft investigations; more user-friendly anti-theft tools for law enforcement will be a critical component of a successful solution

Consumers must understand the benefit to broadly adopt phone theft deterrent measures – “opt-out” solutions should be the norm going forward

The most effective anti-theft messaging comes from local law enforcement

- Service provider and manufacturer outreach is needed to supplement this effort



Top Priority Recommendations



National Framework

The FCC TAC recommends that the FCC establish a national framework for smartphone anti-theft measures that would include:

- Using the CTIA “Smartphone Anti-Theft Voluntary Commitment” and the existing laws in California and Minnesota as input
- Exploring the basis for preemption to prevent fragmentation of requirements
- Establishing a single law enforcement point of contact to serve as a clearinghouse of information and expertise on mobile device theft
- Defining a process for the capture of comprehensive data, while addressing privacy considerations



National Framework - continued

- Tasking CSRIC with developing methods for law enforcement to obtain device identifiers from smartphones
- Tasking ATIS with developing standards to obtain device identifiers
- Tasking CTIA to convene a joint task force to define consumer outreach recommendations
- Developing a reseller code of practice to prevent the trade of stolen devices
- Remaining technology neutral
- Continuing MDTP working group focus on this issue



Deploy and Continue to Evolve Technology Solutions

- Baseline anti-theft solutions which during initial device setup process, prompts an authorized user to enable the technological solution to allow:
 - Remote wiping of the authorized user's data
 - Rendering the smartphone inoperable to an unauthorized user
 - Preventing reactivation without authorized user's permission
 - Reversing the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible
- Securing mobile device identifiers / making identifiers resistant to change
- Expanding use of existing databases and deployment of technology for network operator blocking of identified stolen devices

Engaging Consumers

- The FCC TAC recommends that the FCC seek input from consumer organizations on how consumers are utilizing the anti-theft solutions and related security capabilities available on their devices
- The FCC TAC recommends the FCC work with industry on additional consumer education efforts



Engaging Law Enforcement

- The FCC TAC recommends that the FCC reach out to the following organizations to effectuate a comprehensive and effective consumer outreach effort:
 - The Major Cities Chiefs Association
 - The International Association of Chiefs of Police
 - The National Sheriffs Association
 - The National Crime Prevention Council
 - ASIS International
- The FCC TAC recommends that the FCC develop a “kit” to be shared with local law enforcement agencies for the purpose of educating consumers on how they can protect their smartphones, their data and what to do if their smartphone is lost or stolen.



Engaging the International Community

- The FCC TAC recommends that the FCC Chairman encourage his international counterparts to become more engaged on the Mobile Device Theft Prevention issue to:
 - Promote adoption of shared network-based solutions (e.g. GSMA database) globally, which will extend the reach of device blocking and increase deterrence of device trafficking
 - Promote greater coordination and cooperation on this global issue



Additional Recommendations



Industry Reporting

- GSM Association's North American Regional Interest Group and CTIA jointly develop a process to report to the FCC statistics on devices reported lost or stolen over a 12 month period
- GSM Association's North American Regional Interest Group develop best practices and guidelines on how to measure and report on blacklisted devices



Device Identifier and Enrollment Status Check

- CTIA in coordination with the carriers and wireless industry develop a procedure to lookup smartphone IMEI/MEID status
- Smartphone anti-theft solution providers should offer a mechanism to check if a smartphone is enrolled in a device-based anti-theft solution
- Additional recommendations regarding reverse logistics are detailed in the report



Study and Assessment

- FCC should continue the efforts of the TAC to address further work items including:
 - Ongoing study and monitoring of the dynamic and changing threat environment
 - Ongoing study and consideration of new and emerging technologies and global standards for the purpose of aiding in the mitigation of smartphone theft
 - An annual assessment of smartphone theft and the effectiveness of the measures undertaken to combat it



Mobile Device Theft Prevention WG Summary & Next Steps

- Mobile device theft is a significant national and international problem
- Theft mitigation requires broad participation from industry, law enforcement, consumers, and the FCC
- Activities initiated by the FCC TAC should continue until there is an effective resolution





S T E P S

Solutions That Enable Phone Security



| Our Focus

Smart device owners care the most about their devices at these moments of truth:

Purchase

Loss



| Meet Lauren

Lauren is your
“typical”
college student.



34%
Set Pin



73%
Own
second
device



85%
Phone is
central to
life

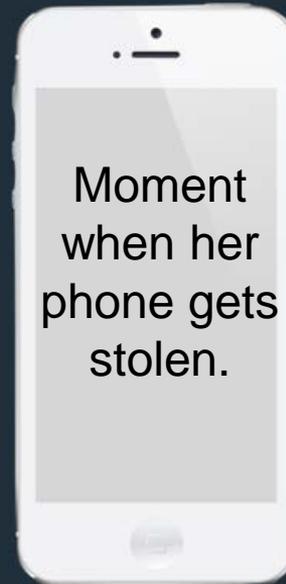


| Lauren's Story before STEPS

Does not set pins

**Does not set up
Cloud Storage**

**Does not tether
Secondary Device**



Phone gets stolen

Identity data at risk

Personal media lost



How many of you have had a
device get lost or stolen?



| Class Themes

Tethered Secondary Device

Device that is connected to the phone via Bluetooth, wireless, or 4G and can erase data remotely if the device is stolen.

Security Software

Third Party app that can remotely wipe out the data on the device

Cloud based Phone

Device that stores all of its data on the cloud.

Hardware Components

Separate components that keep security software functioning even when the device is off or the battery removed.



| S.T.E.P.S



1

Required Pins

Multiple Pins set up at time of activation



2

Secondary tethered device

Tethered Device with Kill Switch and Cloud Backup capability



3

Fraud Detection

OS feature that logs usage pattern and alerts Provider of suspicious activity

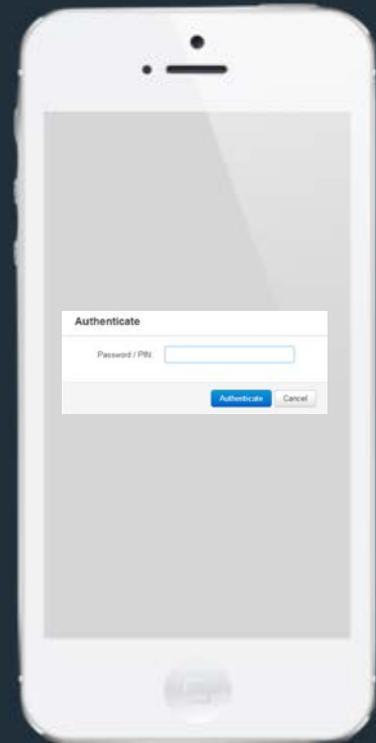
**Lauren buys a new phone!
(She's excited.)**





1 Required PINs ● ● ● ●

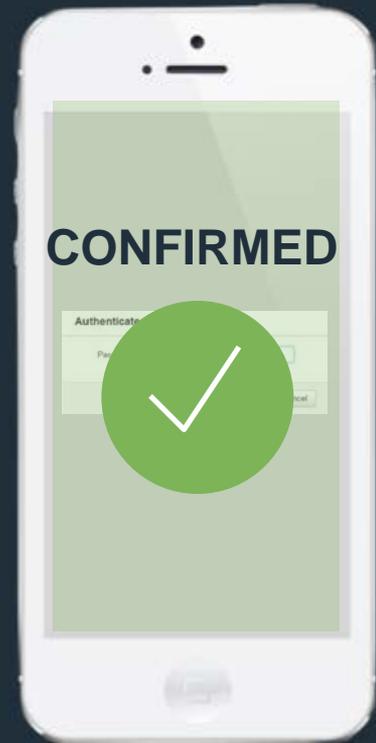
Lauren's phone prompts her to set up her pin.





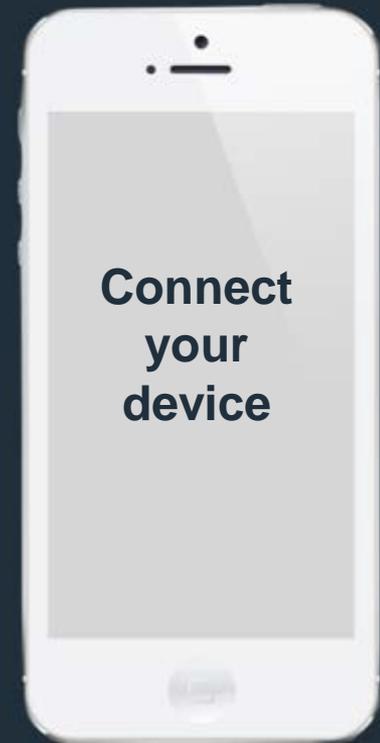
1 Required PINs ●●●●

Lauren's phone prompts her to set up her pin.



2 Tethered Secondary Device

Lauren's phone also prompts her to connect one her secondary devices as a tether for security.





2 Tethered Secondary Device

Lauren's phone also prompts her to connect one her secondary devices as a tether for security.



2 Tethered Secondary Device

Lauren's phone also prompts her to connect one her secondary devices as a tether for security.

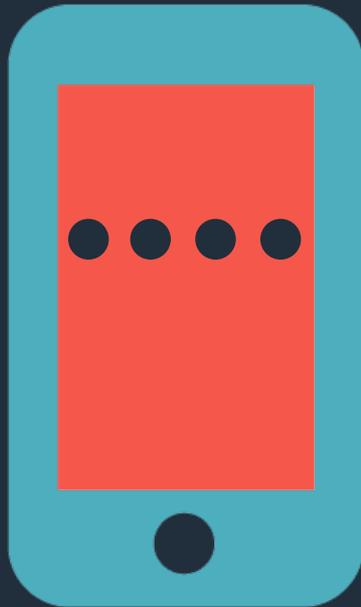


**Oh no! Lauren's device
gets stolen.**





Security Layer 1: Required Pins



Denied.

Lauren's three pins will prevent the thief from accessing her phone.



Security Layer 2: Secondary tethered device





Security Layer 2: Secondary tethered device





Security Layer 2: Secondary tethered device



Kill.



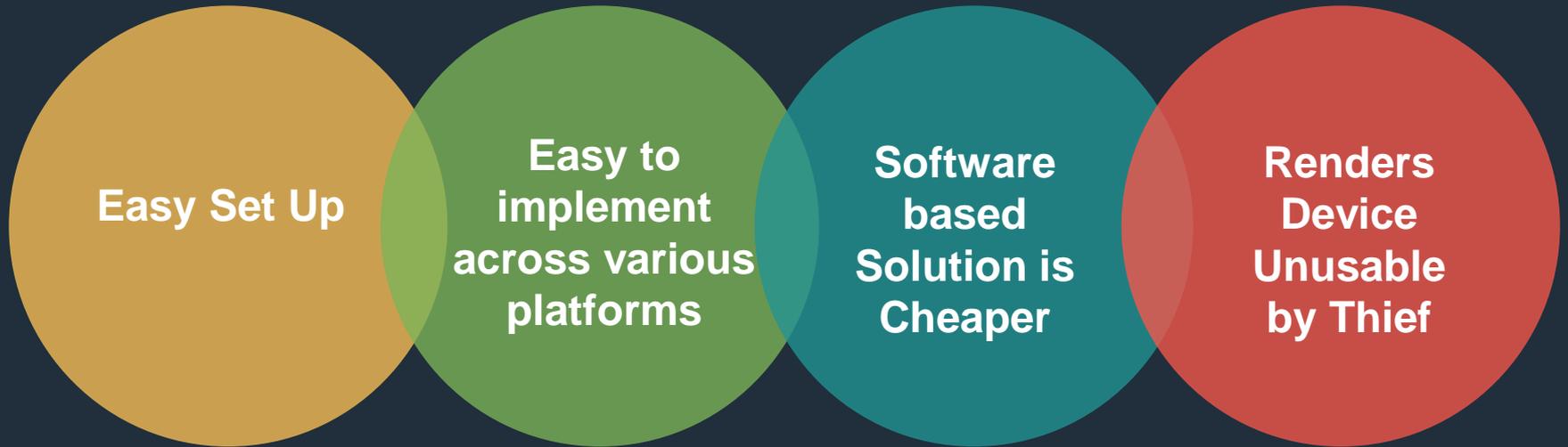
Security Layer 3: Fraud Detection



Lauren's phone alerts her cell phone provider that someone is making calls to a foreign destination.



| Benefits of S.T.E.P.S





Thank you!
Questions?

Cybersecurity Working Group

Chair: Paul Steinberg
Vice Chair: Ramani Pandurangan
FCC Liaisons: Jeffery Goldthorp,
Lauren Kravetz

4-December-2014



Mission Statement

New security vulnerabilities in software and hardware continue to emerge, imposing even greater externalities and societal costs on users. Security software is widely available, but most security solutions aim to protect software and hardware after systems have been built and deployed. Software and hardware security are too frequently seen as an afterthought or a potential hindrance to businesses, routinely addressed after a product is released into the marketplace. Improving security and reducing the aftermarket and social costs of security failures requires building security into software and hardware at the initial stages of the design and development process.

- What collaborative activities within or between industry and government organizations focus on building security into software and hardware, and how can these or other collaborative activities be strengthened, modified, or initiated to more effectively address security problems? How can the FCC act to promote the effectiveness of these activities?
- How can the FCC collaborate with academic institutions to bridge the gap between current computer sciences curriculums, which lack focus on security as a core tenet, and the need for secure coding as an integral piece of computer sciences degrees?

Mission Statement Key Objectives

- How do threats appear in the supply chain paradigm, and how can supply chain resiliency be improved to address these issues?
- What are the most important considerations that should be addressed in determining how software and hardware are designed and developed to reduce the number of security patches that are needed post-deployment?
- Who are the important stakeholders, and how can new or smaller manufacturers and vendors be included in the process?
- What processes are needed to allow for the open sharing of software and hardware security threats and solutions, while providing adequate safeguards for confidential information?
- Where can new or modified procedures highlight and address software and hardware security concerns in the design and development process?
- What technical measures can manufacturers and vendors take, as part of the design and development process, to reduce the risk their products will have security issues post deployment?
- How can training be improved to help manufacturers and vendors build security into software and hardware?
- What roles, if any, do testing and auditing have to play in building security into software and hardware, and how can they be used more effectively?

Working Group Members

- WG Chair: Paul Steinberg, Motorola Solutions
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Lauren Kravetz

- Members:
 - Ernie Bio, incNetworks
 - Brian Daly, AT&T
 - Renato Delatorre, Verizon Wireless
 - Martin Dolly, AT&T
 - Adam Drobot, Open Tech Works
 - Jeff Foerster, Intel
 - Russ Gyurek, Cisco
 - Mike McNamara TWTelecom
 - Lynn Merrill, Monte R. Lee
 - Jack Nasielski, Qualcomm
 - Katherine O'hara, Verizon
 - Anand Palanigounder, Qualcomm
 - Deven Parekh, Insight Partners
 - George Popovich, Motorola Solutions
 - Jesse Russell, incNetworks
 - Harold Teets, TWTelecom
 - S Rao Vasireddy, Alcatel Lucent
 - Jack Waters, Level 3 Communications



Cybersecurity Working Group

Projects requested by the FCC for the 2nd half of 2014

1. Mobile Device Consumer Interface for Privacy & Security
 - Enhance & Automate FCC Security Checker in a User-friendly way (CAC/TAC Collaboration)
2. Security Practices for Core Network Equipment
 - Cyber Rating/Certification for Equipment (Analogous to a Cyber UL Rating)
3. Future Mitigation Technologies for Insider Threats
 - Identify Promising Nascent Technologies for Mitigation of Insider Threats that the FCC could advance



Lead: George Popovich

1. MOBILE DEVICE CONSUMER INTERFACE FOR PRIVACY & SECURITY



Mobile Device Consumer Interface for Privacy & Security

- Background

- The Public Safety and Homeland Security Bureau and the Consumer and Government Affairs Bureau are working on a consumer-facing cyber security and privacy project
- The FCC’s long term goal is to enable consumers to configure security/privacy decisions in a simple, consistent manner that automatically triggers the appropriate settings on any platform
- The FCC is exploring the development of a consumer education app focused on mobile security

- Requests of the Cyber Security Work Group

- Explore a consumer education smartphone app focused on mobile security
- Discuss a plan for how platforms and providers could best interface with consumers
- Look for means of the existing FCC Smartphone Security Checker to be updated from a technical perspective, including developing “plain English” consumer content

- Progress since the September update

- We collaborated with the FCC Consumer Advisory Committee (CAC), which helped shape the CAC’s recommendations in October 2014
- We collaborate with the CTIA Cyber Security Work Group on practical steps to take going forward
- We brainstormed with the Executive Director for the National Cyber Security Alliance (NCSA)
- We met with one of the members (from Lookout) of the TAC Mobile Device Theft Prevention to capture the perspective of a mobile security application provider



Mobile Device Consumer Interface for Privacy & Security

Takeaways from our collaboration with CTIA and NCSA (National Cyber



Security Alliance):



- The brick and mortar store Point of Sale experience is not ideal for educating consumers
- A fixed set of security questions across all device types does not seem to be practical
 - A universal app will be obsolete almost immediately due to rapid technology advancements
 - A, cross-platform configuration app will require the opening up of new, vulnerable APIs
- It is recommended the FCC encourage the creation of a cyber security education app, *and not a security parameters configuration app*, for the reasons outlined above
- NCSA recommends the FCC should actively participate in future NCSA events, such as Data Privacy Day on January 28, 2015, an initiative centered on "Respecting Privacy, Safeguarding Data and Enabling Trust."
- The FCC should consider making the current smartphone security checker available in an unbranded format, allowing it to be more directly leveraged by other websites such as the NSCA website <http://www.stopthinkconnect.org/>
- *The key takeaway: It is not so important from where the consumer education is sourced but rather that it does happen*



Mobile Device Consumer Interface for Privacy & Security Recommendations

1. Improve the FCC Smartphone Security Checker update process
 - The recommendation is to have either an individual person for each of the 4 OS's, or an automated app, “automatically” update the checker as smartphone features evolve
 - CTIA CSWG is willing to help the FCC on this task, including reaching out to OS makers and OEMs
2. Encourage OS makers, OEMs, and mobile app vendors to make existing educational material more accessible on their devices
 - Examples include CTIA, tutorials from carriers, the FCC Smartphone security checker, and NCSA
 - These resources should be directly available to their consumers on their smartphones, either through a separate app, or as a default home page on the smartphone web browser
3. Seek greater collaboration with industry associations and public private partnerships
 - Collaborate with CTIA on future consumer research study areas of focus, and on the streamlining of the FCC Smartphone Security Checker website update
 - Look for opportunities to actively participate in the NCSA's “Stop, Think, Connect” campaign
4. Act as a catalyst for harmonizing consumer education messaging
 - Strive for greater message sharing across resources such as the FCC, DHS, CTIA, carrier education websites, OEM/OS maker websites, and NCSA resources
 - Consider an “unbranded” version of the smartphone security checker, which will help reach consumers that may be reluctant to utilize government initiative

Lead: Ramani Pandurangan

2. SECURITY PRACTICES FOR THE CORE NETWORK EQUIPMENT



Security Practices for the Core Network Equipment

Goal, Contributors, Methodology, Existing Practices and Under Development

- Develop recommendations for security practices to be considered for core network equipment (network backbone, operations & mgmt, cloud / data centers, BGP, DNS, etc.) and for a tiered compliance checklist
- Contributors - Vasireddy Rao, Alcatel-Lucent; Martin Dolly, AT&T; Brian Scarpelli, TIA; Renato Delatorre, Verizon; G. (Ramani) Pandurangan, XO Communications
- Methodology - Research on existing practices and standards and, consultations with guests from certification labs and organizations involved in the CC framework
- Existing practices and under development in SDOs, Governmental organizations, industry organizations and communities
 - ISO / IEC has specified requirements for information security (27001) and basis for Common Criteria (CC) with international agreement (15408)
 - 3GPP / GSMA developing security assurance methodology and administrative framework for Mobile Network Equipment
 - US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing
 - NIST and CSRIC have published several practices (e.g. BGP, DNS)
 - NIAP, an NIST – NSA partnership, working with Technical Communities CC Protection Profiles specifying the security requirements for different technologies and administers National Voluntary Laboratory Accreditation Program (NVLAP)
 - Open Communities contribute and participate (e.g. CC User Forum, Open Web Application Security Project, The Open Group, Cyber Security Council)
 - Besides the NVLAP-accredited US labs for CC, independent labs provide security certification (e.g. ICSA Labs) of core network equipment



Security Practices for the Core Network Equipment

Conclusions

- Although no single framework seems to be available today with tiered security assurance levels for core network equipment for non-Government use, several security best practices are available and are being developed. Such a framework could benefit the industry in general
- Instead of developing yet another new framework, the good work and practices which exist and are being developed today in 3GPP / GSMA, ISO 27001 and ISO/IEC 15408 (Common Criteria) should be leveraged to come up with a responsive, agile, consistent, cost-effective certifications and accreditation framework, with industry collaboration and partnership
- Vendors should be able to carry out self-assessment or use an accredited lab. Vendors should disclose this information so that equipment procurers can use this information to discern and make purchase decisions
- User awareness of security standards and certifications should be promoted and users encouraged to ask core equipment vendors about such certification; this would also provide marketplace incentive for the vendors to get their equipment certified

Security Practices for the Core Network Equipment Recommendations

For non-Government use, recommended that FCC

- Facilitate bringing standards organizations such as 3GPP, ISO/IEC, ANSI and, NIAP together
 - to develop a tiered security compliance requirement list for core network equipment
 - to develop requirements for accreditation and auditing of the certification labs whether independent or vendor's own
 - to create a repository of security certification status of core network equipment, easily accessible to the industry players
 - promote awareness of the equipment procurers of the repository
 - TAC should be able to assist in such a harmonizing initiative
- In 2015, continue the work to determine impact on the framework as the industry moves from Proof Of Concept (POC) to production NFV / SDN architectures



Lead: Adam Drobot

3. FUTURE MITIGATION TECHNOLOGIES FOR INSIDER THREATS



Future Mitigation Technologies for Insider Threats

Goal and Objectives

- Develop a high level survey of promising security technologies, tools, and processes for core network operations that address the “insider threat”.
- Following the NIST Cyber-Security framework to identify technologies or tools that are most likely to make an impact on security for each of the five functional areas of the framework.
- Make recommendations for how the FCC can best impact/advance technology security outcomes in the short and long term.

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			



Future Mitigation Technologies for Insider Threats

Technology, Tools and Process Impact Areas

Functions	Access Control	Big Data	Software Analysis	Trusted Computing	Probabilistic Risk Assessment (Process)
	<ul style="list-style-type: none"> - Biometrics - Challenge Q&A - Dynamic Security 	<ul style="list-style-type: none"> -Multi-source -Unstructured -Characterization -Pattern Detection -Event Identification 	<ul style="list-style-type: none"> -Software -Systems -Applications -Script -Malware Detection -Path Identification 	<ul style="list-style-type: none"> -Defect elimination -Secure Hardware -Secure IO -Isolation -Sealed Storage -Attestation 	<ul style="list-style-type: none"> -What May Happen -Impacts -Probability -Target Prioritization
Identify	Now	Now Future	Now Future	Future	Now
Protect	Now	Now Future	Now Future	Future	Now Future
Detect	Now	Now Future	Now Future	Future	Now Future
Respond	Now	Future	Future	Future	Future
Recover	Now	Future	Future	Future	Future

Now: Trending toward broad use and likely to be common with 3 years

Future: Earlier stages of R&D and more likely to be common in 3-7 years



Future Mitigation Technologies for Insider Threats

Recommendations

1. Active encouragement demonstration and experimentation with advanced cyber security technologies
 - Partnership with Government Labs, Academic Institutions, Industrial Laboratories, and Other institutions focused on Security to conduct trials and demonstrations.
 - Promotional Awareness / Conferences
 - Collaborate with other Agencies/Industry to publish periodic reports that specifically prioritize threats and map them to emerging technologies
2. Encourage technology information and practices sharing venues
 - We have over 4500 communication service providers in the country. Most lack the resources of the large SPs. It is hard for a small provider to have the technical capability to deal with the issues faced by "security" (to knowledgeably deal with policy, processes, understand the security tools, and to adopt new technologies).
 - Promote regulator-safe and business practice-safe environments (e.g., clean rooms) for information sharing
 - Practices and technologies
 - Review/prioritization/assessment of emerging threats vs. technologies



Cybersecurity Working Group

Potential 2015 work

- Mobile Device Consumer Interface for Privacy and Security
 - The TAC could engage directly with the CTIA CSWG to further the evolution of the FCC smartphone security checker
 - The CAC, once re-chartered in 2015, could build upon their 2014 work to continue evolving the consumer education options for smartphone security
- Security Practices for Core Network Equipment
 - The TAC could play the role of convener on behalf of the FCC and orchestrate the development of a structure that weaves this year's identified best practices together
 - The TAC could continue the work to determine impact on the framework as the industry moves from Proof Of Concept (POC) to production NFV / SDN architectures
- Future Mitigation Technologies for Insider Threats
 - Develop and promote specific insider threat mitigation technology analysis:
 - » Convene industry partners (academia, research labs, etc.)
 - » Prototype the 'threat vs. emerging technology mapping' report
 - Assist the FCC in convening information sharing / evaluation (clean room) environment

THANK YOU!



Technological Advisory Council

Supporting the Transition to IP

Working Group

4 December 2014



Working Group Members

- Tom McGarry (Neustar)
- Theresa Hennesy (Comcast)
- Kevin Kahn (Intel)
- Fred Kemmerer & John Barnhill (Genband)
- Steve Lanning (Viasat)
- Marvin Sirbu (SGE)
- Kitty O'Hara & Tim Dwight (VZ)
- Kevin Sparks (ALU)
- Russ Gyurek (Cisco)
- Dale Hatfield (UCol)
- Harold Teets & Mike McNamara (TW Telecom)
- Lynn Merrill (NTCA & Monte R. Lee)
- Peter Bloom (General Atlantic)
- Dick Green (Liberty)
- Jack Nasielski (Qualcomm)
- Nomi Bergman, John Dickinson (Bright House)

Special thanks to the FCC members: Walter Johnston and William Layton for their contributions.





Today's Discussion

- Refresher: Review our original mission
- Executive Summary of our broad conclusions
- Share our approach: Stake holder interviews; Reference Architecture; Review Corner Cases; Identify insights and opportunities
- Update on where we are:
 - Review Reference Architecture and our insights.
 - Review Access Architecture Evolution Paths
 - Findings from transition stakeholder interviews and observations
- Actionable suggestions



Review our Original Mission

- Examine opportunities for new communication technologies to better serve the needs of people with disabilities
- Identify potential opportunities for improvements in emergency alerting and information support during disasters enabled by an IP infrastructure and associated technology
- Identify opportunities for experiments or R&D that would support the understanding of the impact of tech transitions on the enduring values
- Analyze potential for new fiber technologies and wireless systems to better serve low population areas ensuring that rural communities are connected to the evolving broadband environment
- Identify opportunities and objectives for trials designed to support advanced communication capabilities to rural areas
- Support activities focused on improving acquisition of information on deployment of broadband technologies



Broad Conclusions from our combined Work Group

- IP Networks are enormously capable
- Access Networks studied are more similar, than different, in terms of capabilities, and evolution paths.
- All platforms can evolve to higher bitrates/customer to support Internet access and specialized IP based services (e.g., VoIP, Video).
- Higher speeds are fueled by driving fiber deeper into neighborhoods, spatial reuse and/or increasing spectrum (cable or wireless).
 - These carry significant construction, CPE replacement or spectrum costs.
- What does this mean for replacing legacy PSTN services with modern services, supported by IP networks?
 - Technical alternatives appear to exist for every use case evaluated
 - There are consistent cost hurdles
 - Cost is made up of many components
 - Most significant are construction and CPE replacement costs
 - There are realistic and achievable solutions worth pursuing further in many of these areas.
 - Public safety as a specialized service flow
 - Interoperable real-time text in IP



IP Transition Reference Architecture Effort

- Objective was to create a reference architecture to frame the evolution of broadband access and backbone network technology solutions.
- Reviewed the technologies that provide broadband IP access:
 - The Access network
 - The In-home network
 - The Physical and Logical characteristics
 - How the transport network interconnects with the service layer and other service providers.
- Reviewed how access technologies can evolve to support higher bitrates per customer.

IP Transition Reference Architecture Effort

- A high level architecture that depicts a Service Provider that can provide various services to a user (i.e., consumer or enterprise)
 - The services include broadband Internet access and often include communications and/or video service
 - The architecture describes how these services
 - a) Are supported by the underlying transport networks
 - b) Interconnect with the service layer infrastructure of other service providers
- Each plane (service and transport) can be functionally divided as below

Transport Plane

Functional separation = network topology

Access	host attachment
Regional	Transport within a region, aggregation, mobility mgmt
Core	Transport between regions, service plane attachment

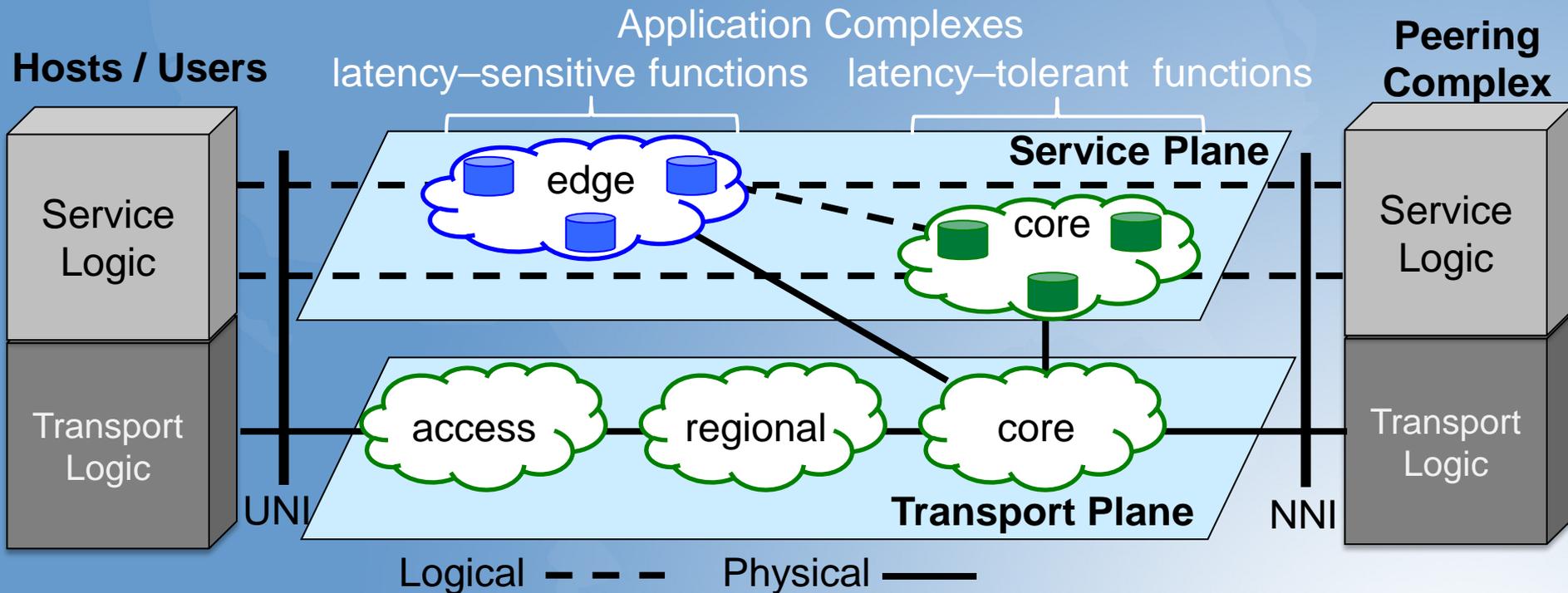
Service Plane

Functional separation reflects proximity to the served user

Edge	Near the served user
Core	Not (necessarily) near user

Additional planes (e.g., management) are similar but not illustrated

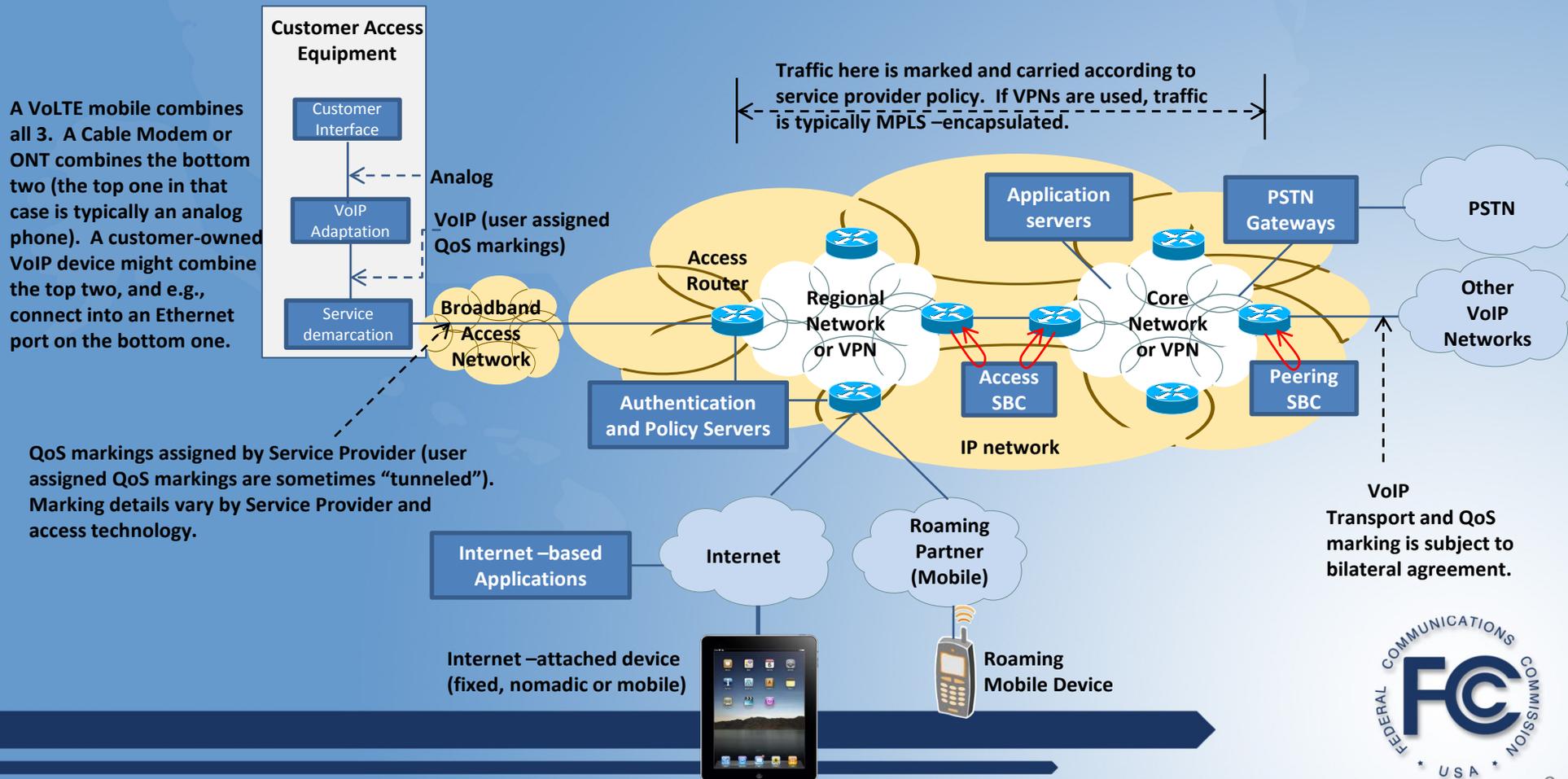
Layered Network Design



- Service Plane elements (hosts, servers, gateways, etc.) attach physically to the transport plane and logically to the service plane
- Service Plane functions may be near the served user (e.g., if latency sensitive) or centralized

Simplified Representative Diagram – actual designs will vary

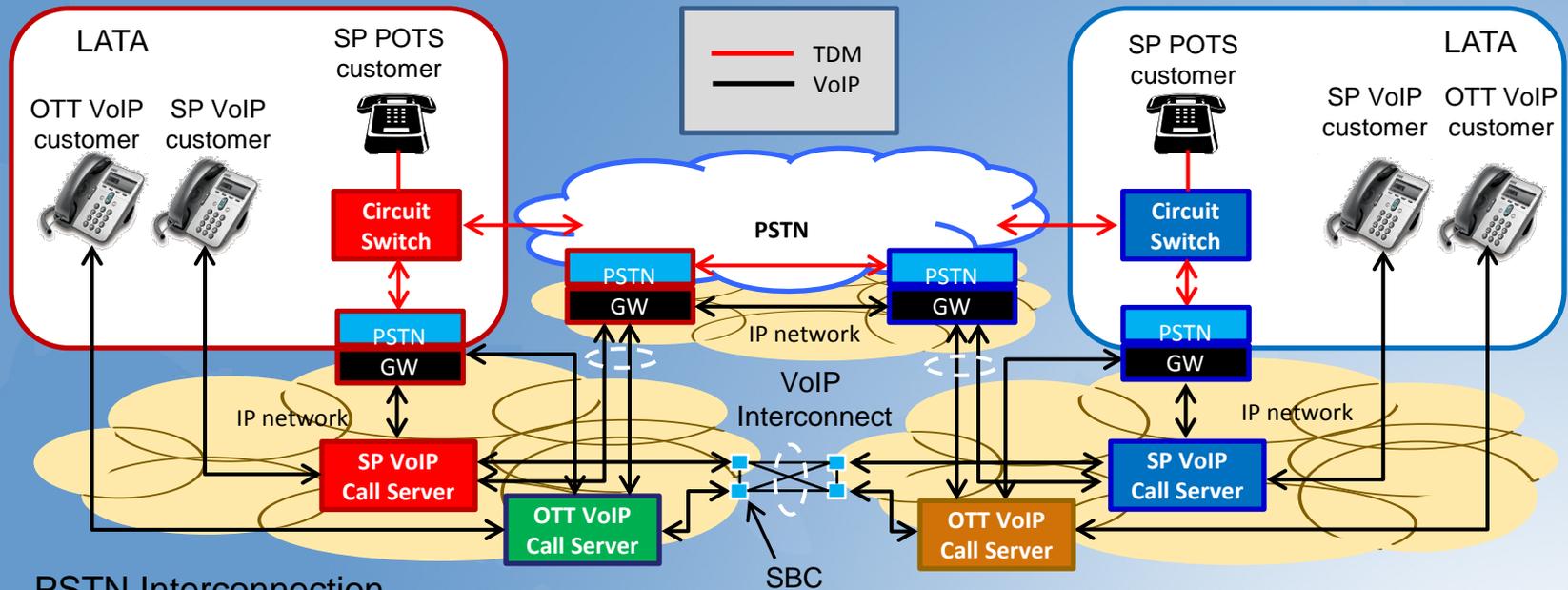
Perspective on Service Provider VoIP



Perspective on Service Provider VoIP – (Description for prior slide)

- Three elements of customer access equipment
 - Customer interface-(analog)->VoIP adaptation-(VoIP)->Service demarcation
 - A VoLTE mobile combines all three
 - A cable Modem or ONT combines the VoIP adaptation and service demarcation, the customer interface in that case is typically an analog phone
 - A customer-owned VoIP device might combine the customer interface and VoIP adaptation, and connect into an Ethernet port on the service demarcation
- QoS markings assigned by the Service Provider at the service demarcation
 - Marking details vary by Service Provider and access technology
 - User assigned QoS markings are sometimes “tunneled”
- Traffic in the Regional and Core Networks/VPNs is marked and carried according to service provider policy
 - If VPNs are used, traffic is MPLS –encapsulated.
- Transport and QoS marking between networks is subject to bilateral agreement

VoIP vs. PSTN Interconnection



- PSTN Interconnection
 - Calling network must deliver call to geographic area of called party. Many points of interconnection.
 - “default route” to terminate calls to any NANP number (including VoIP devices)
- VoIP Interconnection
 - Interconnection is subject to bilateral agreement. Points of interconnection are usually centralized.
 - Calls can be routed to whatever numbers the terminating network advertises as IP-reachable

Scope of Access Technology Review

■ Access Network

- Digital Subscriber Line (DSL) and hybrid Fiber/xDSL technologies (xDSL)
- Fiber to the Premises (FTTP/FTTH)
- Hybrid Fiber Coax (HFC)
- LTE
- Satellite
- Other wireless
 - WiFi, WiMAX
- Evolution paths for access technologies

■ In-Home Network

- WiFi
- Multimedia over Cable Alliance (MoCA 2.0)
- Power Line Networking: HomePlug AV, IEEE Std 1901-2010
- Structured cabling (e.g. Ethernet)
- Phone wiring: HomePNA ITU G.hn standard

Physical vs Logical Architecture

■ Physical

- Cabling, nodes, layout, physical-layer features

■ Logical (layer 2)

- Each access architecture provides a means of separating traffic into distinct “flows” that can be given separate QoS treatment
- We describe how each architecture accomplishes this

■ Boundary of layer 2 network: location of first layer 3 router

- Divides access network from metro network

Insights from Access Network Review

- IP broadband is a platform that supports both Internet access and specialized IP-based services (e.g. VoIP, video delivery)
 - These multiple logical networks differ with respect to:
 - QoS
 - Interconnection
 - Services available
 - Logical networks may be separated by:
 - Assignment to separate physical channels (e.g. separate wavelengths); or
 - A guaranteed share of link resources; or
 - Different priority levels
- Any of the access technologies can easily handle VoIP bitrates
 - Conversational video requires more
 - OTT (nomadic) VoIP may behave differently than dedicated (fixed) VoIP
 - Do consumers need to be educated about these differences in order to understand how behaviors may differ?
 - *E.g.* location determination for E911 may be different for OTT and dedicated VoIP

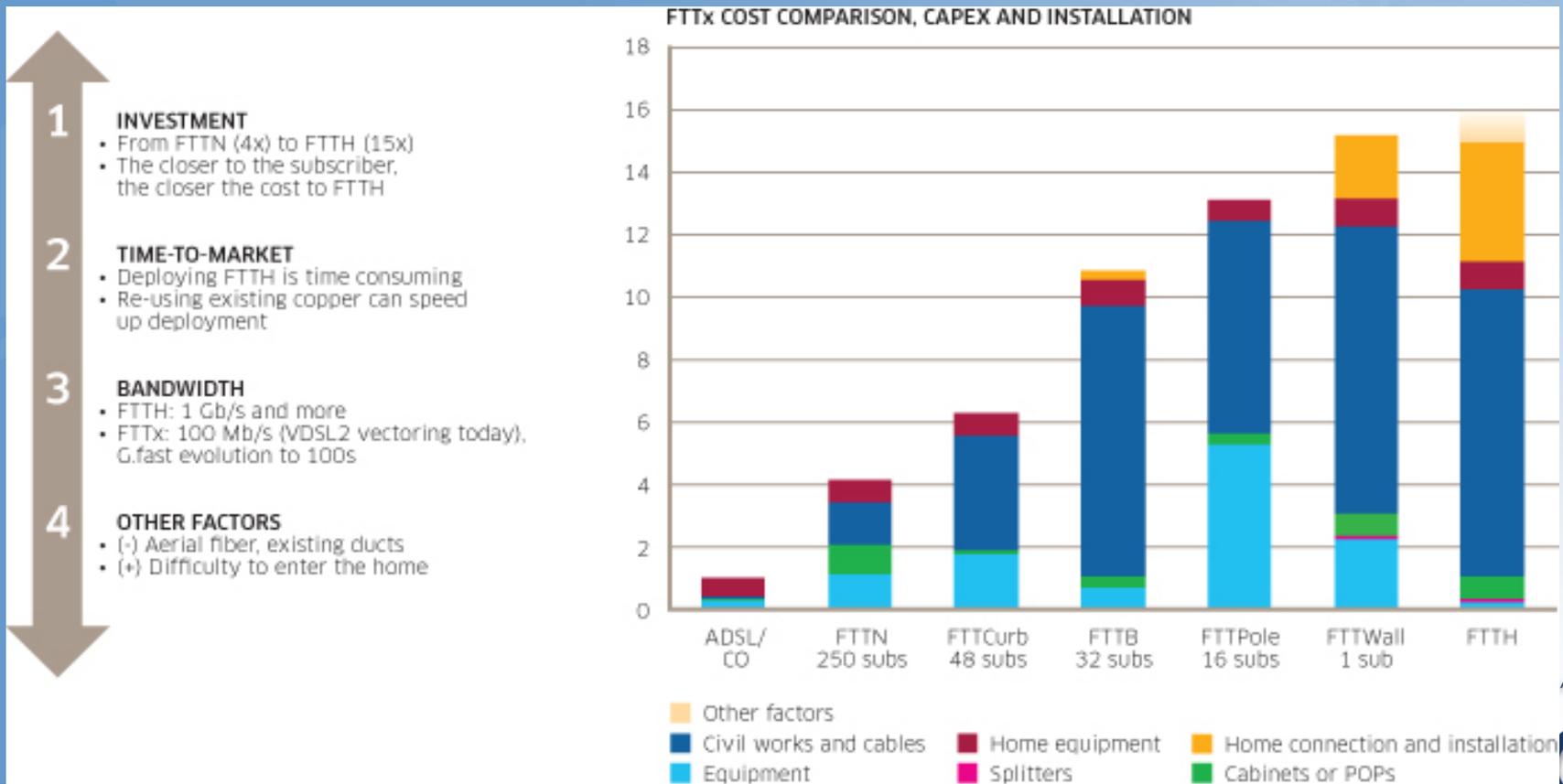


How access technologies can evolve to higher bitrates per customer

- There is no fixed technological limit on the speeds/household available using HFC, xDSL, FTTH or LTE, or satellite
- Issue is the cost of upgrading to realize higher speeds
- Higher speeds often means pushing fiber deeper into neighborhoods.
 - This can have significant construction costs
- In the case of satellite, this means more spot beams (spatial reuse)
- May also require changing access node electronics and CPE;
 - changing CPE is typically more costly, as more numerous.
- Reducing bit rate per video stream through better compression can increase capacity available for other broadband applications.



How xDSL Costs Change as Fiber is Extended



Working Group Findings on IP Transition

- **2014 Transition Stake Holder Interviews and Observations**
- **Deep Dive Examples**
 - IP Transition Observations: Rural Service Providers
 - IP Transition Considerations for Telephony Services for the Hearing Impaired

2014 Transition Stake Holder Interviews and Observations

Interviewees

- **Service Providers**
 - Small and mid-size rural providers
 - Satellite broadband provider
 - Middle-mile providers
- **Manufacturers**
 - Broadband equip. manufacturers
 - Fiber cable manufacturers
- **Issue Advocates - Corner Cases**
 - Assistive device performance expert
 - State provider of assistive devices
 - Technology and policy issue experts for those with disabilities
 - Public safety/ elevator phone expert

Interview Findings

- **Rural Service Providers Report**
 - High Construction Costs – density, terrain, regulation
 - Working around multiple jurisdictions/ outdated regulations
- **WG encouraged by broadband progress**
- **Other Cases**
 - Technical alternatives exist for every item evaluated (so far)
 - Awareness, budget, manpower, mandate
 - Premise equipment/ Deployment specific issues
- **Ref. architecture framework enables services across multiple technologies**

Ensure that new technology deployments aren't impeded by outdated regulation

IP Transition Observations: Rural Service Providers

- **Often Serves as a Test Bed for Manufacturers of IP Technologies**
 - Uses every asset to develop new and improve service to local customers (i.e., Employee, civic, etc.)
 - Willingness to test new technologies
 - Understands local community needs allowing lower ROI to trigger invest
- **A variety of technical solutions fit within the Reference architecture**
 - **Access:** Use FTTH or COAX to serve inside community, VDSL/ADSL copper in rural areas, and Wireless in areas where new cable placement is difficult to obtain. Use satellite in extremely rural areas.
 - **Backbone:** Middle-mile solutions represent a greater bottle neck to providing broadband access services than last mile solutions. Joins with local and regional providers to construct backbone networks to meet needs of local ISPs, Schools, Hospitals, Public Safety and Wireless Operators
 - Installed larger fiber networks or joined a consortium to form statewide networks
 - Built redundant connection points over several years, for reliability
 - Due to long distances to internet gateways, companies worked to bring traffic closer to end point of their own network to reduce costs and price.
 - **Service Plane:** Rural Operators looking at options to lease soft switching services and servers usage from hosted parties or hosting services to others



IP Transition Considerations for Telephony Services for Hearing Impaired Persons

- Surveyed/ Evaluated
 - Services for those with Disabilities
 - Public Safety
 - Alarm Industry
 - Emergency Phones
 - Utility Industries
 - Proposed Service Experiments
 - Government Agencies



- Potential Issues include:
 - Budget or manpower availability
 - TDM Devices/ Premise Equipment Obsolete
 - Features Retired due to low usage or obsolescence
 - Deployment Specific Issues
- Technical alternatives exist for every use case evaluated
- IP networks enable richer solutions
- Focus should be on accelerating the market deployment

Next Steps for TAC 2015 Work

- Given that the IP Transition happens, what are new, innovative opportunities for broadband services to better serve:
 - Public Safety
 - The needs of people with disabilities

Technological Advisory Council

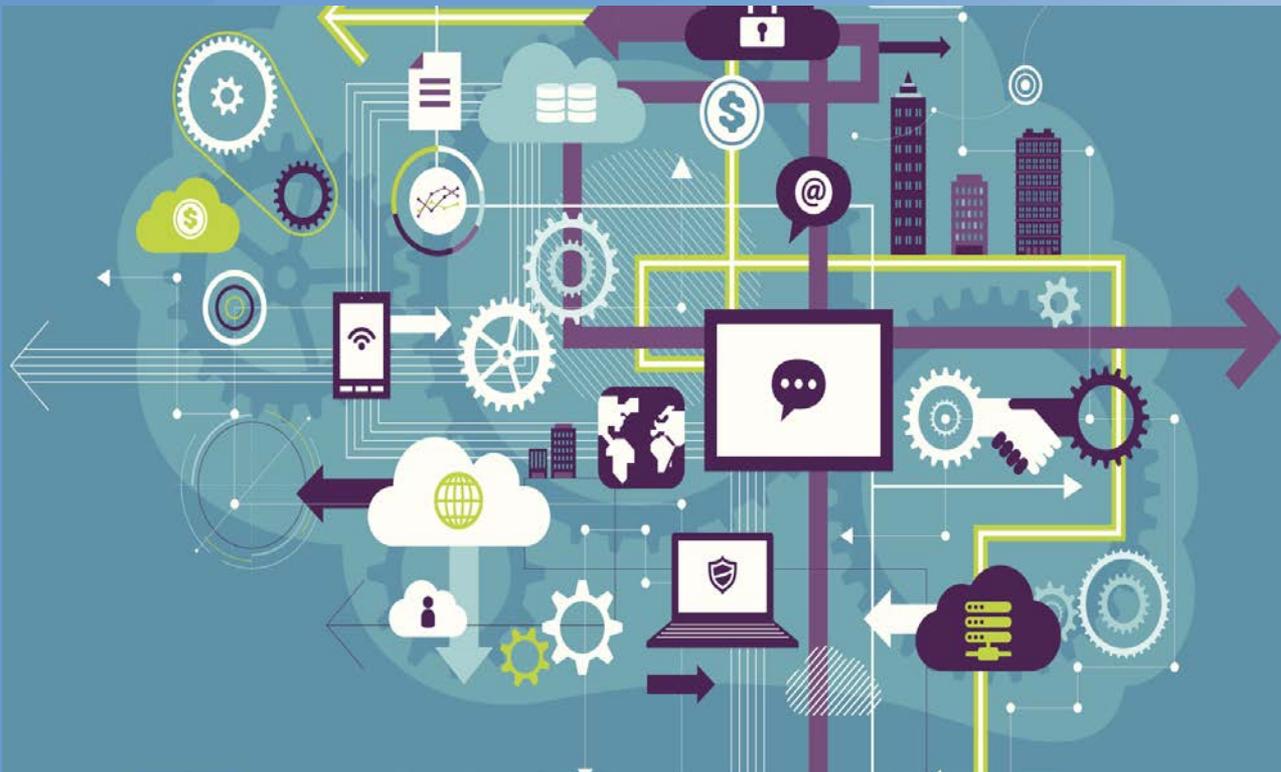
**477 Testing
Working Group
4 December 2014**



Form 477 Status Update

- Filing interface closed on September 26 and reopened November 20 so contractor could address technical issues and implement improvements.
- New filing deadline for data as of June 30, 2014 is December 11, 2014.
- WG will reconvene in 2015 to discuss next steps and to pursue objectives defined by FCC staff

FCC TAC: IoT- Dec 4, 2014



**How will IoT
impact
communications
networks
in 5, 10 years**

IoT WG

Dec 4, 2014

- Russ Gyurek- (Co-Chair), Cisco
- David Tennenhouse- (Co-Chair), VMware
- Walter Johnston (FCC)
- Shahid Ahmed, Accenture
- John Barnhill, Genband
- Mark Bayliss, Visuallink
- Kevin Cage, NAB
- Greg Chang, Yume
- Marty Cooper, Dyna
- Kevin Kahn, Intel
- Mark Gorenberg, Zetta Ventures
- Stephen Hayes, Ericsson
- Anoop Gupta, Microsoft
- Joe Salvo, GE
- Milo Medin, Google
- Bill Morelli, IHS (Ad hoc)
- Adam Drobot, OpenTechWorks
- Amit Jain, Verizon
- DeWayne Sennett, ATT
- Brian Markwalter, CEA
- Lynn Merrill, Monte R. Lee
- Jeff Foerster, Intel
- Jack Nasielski, Qualcomm
- Ramani Pandurangan, XO Comm
- Deven Parekh, Insight Partners
- Marvin Sirbu, CMU
- Kevin Sparks, ALU
- Glen Tindal, Independent
- John Brzozowski, Comcast
- David Gurney, Motorola
- Hans Juergen Schmidtke, Juniper
- Glen Allmendinger, Harbor (Ad hoc)





IoT is about
“Technology and
Stuff”

IoT is the orchestration of people, process, data and things; going much further than connecting items to the Internet



Charter

- Identify key areas in the evolving Internet that should drive the work of the Commission or areas where the Commission should seek key information
- What new demands will the Internet of Things (including M2M) place on the network?
- What technology policy challenges exist in the evolution towards an Internet of Things?
- Explore how the FCC can foster IoT innovation and leverage federally funded R&D in this area



Executive Summary

- **IoT is growing rapidly and will drive network use and scale**
 - Opportunity to add \$T's to GDP, create societal benefits, etc.
- **Multiple waves of new connected devices will enter the market**
 - Most devices will be “unattended” and will push content to the cloud
- **Consumer market is the most likely sector to focus FCC attention with respect to network, spectrum, security, sudden emergence of unforeseen traffic, etc.**
- **Network & Spectrum:**
 - Majority of “things” connect via unlicensed spectrum, or are wired
 - IoT will create new traffic demand across PAN, LAN, and WAN
 - Good News: Forecast pace of traffic growth appears manageable
- **Security:**
 - IoT broadens the attack surface & creates new attack vectors
 - The FCC should clarify its role with respect to IoT Cybersecurity



FCC Actionable Recommendations

Sizing & Connectivity

- FCC to programmatically monitor the consumer IoT network traffic impact on WLAN and WWAN with focus on new high BW consuming applications

Spectrum

- To stimulate IoT growth, the FCC should focus on the availability of unlicensed spectrum suitable to a range of PAN/WLAN services
 - Do not make spectrum allocations unique to IoT
 - Ensure there is sufficient short-range spectrum to meet growth in PAN/WLAN requirements and sufficient network capacity upstream from IoT devices and proxies

Security

- FCC to define its role within the context of an overall cybersecurity framework
- Dedicate resources and participate in IoT security activities with other government stakeholders (per NSTAC recommendation)
- Conduct a consumer awareness campaign related to IoT security and privacy (in collaboration with other agencies)
- FCC to conduct internal periodic scenario exercises to determine appropriate FCC response related to widespread consumer events related to IoT



IoT WG Statements

IoT Privacy Statement

The ubiquity of information in the Internet of Things is a challenge for our society.

Recommendations

1. Working with industry to develop current approaches to transport, use and different vertical sectors
2. Work with appropriate norms applicable to
3. Understand public breaches in relation

The TAC does not form a party to the di

IoT EoL Statement

Technology, whether for a limited transmission capacity, or a limited expected viable lifetime and products will be no different from those issues associated with IoT devices. challenging given the interconnection of low cost and long expected IoT devices.

- End Of Life / End of Service should be publicly available sufficient for parties to manage the impact of downloading any relevant data patches, etc..)
- End Of Life / End of Service should be considered - and where possible - consider exposures that the End Of Life (eg., increased security is)

Safe Harbor Statement

- Many classes of IoT devices have a limited range and a long life (8 years)
- To avoid spectrum congestion over a long period, it is necessary to have devices, and to utilize unlicensed spectrum in a practical.
- This recommendation for a safe harbor for IoT evolution is

Unlicensed Etiquette Statement

In unlicensed bands, FCC rules provide that unlicensed users must accept interference (and may not cause harmful interference).

Although this regimen has worked well; now may be the right time for the FCC to investigate potential next steps in the evolution of the "digital etiquette".

Recommendations

- SDO's should continue to coordinate with each other to facilitate co-existence.
- Non-standard wireless solutions should strive to protect the commons in ways that allow the operation of other technologies.
- As new frequency bands are allocated there may be significant value in re-examining co-existence techniques for unlicensed spectrum. the FCC should be open to future policy supporting ultra-efficient spectral technologies which may require that some newly allocated bands be restricted to use of specific technologies and or control protocols

The IPv6 network protocol offers several advantages over IPv4 ... and should be used where feasible.

IoE WG Topics Studied

- Taxonomy
- Standards
- IoT Sizing & Network Traffic*
- Spectrum Implications
- Security* & Privacy†

* Topics new/revised since September meeting

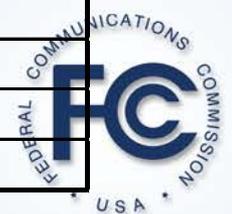
† See Privacy Statement



IoT Taxonomy by Vertical

FCC IoT Taxonomy				
USAGE -->	In-home	Government	Enterprise	Public
Spectrum				
Security				
Privacy				
Interference				
Reg. Agency				
Bandwidth				
Priority				
Latency				
Power mngt				
Public Safety				
Standards				
Numbering				
Class				
Registration				

See Excel spreadsheet
 Differentiated markets emerging:
 Consumer; Government/Critical Infra;
 Enterprise/Industrial; Public Spaces



IoT Standards

IoT Areas of Focus and efforts															
Standards Body/ Organization	Standard effort?	Efforts status	Security	Privacy	Network/ Protocol	Traffic/ Transport	Archi- tecture: Endpoints	Archi- tecture:	Smart	M		Success	Notes / Comments		
Gov. Agency	No		NIST Framework for Improving Critical										FCC, DOT, NIH,		
IEEE	Yes	Mature	Wi-syn, 802.15.9	Varies by Society	2011, 802.16, Ethernet, 1901.2	No	SmartGrid, Energy, Industrial, Agriculture, Mining	above L2, New project, 2314, will be defining IOT Arch.	No	No	Yes, reference materials only	No	No	Varies by technology, Generally good to excellent	They have an IOT Group in the Corporate Advisory Group. They are adding entity based IOT projects as well as IOT promotion.
IETF	Yes		Wi-syn, ACE, DICE		6Tish, IPv6, 6LoWPA N, RPL, MPL, CoAP	UDP, TCP					COMAN				

See Excel spreadsheet
Many organizations taking a
role



IoT Sizing/Network Impact



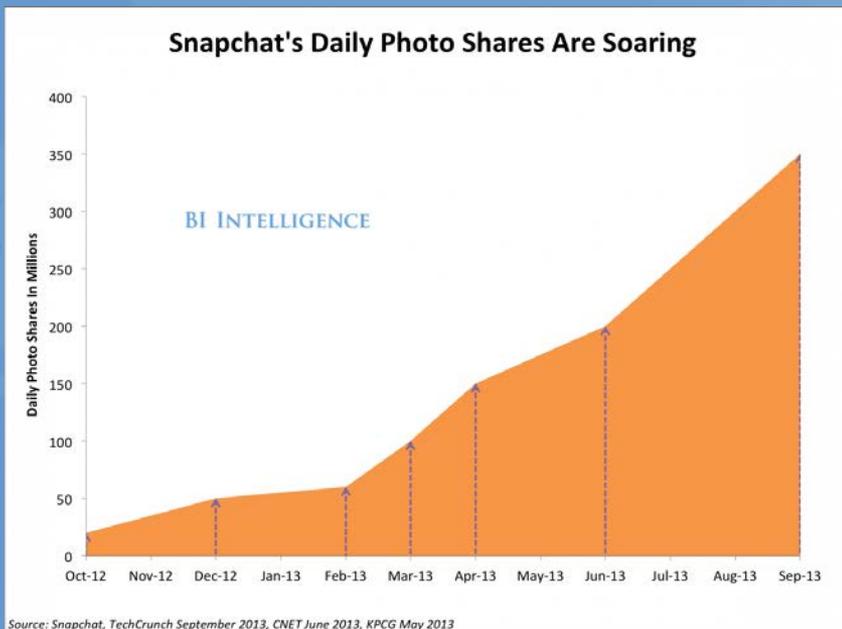
IoT Sizing: Millions of Apps, Billions of Connected Devices

- All Projections indicate very substantial growth
 - Project 50B Devices by 2020; Project Over 1 Trillion in 20 years (WW)
 - GDP impact – estimated range of 20T USD to 73T USD (WW)
 - Growth acceleration driven by: microcontroller price/performance, sensor advancements, ubiquitous access, cloud infrastructure, and apps
- Differentiated markets emerging:
 - Consumer and Enterprise/Industrial are experiencing rapid growth
- Factors not addressed:
 - New apps/ radical changes in data sources (e.g. video as a sensor)
 - Migration of data between private , hybrid and public clouds

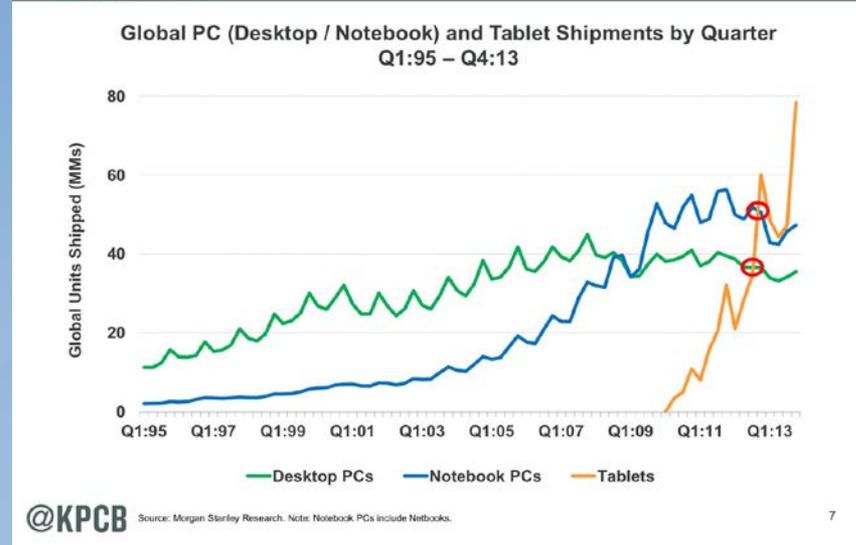
Device Activations: Today = 80 per Second. 2020 = 250 per second



Examples of Past Market Disrupters



Tablet Units = Growing Faster Than PCs Ever Did...
+52%, 2013



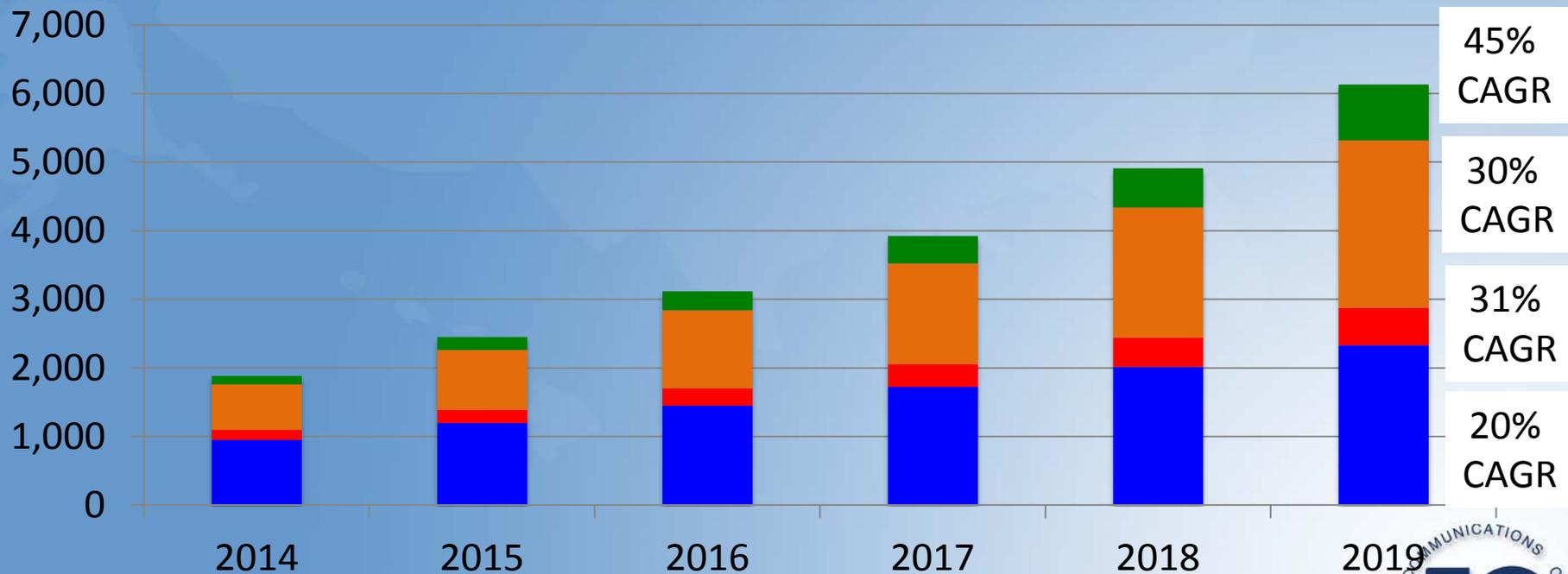
- Explosive growth of a new *application* or *technology* could challenge the network, similar to the smartphone -- Is there a canary in the coal mine?



USA* Device Growth (M)

Chart Data Courtesy of Harbor Research

■ Wireline ■ WWAN ■ WLAN ■ WPAN



* Based on 85% of North American Growth as projected by Harbor Research Market Sizing Information



Sizing: TAC Focus Areas

Harbor Research

Table FCC - Extended Forecasts - IoT Internet Connectable Devices

	2014	2020	CAGR 11-25	USA Multiplier	Connected Multiplier (2020)	Traffic Vol. Multiplier	Network Impact	Comments
Automotive								
Under-the-Hood								
WWAN	21,660	184,349	34.9%	50.0%	30.00%			
Infotainment								
WLAN	5,128	55,530	66.6%					WiFi In the car
WWAN	14,440	122,900	34.9%	50.0%	35.00%			LTE backhaul - MONITOR
Communications								
Mobile Handset								
WLAN	1,721,516	4,553,459	22.4%	10.0%	90.00%			Carrier Grade WLAN?
Consumer								
Home Appliance	194,720	504,389	16.7%					
WLAN	389	1,992	32.7%					In-home, controlled env.
Home Automation								
WLAN	366,725	689,327	30.8%					In-home, controlled env.
WWAN	76,887	241,485	28.2%	70.0%	35.00%			Digital Life offer w/cellular
Sports & Fitness								
WWAN	1,579	7,494	66.3%		15.00%			Mostly PAN; to s-phone Potential caution MONITOR

- Data volume and network impact is dependent on apps
- Several segments worthy of active monitoring

Legend

Pink = High Growth Rate

Yellow = Monitor

Green = Impact

Sizing & Impact: Enterprise/Industrial

- Growth in devices & traffic
 - Projections of extremely large device counts by 2020
 - BUT...CAGR by industry segment is moderate → steady, manageable growth
 - AND...bulk of traffic will likely be short bursts → limited traffic / device
- Most enterprise/industrial “things” will be on enterprise premises
 - Bulk of devices will be connected via wired LAN and/or locally coordinated unlicensed spectrum
 - PAN device growth will also be significant
 - WLAN impact will likely be constrained to WiFi Spectrum except in unique circumstances
 - Many IoT-based applications will reside in the cloud
 - enterprises, factories, warehouses, etc. typically have fiber connectivity to ISPs
 - IoT driven growth in upstream traffic to/from cloud, etc. will also be manageable
- Some Industrial “things” (e.g., automotive) will be mobile and/or rely on WWAN

Conclusion: Enterprise/Industrial traffic arising from IoT is largely manageable



Sizing & Impact: Consumer

- Consumer sector may be volatile wrt # of devices and traffic/device
 - Business models are also evolving
 - Potential for unexpected new application(s) with a Netflix like traffic impact.... in reverse
 - e.g., “Immediate” (rich) video uploads; Mass event streaming applications
- Most consumer “things” will be within home and/or mobile (e.g., on body)
 - Bulk of devices will be connected via PAN/WLAN
- Most consumer IoT-based applications will reside in the cloud
 - Traffic to/from cloud may impose new demands on local ISPs and/or WWAN capacity
 - Future IoT traffic may be more upstream-intensive than current traffic.

Conclusion: The FCC must be alert to rapid shifts in consumer-based IoT



Spectrum



Wireless Spectrum Connectivity Framework

Three dominant classes of wireless IoT links (there are others)

1. **Thing to Thing** (vehicles, sensors/actuators, etc.)

WLAN/PAN range; use spectrum suited to short distances; extensive spatial reuse

2. **Thing to Proxy** (e.g., gateways, hubs, hubs within vehicles, etc.)

WLAN/PAN* range; use spectrum suited to short distances; extensive spatial reuse

- IoT adds significant load to existing services, such as WiFi/WLAN and BT
- Traffic upstream from proxies shares allocations and adds significant load to existing ISP and/or WWAN services used to link WiFi, etc. to core Internet.

3. **Thing to Internet via WWAN** (e.g., direct connection to 4G, WISPs, TVWS, etc.)

last mile range; share spectrum with and/or use other wide area services

- IoT adds load to 4G/TVWS services and poses challenges wrt long-lived things

* Personal Area Network -- typically operates within a range < 10M



Spectrum: Findings

Thing-to-Thing and Thing-to-Proxy spectrum requirements can be met, provided:

- The FCC continues to increase the availability of LAN/PAN range spectrum on a timely basis
- Industry continues to adopt spectrally efficient technologies that support limited range deployments with very high levels of spatial reuse

Demand on upstream links from Proxies to Internet is expected to grow significantly.

This demand can be met, provided:

- The FCC continues to encourage the rapid adoption of innovations in spectral efficiency
- There is a persistent and predictable roll-out of small cell technology (4G, TVWS, etc.)
- Most high throughput IoT traffic (e.g., video streams) is *off-loaded* “close” to the thing/proxy.

Comments & Caveats:

- IoT growth may be accelerated if short-range spectrum availability stays well ahead of demand
- Not saying there is “unlimited spectrum”
- Rural deployments may require additional/special consideration



Spectrum: Conclusions

- No unique allocations of spectrum to IoT are required
 - The FCC should periodically and systematically refresh its analysis and plans to address spectrum demands associated with IoT to ensure there is:
 - Sufficient short-range spectrum to meet growth in PAN/LAN requirements arising from IoT
 - Sufficient capacity upstream from IoT Proxies to accommodate increased demand associated with IoT
- This analysis should take account of significant technical innovations and **the resultant plans should be sufficiently concrete and timely as to guide industry planning related to IoT.**
- Long-lived things should use short range unlicensed spectrum whenever a *safe harbor* from wireless technology evolution is required (see statement)
 - To stimulate IoT growth, the FCC should focus on the availability of unlicensed spectrum suitable to a range of PAN/LAN services (including, but not limited to IoT)



IoT Security



IoT Security Context

- Multiple waves of new devices are going to enter the market
 - Vast number of these devices will push content to the cloud
 - Majority of devices are “unattended”
 - Many of these devices are not focused on or capable of addressing security exposures
- Network security exposure includes: identity theft, snooping, spoofing, botnet attacks, etc
- The IoT market is still nascent; IoT security is the role of multiple organizations, SDO’s and government agencies
 - SDO’s, Consortiums and Service Providers are creating best practices
 - The industry has recently demonstrated it will act quickly to address significant issues
 - The line between IoT security and Cybersecurity is unclear, but being dealt with today

IoT broadens the attack surface & creates new attack vectors



Proposed IoT Security Component Framework

- Things/sensors
 - Leverage Manufacturers and their partners
 - SDOs should drive reference architectures
- Gateway/Proxy
 - Vendors: Ensure data transport security
- Higher aggregation layers in network (e.g., at Enterprise / ISP firewall)
 - Hand off to existing IT and/or ISP cybersecurity;
 - Datacenter/Cloud
 - Predictive IoT security and/or cybersecurity capability
- End-to-End Platforms
 - Embed Security in the platforms that connect things- Market driven
 - Platform players also enforce security within Cloud



Existing Security Work- *IoT Impact

- DHS/NIST: Cybersecurity focused on “organizational implementation”
- CSRIC: (Review NIST framework and determine if applicable)
- DHS/NSTAC: IoT critical infra and emergency preparedness
- TAC: Cyber and Device Working Groups
- CTIA: User Security
- RITA: (DoT Division) focus on V2V and V2I (now OST-R)
- IOT-A: EU Program- Architectural reference model for interoperability
- SDO: IETF, IEEE, OneM2M
- Consortiums: IIC, OIC, Allseen, etc

Bottom line: *There is not an existing “end-to-end” standard for IoT security*



NSTAC Recommendations



- Ask NIST to define IoT
- Have federal agencies (via OMB directive)
 - Assess internal IoT security risk
 - Develop plan for securing IoT within government
- Create inter-departmental task force to coordinate IoT issues
 - Encourage IoT security best practices
 - Update nation security strategy docs to include IoT
 - Add IoT awareness to security awareness programs
 - Encourage research into IoT security
 - Encourage international standards on IoT security
- Government to facilitate industry to develop IoT deployment guidelines
- Review priority communications for IoT considerations
- Review current funding for IoT security R&D

TAC
Alignment



Security: Findings

- **Growth of IOT will greatly increase the *attack surface*.**
 - Solution is industry responsibility; government may be involved in establishing the framework.
 - Critical devices affecting safety of life and property may have additional security requirements set by relevant government agencies and/or standards bodies
 - The TAC supports the recommendations of the NSTAC
- **There is a lack of clarity concerning the FCCs role within the IoT Security landscape**
 - Candidate areas within-scope: Attacks on the network itself (e.g., DDOS attacks emanating from “things”), RF jamming (aka harmful interference) and/or other forms of DOS attacks on “things”
 - Many areas would be outside of scope: e.g. IoT Standards, Security of individual things
- **Challenge:**
 - The FCC’s role related to consumer devices is limited BUT, if/when things stop working, consumers and their elected representatives will expect the FCC to come to their rescue



Recent Example

Your Webcam Could Be Spying on You and You Can Stop It

By **Column** by ADAM LEVIN, [Credit.com](#)

November 23, 2014 6:30 AM

[Good Morning America](#)



- Security
- Privacy
- Awareness/
Education

If the thought of being the unwitting star of your own prime time reality show gives you the willies, consider the recent revelation that more than 73,000 unsecured webcams and surveillance cameras are, as I write this column, viewable on a Russian-based website.



Consumer Awareness is Critical

The Internet of Things has arrived making homes smart, fitness totally interactive and tasks infinitely easier, but the devices we buy to streamline day-to-day life create vulnerabilities that, when exploited, could bring your day to a screeching halt, and the risks are much higher if you don't apply common sense during the setup of these password-protected devices. The rule here couldn't be simpler: Anything that hooks into a network must be locked down.

Don't think it will happen to you? Consider this: There are websites that list the default passwords of all kinds of devices. If you have something wireless that's hooking up to your household router, it likely came with a pre-set password and login. And there's a good chance, whatever the device, there's a forum online where it's been figured out, hacked, cracked and hijacked for all stripe of nefarious purpose.

Source: GMA 11.16.14



Incentives & Removing Barriers for IoT



IoT: Creating Incentives / Removing Barriers

- Spectrum roadmap and utilization visibility
 - Similar to IPv4 address space utilization projections
- Interoperability
 - Gateway interoperability, Carrier Portability, etc.
- Address evolving concerns over Security & Privacy
 - Public awareness campaign
- Encourage IPv6 adoption
- Identify key R&D challenges related to IoT
 - Spectrum efficiency, Security, Privacy, etc.



Summary



FCC Actionable Recommendations

Sizing & Connectivity

- FCC to programmatically monitor the consumer IoT network traffic impact on WLAN and WWAN with focus on new high BW consuming applications

Spectrum

- To stimulate IoT growth, the FCC should focus on the availability of unlicensed spectrum suitable to a range of PAN/WLAN services
 - Do not make spectrum allocations unique to IoT
 - Ensure there is sufficient short-range spectrum to meet growth in PAN/WLAN requirements and sufficient network capacity upstream from IoT devices and proxies

Security

- FCC to define its role within the context of an overall cybersecurity framework
- Dedicate resources and participate in IoT security activities with other government stakeholders (per NSTAC recommendation)
- Conduct a consumer awareness campaign related to IoT security and privacy (in collaboration with other agencies)
- FCC to conduct internal periodic scenario exercises to determine appropriate FCC response related to widespread consumer events related to IoT



FCC TAC 2015 Recommendations

- *As FCC gains clarity on its IoT role, engage the TAC to provide further technical guidance*
- *Focused effort in relation to IoT security for consumer & public sectors*
- *Finalize the detailed traffic volume forecast focused on high growth areas defined in 2014 findings (first quarter 2015)*
- *Consider IoT scenarios, potential viral implementations and related network impact*
- *Explore economic models in relation to barriers to entry*





THANK YOU!



IoT WG Statements

- End of Life
- Safe Harbor
- Etiquette
- Privacy



IoT Privacy Statement

The ubiquity of information exchange in the Internet of Things is creating privacy challenges for our society.

Recommendations to FCC:

1. Working with industry, develop an understanding of current approaches that support the reliable acquisition, transport, use and exchange of information across different vertical service/market groups.
2. Work with appropriate agencies and industry that define norms applicable to Internet of Things.
3. Understand public concerns and the impact of data breaches in relation to IoT on the consumer.

The TAC does not foresee the FCC playing the lead role on IOT privacy, however the FCC must be well-informed and a party to the discussions



IoT EOL Statement

Technology, whether for application, transmission capacity, or device, has an expected viable lifetime and IoT capable products will be no different. However, EoL issues associated with IoT can be especially challenging given the intersection of the very low cost and long expected life nature of many IoT devices.

- *End Of Life / End of Service Announcements be made publicly available sufficiently in advance allowing parties to manage the impact of EoL actions (e.g., download any relevant documentation, install final patches, etc..)*
- *End Of Life / End of Service Announcements should consider - and where possible highlight - critical exposures that the End Of Life action might create (eg., increased security issues)*



Safe Harbor Statement

- Many classes of IoT devices operate over a limited range and are expected to have a long life (8 year or greater life expectancy).
- To avoid spectrum support issues over this long period, it is recommended that such devices, and the networks to support them, utilize unlicensed operations where practical.
- This recommendation is critical whenever a safe harbor from wireless technology evolution is desired.



Unlicensed Etiquette Statement

In unlicensed bands, FCC rules provide that unlicensed users must accept interference (and may not cause harmful interference).

Although this regimen has worked well; now may be the right time for the FCC to investigate potential next steps in the evolution of the “digital etiquette”.

Recommendations

- *SDO's should continue to coordinate with each other to facilitate co-existence.*
- *Non-standard wireless solutions should strive to protect the commons in ways that allow the operation of other technologies.*
- *As new frequency bands are allocated there may be significant value in re-examining co-existence techniques for unlicensed spectrum. the FCC should be open to future policy supporting ultra-efficient spectral technologies which may require that some newly allocated bands be restricted to use of specific technologies and or control protocols*
- *The IPv6 network protocol offers several advantages over IPv4 ... and should be used where feasible.*



Back-up & Reference Material



IPv6 as an enabler of IOT

- IoT with its projected Billions of devices will require the use of IPv6.
- Only 84. billion total IPv4 address 90% already exhausted.
- Advanced features of MIPv6 will enable greater mobility and security needed for IOT devices.
- Use of IPv6 and MIPv6 will decrease the use of spectrum capacity and network resources allowing for quicker growth of IOT devices.
- IPv6 will Lower power usage of IOT devices. Resulting increased Battery life and smaller lighter IOT devices
- Since large scale deployment's of IOT devices will quickly exhaust IPv4 resources we recommend that all IOT devices be IPv6 enabled and support the use of MIPv6

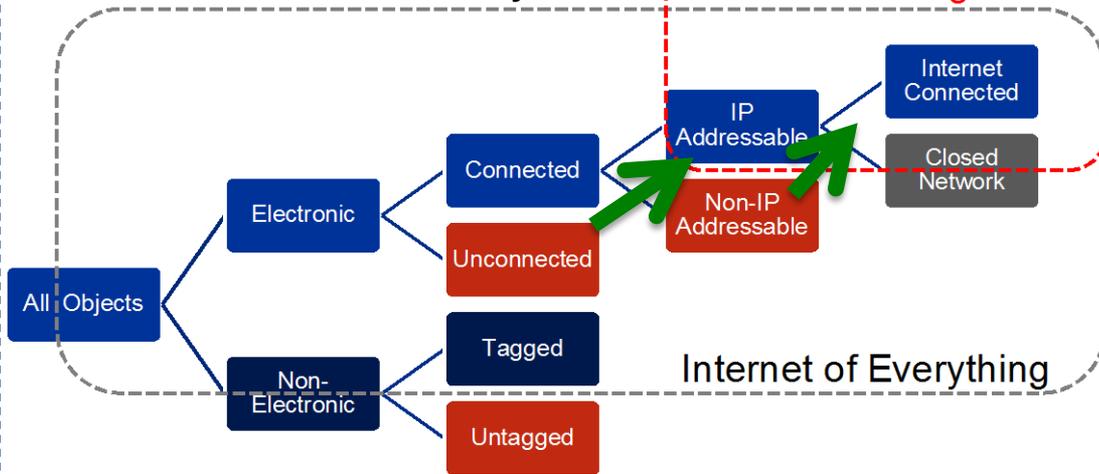


Narrowing the Scope – Connected Devices

Global Reports

Source Courtesy of Bill Morelli, IHS

TAC Focus – US Only



Potential Growth items to Consider:

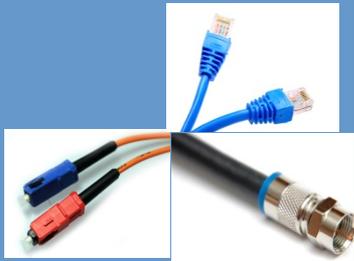
- Disruptive Business Models (OTT's and more)
- Low cost of cloud computing promotes connectivity
- Desire to capture previously "transient" data for analytics
- Video enabled devices
- Forward looking projections based on current apps. New apps could accelerate #'s

IoT Connectivity Technologies

Source: Courtesy Bill Morelli, IHS Technologies

Wired

- Ethernet, Coax, Fiber, etc. considered as a single category



WPAN

- ANT+
- Bluetooth – Classic & Smart Ready
- Bluetooth Smart



WLAN

- ZigBee PRO
- ZigBee RF4CE
- ZigBee Multi-Protocol
- EnOcean
- ISA100.11a
- WirelessHART
- Z-Wave
- Other 802.15.4



- 802.11a/b/g
- 802.11n
- 802.11ac
- 802.11ad
- Other 802.11
- DECT ULE
- Other 2.4GHz
- Other Sub-GHz



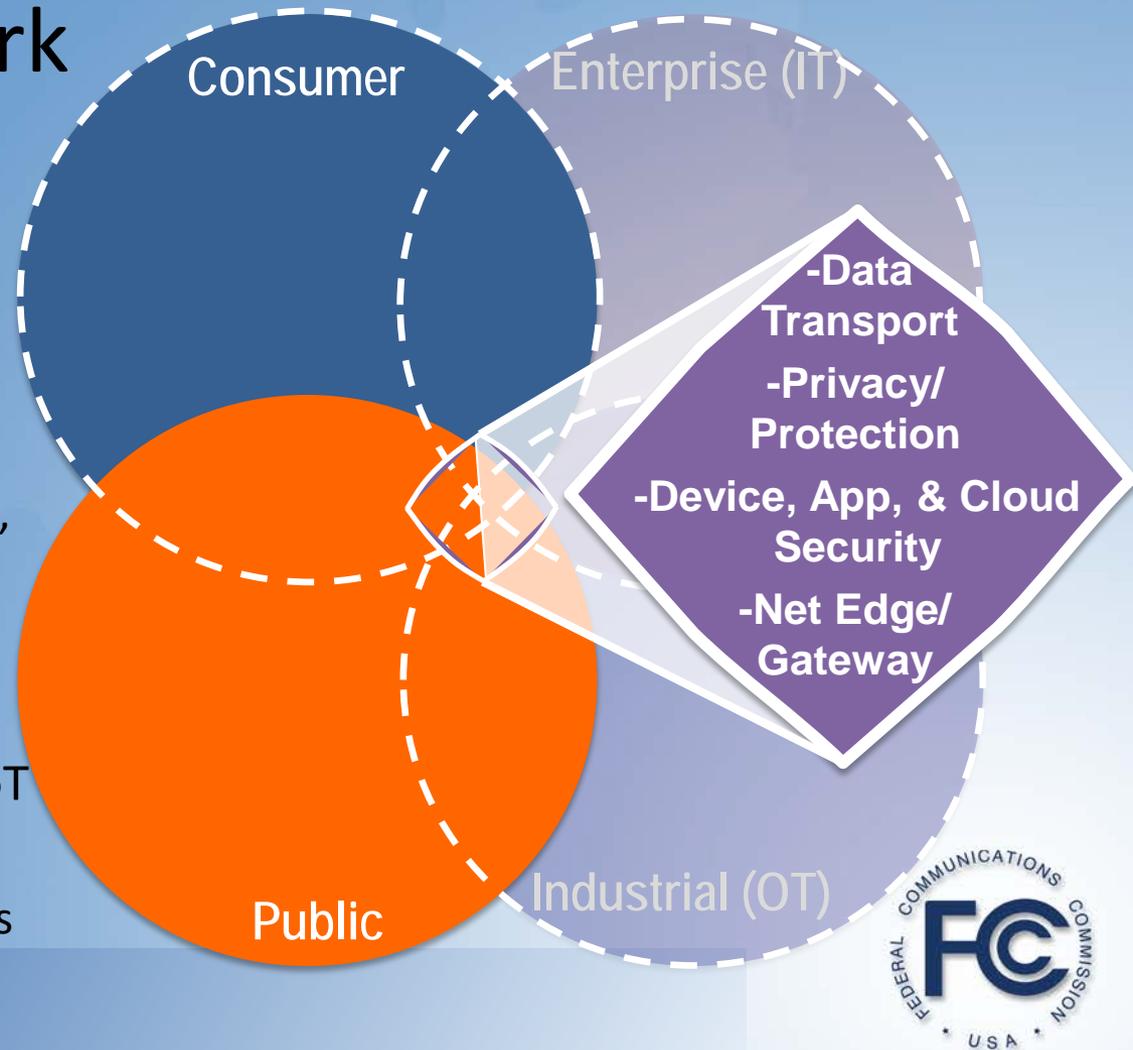
WWAN

- 2G Cellular
- 3G Cellular
- 4G Cellular



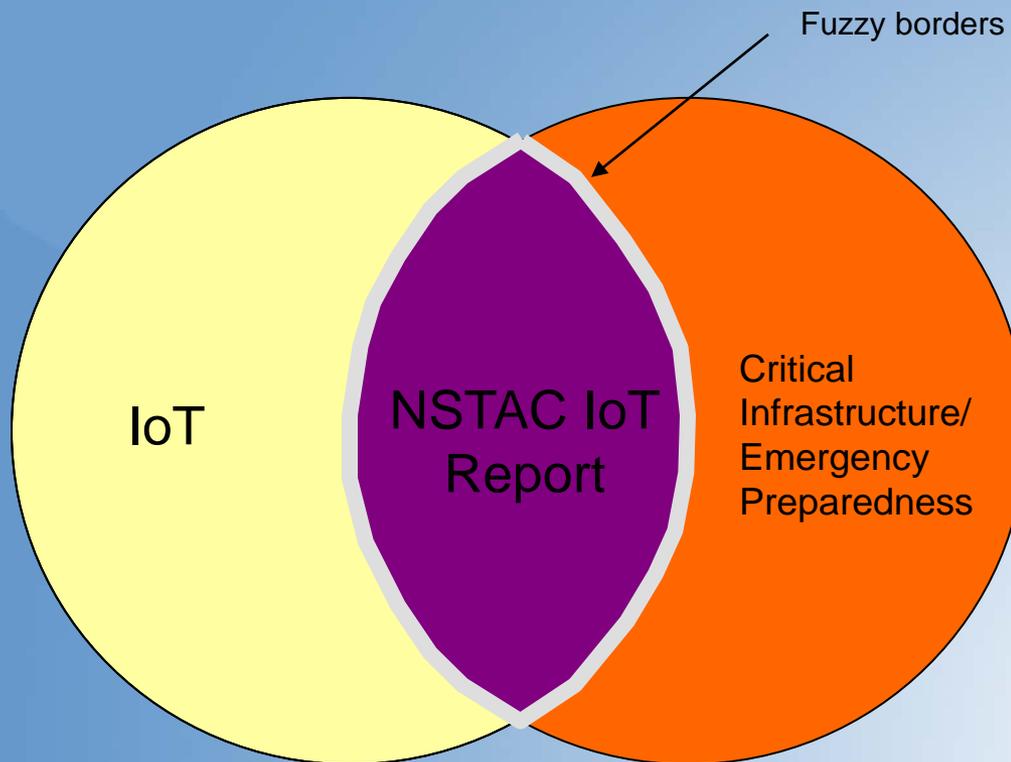
Security Framework

- Outline IoT related security gaps/concerns.
 - Issues? Things? Network Security? Data security?
- Systematic Approach:
 - Identify/Access, protect, detect, respond, recover
- TAC must have “FCC lens” on topic
- There is a hand-off between IoT security and Cybersecurity
 - Relationship, intersection needs to be determined





Scope of NSTAC Report



Key Findings on IoT



- Dangerous – IoT allows remote attackers to do a lot of damage.
- Unstoppable – It will happen regardless what the government does
- Ubiquitous – Critical Infrastructure can't avoid IoT even if they try
- Unpredictable – We don't know what new attack vectors IoT will create
- Security Afterthought – In the push to get things to the market, security often not considered initially



Technological Advisory Council

Spectrum and Receiver Performance

Working Group

December 4 , 2014



2014 Mission

- **Make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a system and receiver perspective**
- **Provide support as the Commission considers TAC recommendations related to the proposed interference limits policy**
- **Conduct analysis and make recommendations related to enforcement issues in a rapidly changing RF environment**



Working Group

- **Chair:**

- Lynn Claudy, NAB

- **FCC Liaisons:**

- Julius Knapp
- Uri Livnat
- Bob Pavlak
- Matthew Hussey

- **Participants / Contributors:**

- Dale Hatfield, John Cook, University of Colorado
- Greg Lapin, ARRL
- Pierre de Vries, Laura Littman, Tyler Cox, Silicon Flatirons
- Brian Markwalter, CEA
- David Gurney, Motorola Solutions
- Geoff Mendenhall, GatesAir
- Rauf Hafeez, AT&T
- Hossam H'Mimy, Ericsson
- Robert Miller, incNetworks
- Patrick Welsh, Kitty O'Hara, Max Solondz, Verizon
- Doug Brake, Information Technology & Innovation Foundation
- Mike Marcus, Marcus Spectrum Solutions
- Scott Burgett, Garmin
- Dennis Roberson, Illinois Institute of Technology



Working Group Areas of Focus

- **Develop recommendations about statistics of interference and risk-informed decision making**
- **Interference resolution, enforcement & radio noise**
 - **Recommend strategies for interference resolution and enforcement to address new RF environment challenges**
 - **Coordinate with CSMAC in the development and recommendation of enforcement strategies for a shared spectrum environment with federal incumbents**
- **Explore technical topics on receiver performance and emerging radio technologies for a shared spectrum environment**



Risk-informed interference assessment

Goals and Scope

- Goal: Find quantitative ways to reason about the risks of harmful interference due to changes in radio service rules, e.g. new allocations, rule changes, and waivers
- Immediate objective: Begin a conversation about how to implement a balanced risk assessment when assessing harmful interference
- Focus on the assessment of harmful interference during rulemaking
 - not adjudication & enforcement
 - not cost / benefit trade-offs
- This work is a complement to customary and well-established ‘worst case’ analysis





Risk-informed interference assessment

Background

- Need statistical analysis of interference scenarios because
 - There are many causes and consequences of RF interference
 - Selecting a single value (often ‘worst case’) isn’t representative
 - Over-conservatism due to worst case analysis can lead to the full value of spectrum use not being realized
- Problem was examined from several perspectives
- Opportunity: broaden analysis from “What’s the worst that can happen?” to “What can happen, how likely is it, what are the consequences?”



Risk-informed interference assessment

Definitions

- Risk-informed decision-making (RIDM): An approach to regulatory decision-making in which insights from probabilistic risk assessment are considered along with the public interest and other engineering insights
- Risk Assessment. An analysis technique that sets out to address three questions: (1) what can go wrong? (2) how likely is it? and (3) what are the consequences?
- Risk-informed interference assessment (RIIA): A systematic analysis of the likelihood and consequence of interference hazards caused by the interaction between radio systems



Risk-informed interference assessment

Risk Matrix

			Likelihood				
Qualitative descriptors			Rare	Unlikely	Possible	Likely	Certain
		Quantitative scales	Determined case by case				
Consequence	Very High Severity	Determined case by case	Yellow	Orange	Red	Red	Red
	High Severity		Yellow	Yellow	Orange	Red	Red
	Medium Severity		Green	Yellow	Yellow	Orange	Red
	Low Severity		Green	Green	Yellow	Yellow	Orange
	Very Low Severity		Green	Green	Green	Yellow	Yellow



Risk-informed interference assessment

Elements of a risk-informed interference assessment

- An inventory of all significant harmful interference hazard modes
- Determination of an impact metric to characterize the severity of any of the hazards in a common way
- Assessment of likelihood and severity for each hazard mode
- Guidance from FCC on what risks are acceptable, i.e. combinations of likelihood and consequence that would be considered harmful, or not
 - Engineering assumptions are influenced by the legal and economic context, and vice versa

Risk-informed interference assessment

Advantages of probabilistic risk analysis

- More complete representation of risk than a single-scenario worst case
 - Allows joint consideration of pervasive, low impact interference hazards as well as rare, catastrophic harms
- A structured way to consider and compare many failure scenarios
- Impact metrics + probabilistic analyses are useful for comparing scenarios
- Quantification clarifies what the community of experts knows or does not know, highlighting areas where the record is insufficient
- Provides objective data to commissioners about adverse impact of a new service when weighing benefits of a new service against costs to incumbents





Risk-informed interference assessment

Recommendations

- Changing the culture is going to take a long time, so start small BUT start soon
- Get the community thinking about risk-informed analysis
 - e.g. TAC intro paper, later perhaps bulletins, PNs, NOIs as appropriate
- Develop know-how in the agency
 - Institute annual guest lecture or lecture series on modern risk management
 - Add course(s) on statistics and risk-management at FCC University
- Encourage use of risk-informed interference assessments
 - Pilot approach on low risk/impact proceedings on a voluntary basis, e.g. waivers for services at fixed locations
 - Use quantitative risk assessment in FCC's own analysis



Interference Resolution and Enforcement

- Focus Areas
 - Recommend strategies for interference resolution, enforcement in order to address changing RF environment
 - Coordinate with CSMAC in the development and recommendation of enforcement strategies for a shared spectrum environment with federal incumbents
- Background and Prior Accomplishments
 - Released White Paper: “Introduction to Interference Resolution, Enforcement and Radio Noise”
 - Initiated informal coordination with CSMAC in the development of enforcement strategies for a dynamic federal – non-federal shared spectrum environment





Interference Resolution and Enforcement

- Progress subsequent to enforcement white paper
 - Separated effort to further analyze and develop recommendations regarding the use of transmitter identifiers
 - Studied emission designators as a tool
 - Studied impacts of Passive Intermodulation (PIM)
 - Concepts included in “Straw-man” Enforcement Proposal by the Enforcement Subcommittee of the CSMAC (discussed below)



Interference Resolution and Enforcement

- Progress In Coordination with CSMAC
 - Received briefing from co-chairs of the Enforcement Subcommittee of the CSMAC on a “Straw-man” Enforcement Proposal
 - Proposal assumes
 - A commercially operated SAS
 - Real-time spectrum monitoring operated by federal government incumbents and
 - A spectrum monitoring program operated by NTIA
 - Focuses on protection of incumbent federal government systems
 - Assumes the existence of interference limits proposed by TAC
 - Focuses on aggregate interference case and the concepts can be utilized for other cases e.g., single interferer





Interference Resolution and Enforcement

- Working group feedback on “Straw-Man” enforcement proposal
 - Generally supportive of the concept and direction
 - Concerns expressed related to
 - Who would be responsible for developing the various interference resolution and enforcement systems
 - Interworking between SAS and other systems
 - Potential cost



Interference Resolution and Enforcement Recommendations

- Incorporate the results of the work on (a) transmitter identifiers, (b) emission designators, and (c) PIM, into the “Straw-man” proposal
- Continue coordination with CSMAC on the development and refinement of the “Straw-man” proposal
- Address issues associated with the interworking between SAS and the other systems identified in the “Straw-man” Proposal
- Address the issues and potential solutions where interference is causing an immediate threat to the safety of life and property (e.g., increased automation of interference detection, classification / identification, location/direction finding, and reporting)



Transmitter Identifiers

- Identifiers have been used since the beginning of radio to identify the source of a transmission. One useful application of a transmitted identifier is recognition and eventual mitigation of an interference source
- As we move forward to systems of managed spectrum, we examine the utility and need for transmitter identifiers. While some transmitters will continue to identify themselves over-the-air, others may only be known to a central manager that can correlate reported behavior to the actual transmitter

Transmitter Identifiers

Topics

- Future identifiers
- Identifiers as an aid to enforcement
- Identifiers in managed spectrum
- Recognition of managed transmitters by other services



Transmitter Identifiers

Future Identifiers

- Identifiers historically were assigned to licensees by FCC
 - In modern systems hardware embedded identifiers are used to manage networking (e.g. MAC addresses)
 - Can the same hardware be used for over-the-air identification of an interfering radio signal?
- In managed spectrum systems, identifiers are used within the system to identify individual transmitters
 - Both unique and temporary identifiers in cellular systems
 - Hardware MAC address in WiFi systems
 - Granting frequency requests in shared spectrum





Transmitter Identifiers

Identifiers as an Aid to Enforcement

- Four common types of interferers:
 - Inadvertent hardware failure
 - Anomalous propagation conditions
 - Intermodulation
 - *Malicious (for future study)*
- Recognition of an identifier in an interfering signal can make it easier to locate the source of interference, without involving the Enforcement Bureau
- Identifiers must be made available in a database
 - *Privacy expectations (for future study)*





Transmitter Identifiers

Identifiers in Managed Spectrum

- Identifiers tell the Spectrum Access System (SAS) manager about the location and power of transmitted signals
 - ID may be transmitted to the SAS via internet, not over the managed band
 - Allows the SAS to allocate frequencies to minimize interference
- SAS identification of interferers – examples:
 - Ex Ante – Manager-based interferer determination by momentary scheduled RF power reduction of transmitter
 - Ex Post – Correlation of interference reports with archived frequency use logs by the SAS manager





Transmitter Identifiers

Recognizing Managed Transmitters by Other Services

- Inter-service Interference
 - Difficult to recognize the identity of transmitters in other services due to unknown modulation
- If victim captures a spectrum snapshot (the I/Q data)
 - Can this be used as a signature to identify ex post facto the type of signal, or the service, that was causing the interference?
 - If an identifier is contained within the interfering signal, can the I/Q data be used to demodulate and obtain the identifier?
 - *Signatures (for future study)*



Transmitter Identifiers

Future work

- Identifying malicious interferers
- Privacy vs. identification of transmitters to mitigate interference
- The determination of signatures from I/Q data to identify interferers
- Examine formats of transmitter identifiers that can be understood by other services



Actionable Recommendations to the FCC

- Identify technical collaboration opportunities between TAC, CSMAC and other federal agencies
 - Investigate and refine methods of statistical interference assessment
 - Coordinate on shared spectrum methods of interference resolution and enforcement
- Explore areas where risk informed interference assessment might be used, e.g. waivers
- Investigate policies (retention, privacy) to define what data should be contained in managed spectrum database(s)



THANK YOU



Technological Advisory Council

Advanced Sharing and EWT WG

December 4, 2014



Charter

- Establish an advanced sharing framework to enhance spectrum efficiency while protecting incumbent services, including both Federal and non-Federal services
- Identify and evaluate enabling technologies to enhance sharing efficiency, develop requirements for protection of incumbent services, and encourage co-existence of Federal and non-Federal systems
- Provide recommendations to the Commission regarding the establishment and objectives of “RF Model City” where the proposed advanced sharing framework and enabling technologies can be tested and evaluated

WG Participants

- Co-Chairs:
 - Sanyogita Shamsunder, Verizon
 - Brian Daly, AT&T
- FCC Liaisons:
 - Michael Ha
 - Chris Helzer
 - Kamran Etemad
- Participants/Guest Speakers:
 - Mark Bayliss, Visual Link
 - John Chapin, DARPA
 - Lynn Claudy, NAB
 - Marty Cooper, Dyna LLC
 - Adam Drobot, OpenTechWorks
 - Kumar Balachandran/Mark Racek, Ericsson
 - Kevin Kahn, Intel
 - Milo Medin, Google
 - Dean Brenner/Luis Lopes/Etienne Chaponniere/Yongbin Wei, Qualcomm
 - Kevin Sparks/Milind Buddhikot/Harish Viswanathan, ALU
 - David Gurney/Bruce Mueller, Motorola
 - Prakash Moorut, Nokia Networks
 - Patrick Welsh/Arda Aksu, Verizon
 - Maqbool Aliani, Lightsquared
 - Neeti Tandon, ATT
 - Steve Sharkey, T-Mobile
 - Michael Fitz, TrellisWare

Enabling Technologies Sub-Working Group

- Identified candidate bands for future sharing
- Examined enabling technologies, including interference cancellation or suppression in LTE-Advanced
- Collaborated with NTIA ITS on radar-LTE small cell co-existence testing
- Final Recommendations

Approach To Shared Spectrum (from Sept 23 mtg)

Preferred candidate bands drawn from

- NTIA lists of candidate bands
- ITU-R candidate bands for IMT from JTG4-5-6-7.

< 3 GHz

> 3 GHz

Scope

3 GHz

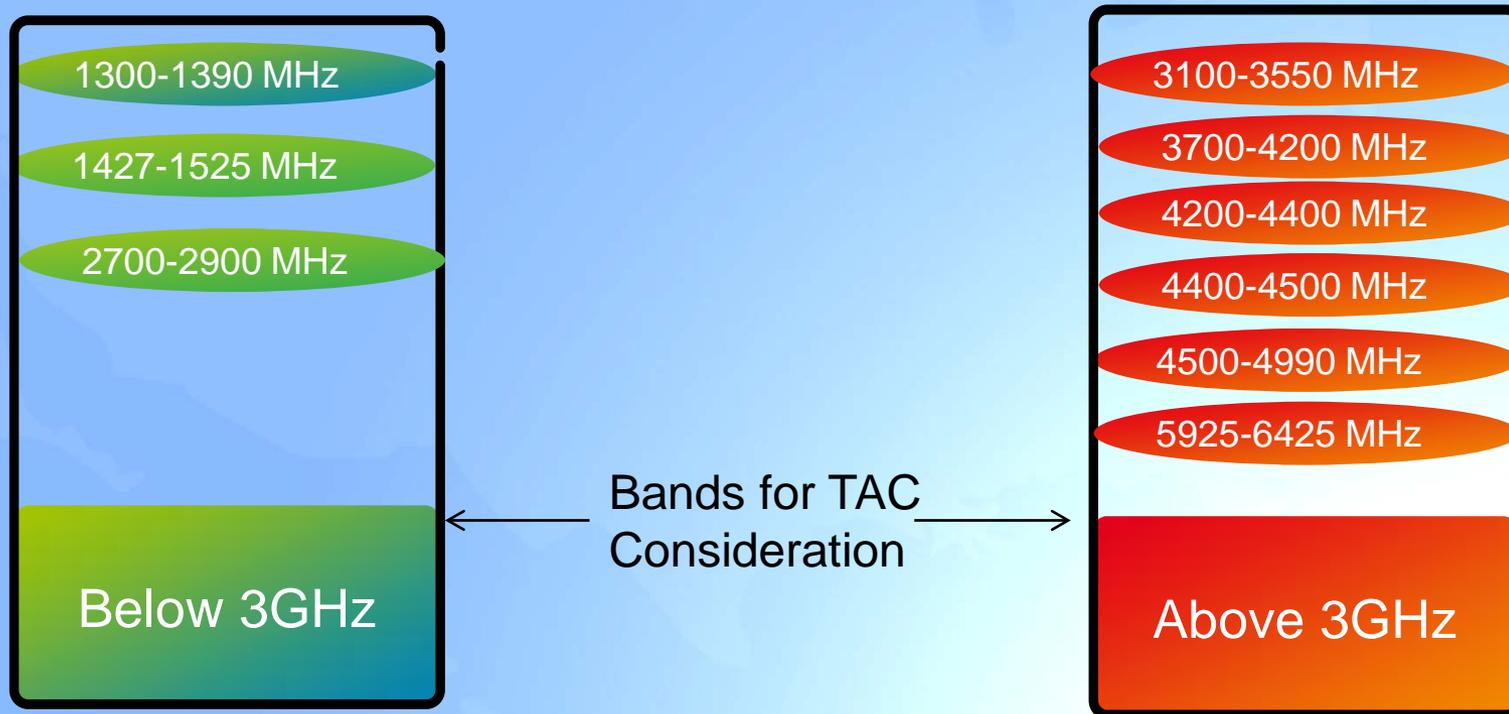
6.5 GHz

- Advantageous for area coverage
- Fewer incumbents and smaller exclusion zones are desired
- Need to maximize band size, expect at least 30-50 MHz

- Suitable for capacity enhancement
- May handle varying degrees of incumbent use
- Outdoor service is preferred and in-building-only service may offer additional interference protection mechanism
- Expected spectrum bonanza should be more than 100 MHz per band

Consider licensed, unlicensed and new spectrum sharing paradigms

Candidate Bands for Shared Use



- Advanced Sharing WG recommends the Commission to consider these bands for future sharing
 - Specific sharing model would depend on the incumbent types and available tools to manage interference among various systems

Sharing Compatibility: Traditional Mobile Broadband

Use Case or Deployment	Known Incumbent	Possible Bands
Macro/micro-cellular	FSS downlink Ground based ATC/ARS radar	1300-1390 MHz, 1427-1525 MHz, 2700-2900 MHz,
Small cell	FSS downlink, AMT, LoS links, portable fixed point-to-point	3100-3550 MHz, 3700-3800 MHz, 3800-4200 MHz, 4400-4500 MHz, 4500-4990 MHz
R-LANs	Radar, FSS, AMT etc.	3100-3550 MHz, 3700-3800 MHz, 3800-4200 MHz, 4400-4500 MHz, 4500-4990 MHz, 5925-6425 MHz (indoor only)
Backhaul: LoS	FSS uplink	5925-6425 MHz
Backhaul: NLoS	Radar, FSS, AMT	3100-3550 MHz, 3700-3800 MHz, 3800-4200 MHz, 4400-4500 MHz, 4500-4990 MHz, 5925-6425 MHz

Sharing Compatibility : Intelligent Transportation

Use Case or Deployment	Known Incumbent	Possible Bands
V2V	LoS, FSS, Aeronautical	4400-4500 MHz, 4500-4990 MHz, 5925-6425
V2I and I2V	LoS, FSS, AMT	3100-3550 MHz, 3700-3800 MHz, 3800-4200 MHz, 4400-4500 MHz, 4500-4990 MHz

V2V: Vehicle-to-Vehicle

V2I: Vehicle to Infrastructure

I2V: Infrastructure to Vehicle



Sharing Compatibility: Internet of Things (IoT)

Use Case or Deployment	Known Incumbent	Possible Bands
Short Range/Wearables	N/A	Further study needed to assess additional spectrum needs
Short Range/Local infrastructure	FSS uplink	3700-3800 MHz, 3800-4200 MHz, 4200-4400 MHz*, 4400-4990 MHz, 5925-6425 MHz
Short Range/Mesh and ad hoc	FSS downlink, FSS uplink, fixed services, AMT, LoS	Outdoor 3700-3800 MHz, 3800-4200 MHz, 4400-4990 MHz, Indoor operation: 4200-4400 MHz*, 5925-6425 MHz
Wide area connectivity/low bandwidth	FSS downlink Ground based ATC/ARS radar	Sub-GHz bands (to be studied), 1300-1390 MHz, 1427-1525 MHz, 2700-2900 MHz,
Critical Communications	FSS, LoS, microwave	3700-4200 MHz, 4400-4900 MHz

* (far away from airports)

LTE Advanced brings different dimensions of improvements

Leverage wider bandwidth

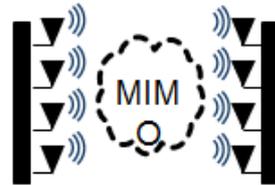
Carrier aggregation across multiple carriers, multiple bands, and across licensed and unlicensed spectrum



Higher data rates
(bps)

Leverage more antennas

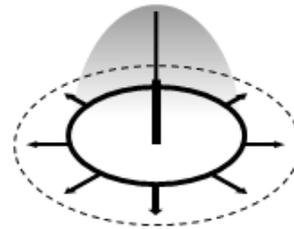
Downlink MIMO up to 8x8, enhanced Multi User MIMO and uplink MIMO up to 4x4



Higher spectral efficiency
(bps/Hz)

Leverage HotNets

With advanced interference management (FeICIC/IC)

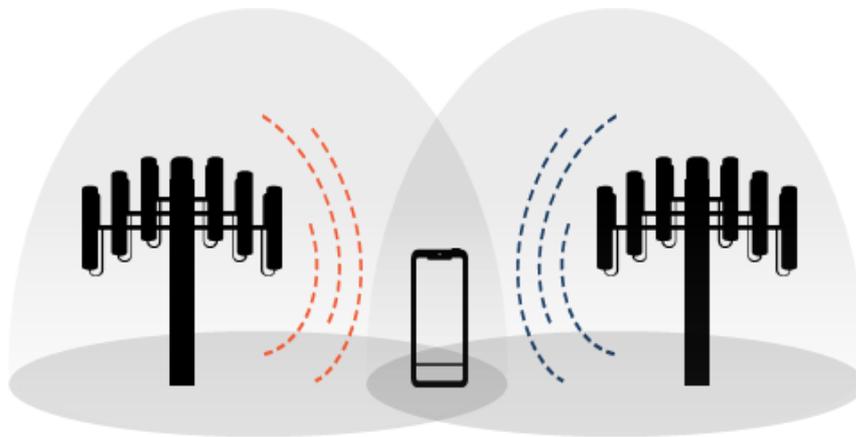


Higher spectral efficiency per coverage area
(bps/Hz/km²)

Small Cell Range Expansion

Enhanced receivers offer better user experience & more capacity

Interference Cancellation



Interference Cancellation	Rel. 10/11	Re. 12
Sync ref. signal	✓	✓
Common ref. signal	✓	✓
Primary broadcast channel	✓	✓
Data channel		✓

- Higher data rates especially at cell-edges

- More network capacity

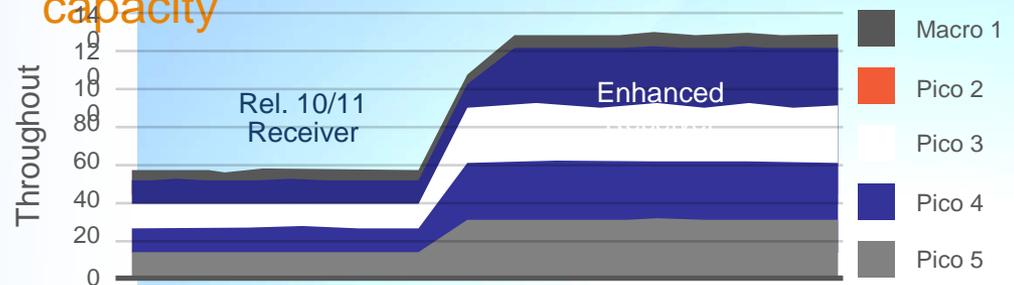
- Even more beneficial in managing interference in small cell deployments

Enhanced receivers further improve HetNet performance

- Live demonstration at MWC 2014, utilizing LTE Advanced test network in San Diego



Higher network capacity



Increased cell-edge data rates



Examples of LTE Features for Sharing

Example of LTE Feature	Enabler for	Comments / findings
Immediate Shutdown	Spectrum Clearing	Effective but calls drop.
Graceful Shutdown	Spectrum Clearing	Effective but TX dynamic range issue (Hardware & deployment dependency)
Cell Barring	Spectrum Clearing	Desired UE behavior depends on UE state. Use with other features.
UL pMax Control	Interference Management	Exclusion zone reduction benefit depends on RF conditions / path loss to UE.

- Current LTE standards and commercial equipment support enablers that serve as a foundation for a spectrum sharing solution
- Future LTE releases and products enable additional capability through such as features as carrier aggregation, load balancing and others

Key Learning: Interference Cancellation/Suppression of LTE Advanced

- Efficacy of interference cancellation depends on knowledge of interferer signal waveform at the victim system
 - Interference cancellation minimizes performance degradation at victim system
 - Statistical techniques are an alternative for *Interference Suppression* instead of cancellation
 - LTE UE has at least 2 RX antennas, and eNB has 2-8 RX antennas; spatial filtering is a powerful tool for interference suppression
- Interference cancellation/suppression is a very important aspect of LTE and LTE-Advanced
 - Today, it's used to improve data rates, especially at cell edge and add network capacity.
- Interference cancellation allows tremendous gains for the hetnet operator when small cells use the same frequency assignment as the macro coverage
 - This is a way to get effective reuse greater than unity

Key Learning: Radar/LTE Co-Existence

- Recent lab testing conducted by NTIA of LTE small cell/radar co-existence verified that LTE is quite robust vis-à-vis some radars, even with very high interference
 - Testing involved 24 unique radar waveforms– simple pulsed and LFM chirp– injected into LTE small cell downlink and uplink
 - Did not replicate any particular system and results could differ for other types of radars.
- Test reports available at:
<http://www.its.bldrdoc.gov/publications/2759.aspx>;
<http://www.its.bldrdoc.gov/publications/2760.aspx>

Propagation Models

- Propagation models are coexistence scenario-dependent
 - Worst-case vs Typical considerations are important
 - Site-specific vs. General and Empirical
- Current defaults:
 - Free space: LoS links such as for fixed systems
 - High tower systems for long range can use the Irregular Terrain Model (ITM)
 - Point-to-point and area modes available for ranges 20 MHz – 40 GHz and distances of 1-2000 km
 - Cellular systems typically use the Extended Hata model valid 30-3000 MHz
 - Valid to 40 km for NLoS and cluttered environment, with extension for short range use (Hata-SRD)
 - Some knowledge exists for models for 2-6 GHz, e.g. ECC Report 203
 - Various other approaches considered by NTIA and ITU-R sharing recommendations or CEPT studies
 - E.g. P.1546, P.452, EPM-73 etc.
- Methodologies and recipes needed for specific scenarios
 - Compatibility between different models in coexistence scenarios
 - Parameterization for specific frequency bands

Recommendations

- FCC and NTIA should continue their dialogue on making additional spectrum available for sharing, including the bands identified herein
 - Bands below 3 GHz should be prioritized for coverage, while those above 3 GHz may be restricted for small cell and short range applications only if wide area coverage is restricted by incumbent protection requirements
- Private sector should aid FCC and NTIA policy considerations of enabling wireless technologies for incumbents and new users of spectrum, including interference cancellation, interference suppression, and co-existence testing
 - Particular use cases will affect the extent to which advanced transmission and receiver techniques can be utilized
- FCC, NTIA and the private sector should jointly agree on pragmatic and realistic deployment models and coexistence requirements
 - Updated propagation models for sharing studies
 - Clutter, density of deployment and loading are key dependencies

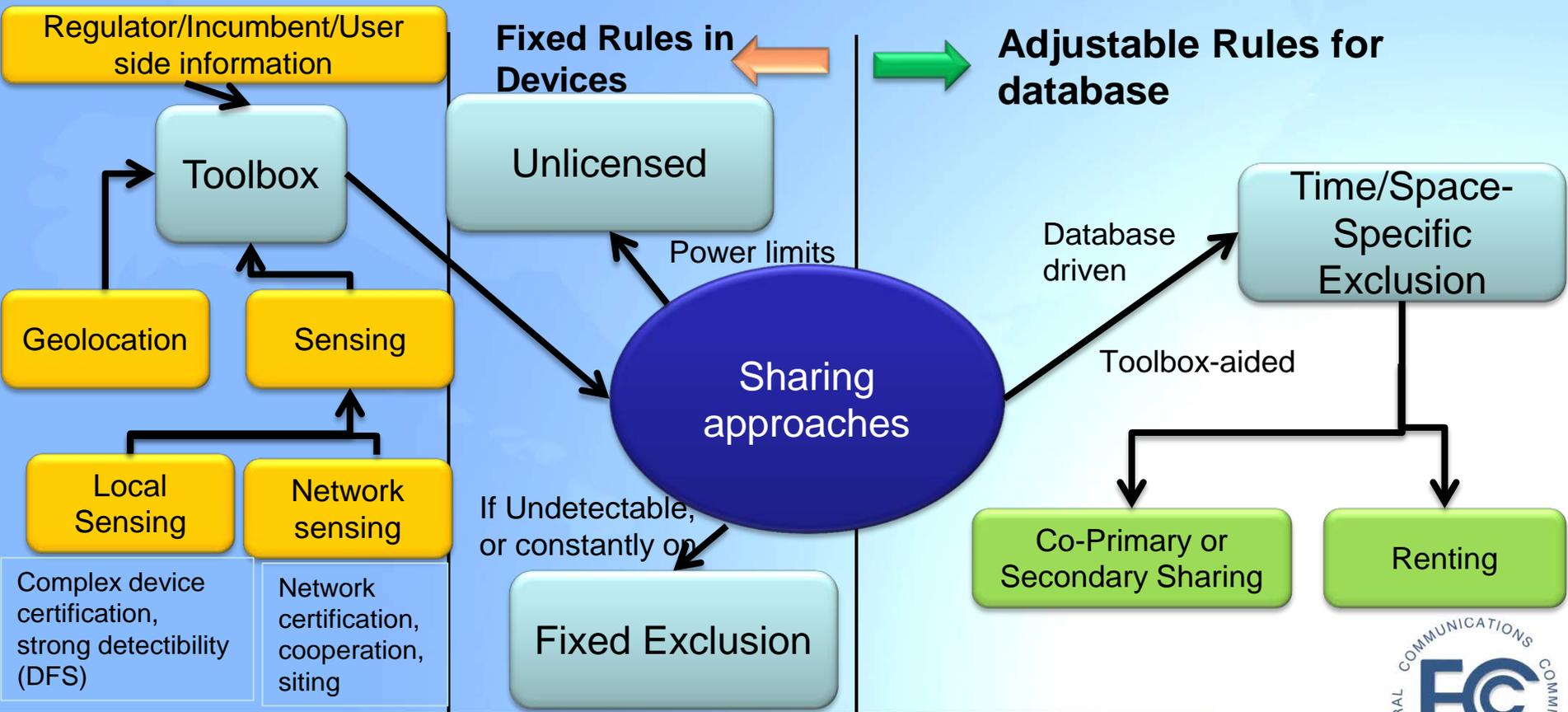


Database Subgroup Summary

- Subgroup explored a variety of database-based sharing methodologies
- Focus on advanced sharing techniques that go beyond what's being proposed in the 3.5 GHz FNPRM
- Sensing may enhance database approaches
- Wide range of implementation options spanning simple coarse grained decision making, more dynamic sharing with integrated user feedback, and detailed propagation modeling



Wide range of solutions should be considered in the creation of Spectrum DataBase (SDB) frameworks





Database Subgroup Summary on Enforcement

- Enforcement: how to identify and locate a rogue device or network of devices
 - One proposed answer is through interference measurement and reporting by devices, empowering the SDB to discover devices operating outside of it's authority
- Concern about predictability of operation of devices distributed through retail chains
 - To be used for lower tier type access and how to ensure they do not cause interference to protected users
 - All base station and user devices have the same operational requirements
 - Should go through the similar certification processes and they may interchangeably operate in protected or unprotected modes
- Need a well implemented certification of devices and have managed retail distribution of them if offered directly to end users like femtocells
- Crowdsourcing enforcement, possibly with incentives for reporting non-compliant devices could be an interesting approach
- → More Study and discussion is needed



Database Subgroup Summary on Security

- Spectrum sharing and Spectrum Database SDB should not expose information which are otherwise accessible through web
 - Concerns, e.g. National Security or user privacy, must be addressed with care
 - Queries to the database must be pertinent to purpose when indicative.
- Risk may be the ease of access to collected set of information provided to SDB
 - May not be a concern given that obtaining, collecting and tracking thru other means is also easy these days

→ More study and discussion on this issue is needed



Recommendations

- Static protection zones may be used when incumbent use is static and/or cannot be shared fully dynamically
- It is preferred to define Static Protection Zones based on incumbent protection criteria rather than fixed geographical zones.
 - Challenge is realistic propagation and interference modeling
- The SDB should not expose more information about Federal primary users than is already able to be determined publicly by other means
- Crowdsourcing enforcement, with possible reward mechanisms for participation can be explored



Additional Topics to Consider

- Enforcements
 - What are the goals of enforcement? How do we quantify enforcement? How much enforcement is needed in various sharing scenarios?
 - How do we design certification and enforcement processes to promote trust and innovation?
 - How much of the enforcement process can and should be automated? Is there a benefit to enforcing on a shorter time scale?
 - What role can crowdsourcing play in the process of enforcement?
- On Security:
 - What is the interplay between data collection for enforcement and privacy?
 - How do we design the entire sharing system to limit security and service degradation in the event of breaches?
- On Interoperation of Multiple SDBs
 - Information Exchange, what, how often, distributed/centralized synch
 - Selection of SDBs by authorized users
 - How to ensure value add services while avoiding conflict with other SDBs/SASs



RF Model City

- RF Model City concept has been discussed in multiple industry/academic workshops
- In particular, NSF hosted a workshop on Future Research Infrastructure for the Wireless Edge in November 2014, where infrastructure sharing was discussed in depth
- Aligning with Smart City initiatives may introduce additional interests from relevant parties

Potential Topics for 2015

- Smart Device Theft Prevention (aka MDTP) Continuation
- Spectrum & Receivers – Interference Limits Policy, Enforcement & Wireless Model City
- Massive MIMO and other Advanced Radio Technologies
- The Evolution of the Internet – Flat or Hierarchical – Taxonomies – Issues and Challenges
- Broadband for Underserved Communities (Rural and Urban)
 - Emerging Technologies to meet the needs
 - Role of Mobile Broadband
- Licensed vs. Unlicensed priorities
- Impact of Critical Infrastructure Services on the structure of future network infrastructures
- To allow personal encryption, or require back doors for law enforcement



Potential TAC Dates for 2015

- 3/11 (Wed)
- 6/11 (Thur)
- 9/24 (Thur)
- 12/3 (Thur)

