FCC Technological Advisory Council

2014

TAC Work Groups

- **Spectrum and Receiver Performance**
  - Chair: Lynn Claudy (National Association of Broadcasters)
- **Advanced Sharing and Enabling Wireless Technologies**
  - Chairs: 1) Ed Chen (Verizon), 2) Brian Daley (AT&T)
- **Internet of Things**
  - Chairs: 1) Dave Tennenhouse (Microsoft), 2) Russ Gyurek (Cisco)
- **Cybersecurity Initiatives**
  - Chair: Paul Steinberg (Motorola)
- **Supporting the Transition to IP**
  - Chair: Nomi Bergman (Bright House Networks)

Agenda

- New Work Groups Discussion
- Spectrum and Receiver Performance
- Advanced Sharing and Enabling Wireless Technologies
- Cybersecurity Initiatives
- Supporting the Transition to IP
- Internet of Things

New TAC Work Groups

- Electronic Reporting of Broadband Availability (Form 477)
- Smartphone Theft Deterrence

FCC TAC: IoT- June 10, 2014

What impact will IoT have on the network in 3 years, 5 years, 10 years?

IoT WG

June 10, 2014

- Russ Gyurek- (WG Co-Chair)
- David Tennenhouse- (WG Co-Chair)
- Walter Johnston (FCC)
- Shahid Ahmed
- John Barnhill
- Mark Bayliss
- Kevin Cage
- Greg Chang
- Marty Cooper
- Jeff Forester
- Mark Gorenberg
- Anoop Gupta
- Stephen Hayes
- Amit Jain
- Kevin Kahn
- Fred Kremmerer
- Brian Markwalter
- Lynn Merrill
- Vish Nandlall
- Jack Nasielski
- Ramani Pandurangan
- Deven Parekh
- Marvin Sirbu
- Kevin Sparks
- Glen Tindal
- Jack Waters

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

Actions

- Developed Taxonomy of IOT by vertical segment
  - Draft presented to TAC
- Mapped standards activity relevant to IOT
  - Draft presented to TAC
- Generated initial findings and strawman recommendations related to spectrum & IoT security
- Identified Next Steps

IoT Taxonomy by Vertical

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

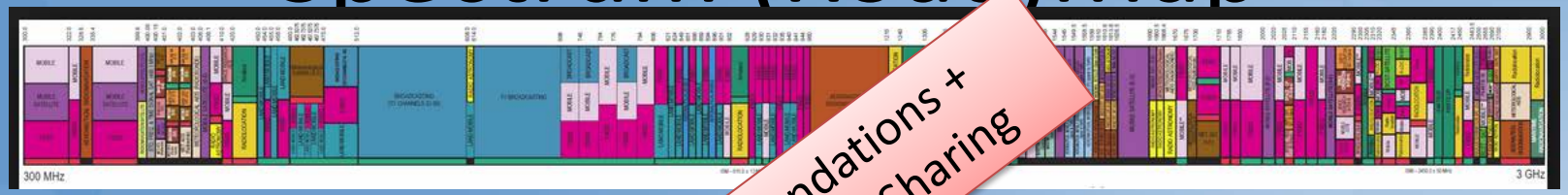
See Excel spreadsheet

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-techture: Other	Spectrum	Manage-ment	Operations & Maint	Applic…		…ss	Notes / Comments
Gov. Agency	No		NIST Framework for Improving Critical Infrastructure Cybersecurit… …has several. Etc						FCC						FCC, DOT, NIH,
IEEE	Yes	Mature	Wi-syn, 802.15.9	Varies by Society	802.11, 802.15.4 G, 80215.4-2011, 802.16, Ethernet, 1901.2	No	Yes: SmartGrid, Energy, Industrial, Agriculture, Mining	Not really 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, 6LoWPAN, RPL, MPL, CoAP	UDP, TCP				COMAN					

See Excel spreadsheet

Spectrum (Road)Map



Initial Finding/Recommendations + Liaison request to Spectrum Sharing

- Develop a spectrum road map focused on [illegible] we expect will be advantageous to IOT and under what auspices (e.g. license[illegible] spectrum access system control, etc.).
- a key aspect of IOT is sharable s[illegible]urces
  - what we know now, and w[illegible]ccur with as much detail as possible would be useful both to inform and to start a d[illegible]
  - Near term somew[illegible]wever, need to have roadmap of what will happen in next 5 years, 10 years…
  - What will end? M[illegible](2G)
  - Future Wireless City?
  - Reclamation opportunity (spectrum group read-out?). Adv. Sharing and Receiver group?
- An annotated band plan focusing on spectrum opportunities for IOT would be beneficial to the FCC

Connectivity Framework

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

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

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

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

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

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

3. **Thing to Internet** (e.g., direct connection to 4G networks, 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

Connectivity Framework (cont'd)

IoT dilemma

→ Significant fraction of "things" will have 10+ yr lifetime

→ want to encourage rapid adoption of ongoing advances in spectral efficiency and security technologies

Potential "best practice"

- Long-lived things use short range Thing-to-Proxy links that are amenable to very high level of spatial reuse
- Proxy upstream links are periodically upgraded to take advantage of new technologies

Spectrum: Initial 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 will 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: Strawman Recommendations

- No unique allocations of spectrum to IoT are required [with the possible exception of short-range unlicensed spectrum that is subject to very high spatial reuse]
- 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
- 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)

Security: Initial Findings

Growth of IOT will greatly increase the *attack surface*.

- Solution remains industry responsibility; government may be involved in establishing the overall framework.
- Critical devices affecting safety of life and property may have additional security requirements set by relevant government agencies and/or standards bodies

For most IoT-sourced data to be actionable, there must be mechanisms to authenticate its provenance (e.g., via identity and authentication of sources).

Scale of deployment may require that devices should have a secure approach to planned end of life (similar to the approach taken to limit satellite debris)

Long-lived / low-cost things pose additional challenges:

- They may not be capable of sustaining security and authentication over time and secure channels to upgrade software/security many not be cost-effective.
- One approach may be to rely on upgradeable secure proxies to geographically limit systemic exposure to wide-scale attacks. This remains to be investigated.

Security: Strawman Recommendations

- IoT suppliers should adopt security capabilities that are current with industry best practice at the time of shipment and have actionable plans for dealing with post-shipment changes in the threat landscape
  - For example, a secure channel to upgrade devices and/or their proxies
- Mechanisms should be provided to authenticate the provenance of IoT-sourced data, at least to the level of the first proxy through which the data passed.
- FCC should focus its security efforts on limiting misuse of spectrum (e.g., malware or faulty workmanship that continuously transmits or transmits too much power).
- FCC should seek to coordinate IOT security needs with other government stakeholders

Next Steps

- Develop use cases for most common classes of IOT devices
- Sizing of IoT-related spectrum requirements:
  - Short range (PAN/LAN) communication
  - Impact of IoT traffic on upstream communication links
  - Exceptional cases, if any, that may require direct “thing-to-Internet” communication and cannot be served by existing services such as 4G networks
- Investigate approaches to stimulating IoT growth by ensuring that availability of short range (PAN/LAN) spectrum will stay well ahead of demand – **partner with spectrum sharing working group**
- Identify additional opportunities for FCC to enable iot industry innovation spur IoT innovation/adoption; Identify potential blockers and approaches to their removal
- Engage stakeholders on vetting of strawman recommendations

Technological Advisory Council

Spectrum and Receiver Performance

Working Group

10 June 2014

2014 Mission

- **The working group will make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a system and receiver perspective**
- **The working group will provide support as the Commission considers TAC recommendations related to the proposed interference limits policy**
- **The working group will conduct analyses and make recommendations related to enforcement issues in a rapidly changing RF environment**

Working Group

- **Chair:**
  - Lynn Claudy, NAB
- **FCC Liaisons:**
  - Julius Knapp
  - Bob Pavlak
  - Matthew Hussey
  - Uri Livnat
  - Bob Weller

- **Participants / Contributors:**
  - Dale Hatfield, John Cook, University of Colorado
  - Greg Lapin, ARRL
  - Pierre de Vries, Laura Littman, Silicon Flatirons
  - Brian Markwalter, CEA
  - David Gurney, Motorola Solutions
  - Geoff Mendenhall, GatesAir
  - Rauf Hafeez, AT&T
  - Hossam H'Mimy, Ericsson
  - Jesse Russell, Robert Miller, incNetworks
  - Patrick Welsh, Kitty O'Hara, Max Solondz, Arda Aksu, 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

- Complete white papers and briefings (initiated 2013)
- Develop proposed charter for multi-stakeholder group
- Develop recommendations about statistics of interference
- Assess technical topics on receiver performance
- Interference resolution, enforcement & radio noise
  - Recommend FCC share information about interference incidents
  - Investigate noise floor impact on radio services
  - Recommend strategies to address RF environment challenges

White Papers and Briefings

- **Publish White Paper on "Introduction to Interference Resolution, Enforcement and Radio Noise" (June '14)**
- **Presentation to TAC members and FCC staff on "Impact of Emerging Receiver Technologies on Changing Standards and Spectrum Allocations" (June '14)**
  - **Receiver hardware**
  - **Dynamic interference mitigation**
  - **Software Defined Radio (SDR)**

Multi-Stakeholder Organization (MSH)

- **Recommend charter for interference limits MSH group**
  - **Outline scope of MSH operations and objectives**
- **Draft prepared for full TAC review June 10, 2014**

Statistics of Interference

- **Situation**
  - **Causes and consequences of RF interference events vary greatly across diverse radio services and industries**
  - **… so understanding and predicting risk requires statistical analysis of scenarios; Risk = probability x magnitude**
  - **Worst-case analysis is necessary but insufficient**
    - **Focuses on magnitude, ignores probability**
- **Opportunity**
  - **Many regulated industries have developed methods for risk-based analysis**
  - **Wireless standards bodies use statistical methods, e.g. Monte Carlo analysis**
  - **… provides a basis for FCC to extend its analytical toolkit beyond worst-case**
- **Overall goal of work stream**
  - **Make recommendations about the use of statistical methods and metrics in the formulation of rules and analysis of harmful interference**

Statistics of Interference Work Plan

- **Survey of the use of statistical risk management, rules and regulations**
  - **Review the use of statistical interference metrics by FCC: DONE**
  - **Review statistical risk analysis used in other regulatory contexts: DONE (below)**
  - **Review use of statistical techniques by industry: PENDING**
- **Examine past FCC proceeding(s) to inform the application of risk-informed hazard assessment to spectrum**
  - **Planned for 3rd Quarter; in scoping phase now**
- **Make recommendations on the use of statistical interference risk management techniques by FCC**
  - **Slated for 4th Quarter**

Risk Informed Decision Making (RIDM)

Used by Other Federal Regulators

- Consider lessons learned from Nuclear Regulatory Commission (NRC)
  - A complement to “deterministic” methods (e.g. subsystem safety margins)
  - Widespread implementation by 2000s, enabled by advanced computers
  - Used for licensing requirements and regulatory decision making
- Potential benefits of RIDM in spectrum management include
  - In-depth understanding of system failures; ability to identify complex interactions due to RF propagation and space/time proximity of radios
  - Better communication among stakeholder groups about problems
  - Better allocation of resources; avoiding “worst case” for every factor in power budgets
- Criticisms of RIDM include
  - Complexity, errors difficult to estimate, requires new regulations

Technical Topics on Receiver Performance

- Survey of emerging receiver technologies - DONE
- Assess key receiver performance factors
  - Relevant to cross-service radio coexistence
  - Across categories of diverse radio services
- Review industry activities and standardization
  - Identify opportunities for cross-industry coordination
  - Identify technical topics in wireless coexistence and inter-system interference analysis, such as
    - RF propagation models, receiver characteristics, industry performance metrics

Interference Resolution, Enforcement and Radio Noise

- White paper draft complete; TAC review June 10, 2014
- Recommendations - FCC should:
  - Release summary information on interference complaints
  - Convene workshops - interference resolution & enforcement, noise floor characterization
- TAC work group in 2H'14 will
  - Investigate public-private partnership as a forum for voluntary & systematic sharing of information on interference incidents
  - Recommend strategies for IX resolution / enforcement

Major Milestones

- **2Q'14**
  - **Completed enforcement white paper and emerging receiver technologies briefing**
  - **TAC proposed charter for multi-stakeholder group**
- **3Q - 4Q'14**
  - **Workshops and investigation report on interference resolution, enforcement, and radio noise**
  - **Analysis of past proceeding(s) for use of risk-informed interference harm analysis**

Major Milestones

- **3Q - 4Q'14**
  - **Recommendations for the use of risk-informed interference harm analysis**
  - **List of technical questions to industry about receiver performance, standards, and causes of inter-system interference**

THANK YOU

Technological Advisory Council

Advanced Sharing and EWT WG

June 10th, 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
  - Robert Weller
  - 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/Etieen Chaponniere/Yongbin Wei, Qualcomm
  - Kevin Sparks/Milind Buddhikot/Harish Viswanathan, Alacatel-Lucent
  - David Gurney/Bruce Mueller, Motorola
  - Moorut Prakash, Nokia Solutions Network
  - Kitty O'hara, Verizon
  - Steve Sharkey, T-Mobile
  - Michael Fitz, TrellisWare

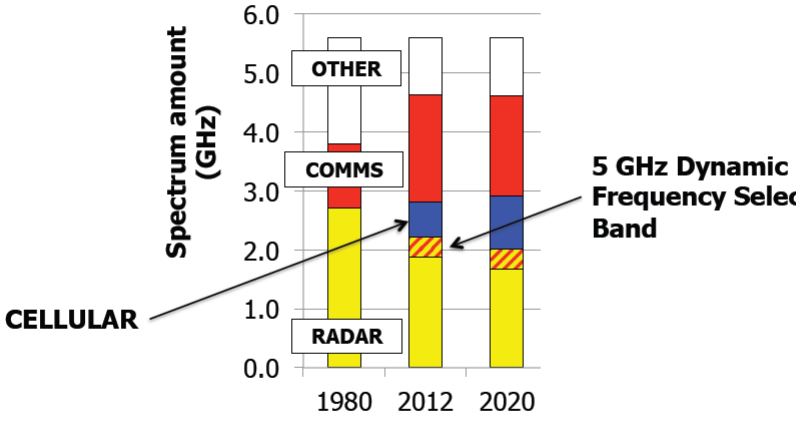
Progress to date

- Review of various sharing models and implementations
  - Exclusive Licensing Model
  - Unlicensed Model
  - White Space Database
  - 3.5GHz DAS
  - CSMAC and others
- Creation of two Sub-WGs
  - Enabling Technologies
  - Database Structure
- Key areas of focus for recommendations
  - Interference Cancellation
  - In-building only Service
  - Database Architecture and Compatibility
  - RF Model City

Spectrum Allocation under 6GHz

DARPA Motivation for radar/communications spectrum sharing

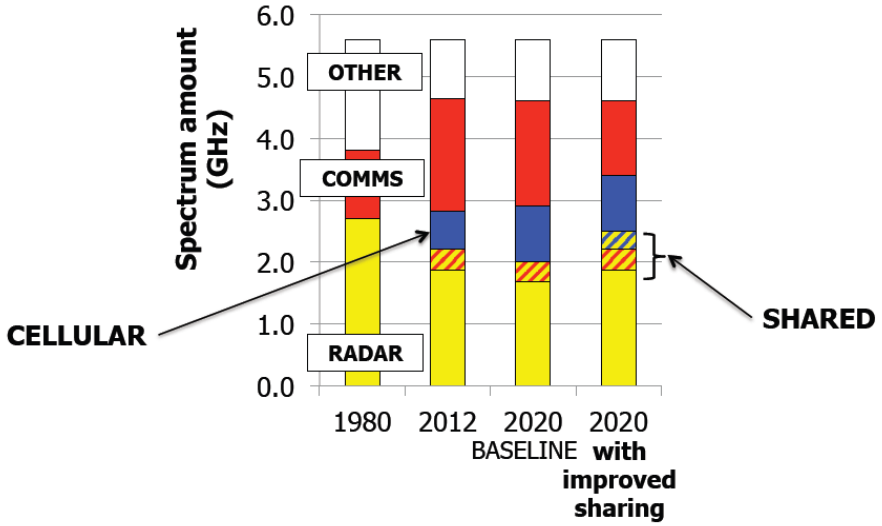
US amount allocated 400 MHz – 6 GHz



2020 prediction is result if planned 500 MHz spectrum transfer to broadband wireless is evenly between non-cellular comms (TV, federal) and radar.

DARPA Opportunity for a win-win capability increase

US amount allocated 400 MHz – 6 GHz



Sharing Types

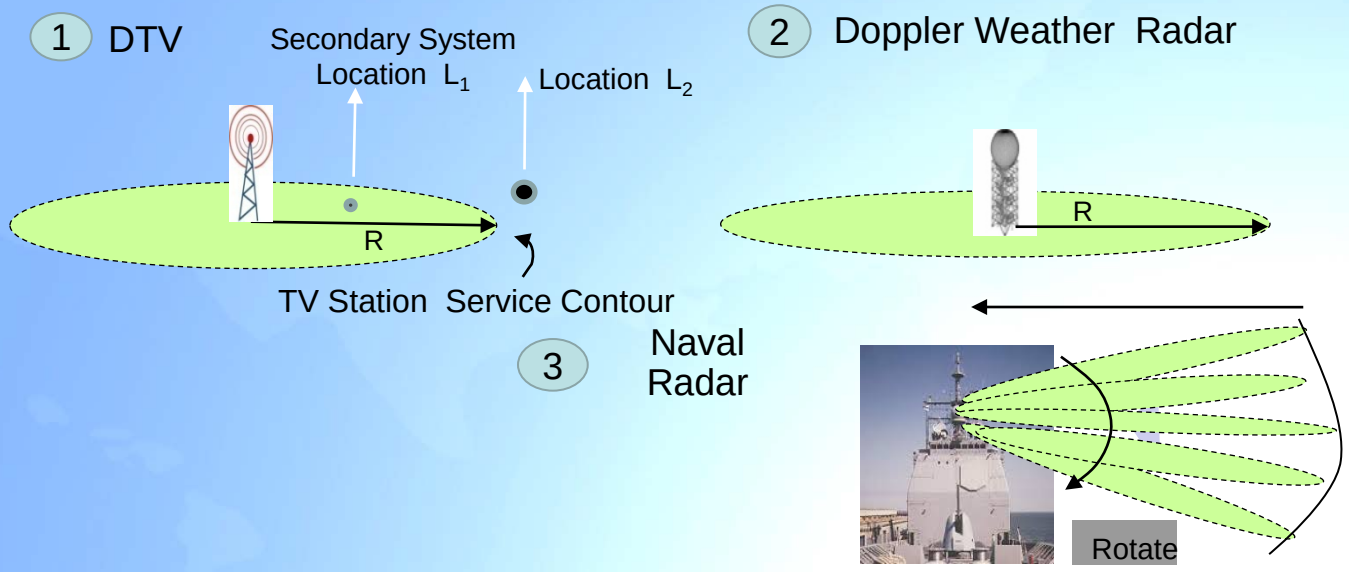
Basic principle of sharing: *Separate* multiple spectrum users e.g.: primary and secondary in various dimensions (e.g.: space, time and frequency)

- **Separation in space:** Operate primary and secondary systems in mutually exclusive / non-overlapping areas of space allowing concurrent use of same channel
- **Separation in Time:** Primary and secondary systems operate in same space and frequency but transmit at *mutually exclusive times*
- **Separation in Frequency:** (Dynamically) assign different frequencies to primary and secondary systems for concurrent operations in space and time

Sharing Types: In Space

Exclusion zone around primary: *Space around primary where secondaries cannot operate*

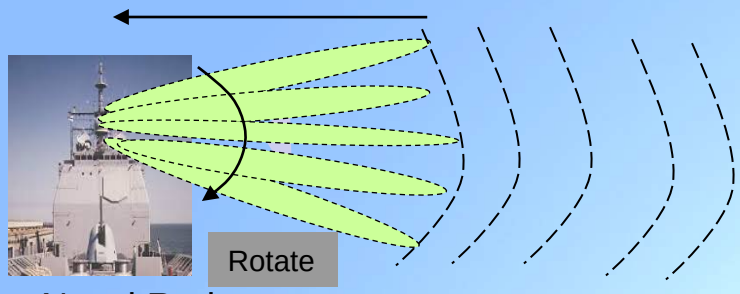
Static Permanent Exclusion Zone Around Primary Systems



Need accurate estimate of exclusion zone and secondary geo-location
- Static propagation model based
- Augmented with dynamic measurements of primary

Sharing Types: In Time

Dynamic Exclusion Zone

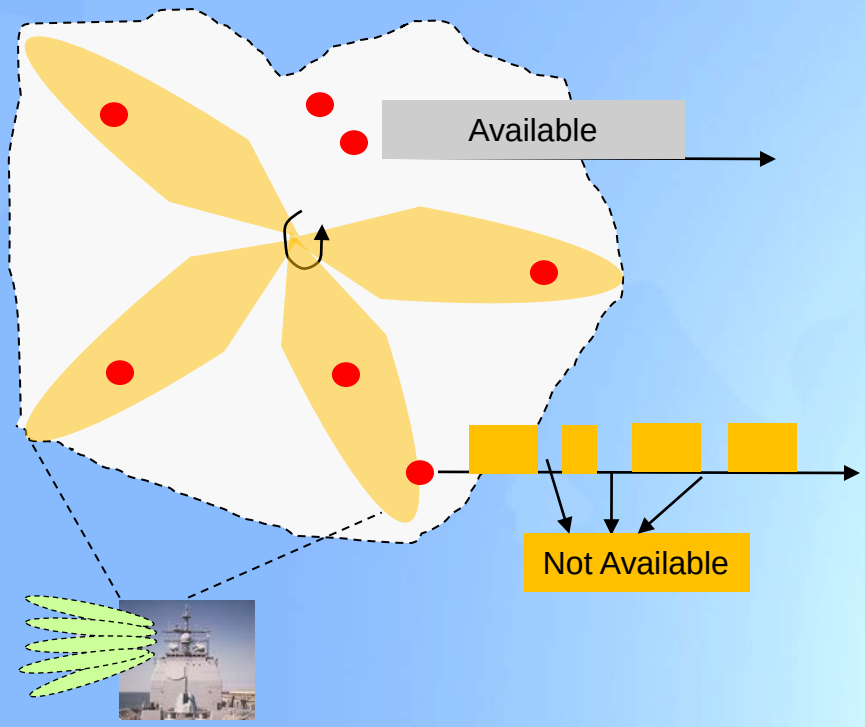


Exclusion zone changes as radar rotates and ship moves

- ***At slow time scale:*** *Via dynamically assigned "time windows" for use in the same space, creating dynamic exclusions zone around primary*
  - E.g.: (1) TV stations with well defined transmission times
    (2) Exclusion zone around Naval Radar moves as radar platform moves

- **Need**
  - Accurate estimate of changes in exclusion zones
  - Close loop information flow between primary and secondary systems to convey when exclusion zones are in effect

Sharing Types: Aggressive Sharing in Space and Time



- ***At fast time scale:*** *Via Media Access Control (MAC) protocol*
  - Secondary systems operate within exclusion zone and transmit when they find "opportunities"
- **Need:** "Listen-before-talk" secondary systems with smart sensing
  - Cognitive functionality

FCC Implementations of Sharing

Different Approaches to Enable Sharing

- *Dynamic Frequency Sensing and Switching (DFS) e.g. used in 5GHz*
- *Spectrum Coordination through Static Exclusion Zones, e.g. planned for AWS*
- *Database approach to spectrum management*
  - *Static/Passive Spectrum Coordination in TV White Space*
    - *Database simply providing list of available spectrum*
    - *Usage follows unlicensed type access*
    - *Static rules for max power levels/masks*
  - *Dynamic Spectrum Access System (SAS) pilots in 3.5GHz*
    - *A granular (time, location. Frequency, and dynamic approach to spectrum management*
    - *Database (re)assigns specific channels and sets max power levels based on deployment*
    - *Supports three tiers of access including priority/licensed access and general authorized access.*

Enabling Technologies Sub-WG Updates

- Sub-WG will look at technologies that can enable sharing
- First call took place on May 22nd
- Had an excellent presentation from Frank Sanders of NTIA (ITS) on radars
  - NTIA performed tests of interference to LTE from radars
  - Report with test results will be released
- Planned activities on interference cancellation technology
  - Interference cancellation at an LTE receiver
  - Potential interference cancellation of LTE signals at an incumbent receiver
- Planned activities on indoor-only services
  - Identifications of potential bands to consider and incumbent system types
  - Propagation profile over a range of frequencies for various building materials

Database Structure Sub-WG Updates

- Subgroups met once on June 5th
- Charter of Sub-WG:
- “Develop requirements for the architecture and interfaces of an advanced Spectrum Sharing database, and investigate options for improving the efficiency and capability of database operation by increased coordination with licensee’s systems.”
- Focus of the study areas is explicitly beyond the effort on the SAS being defined and developed in the ongoing 3.5 GHz docket (12-354)

Database Structure Sub-WG Updates

- There are several candidate areas of study:
  - Core Architecture and Database processes
    - Multi-Tier Access in Spectrum Sharing
      - DB/SAS value add to provide multiple levels of interference protection/Quality of Spectrum (QoS)!
      - Coexistence of high tier and low tier when higher priority user is not active
    - Practical granularity to leverage from separation in time, frequency and location
    - Interference Modeling/Prediction
      - Propagation analysis to optimize license area boundaries
      - Indoor vs outdoor distinctions
    - Examination of what data is useful to make available to potential users to guide assignment (e.g. Likely interference profiles from incumbents and/or protected users)

Database Structure Sub-WG Updates

- There are several candidate areas or study:
  - Optimizations to drive additional efficiency and degrees of sharing
    - Additional degrees of coordination to improve efficiency
      - Timing standard to enable TDD synchronization between users
      - Power level adjustments to avoid mutual exclusivity
    - Opportunities for user data to help the database provide better resource management
      - User devices can report back to the database about what they are hearing and how they are acting
    - Survey of existing features in LTE and WiFi which may be useful to feed data back to the database to improve situational awareness of spectrum use
      - Intersystem Interference Measurement can help improve models for propagation and interference prediction
    - Cognitive DB/Usage Learning to identify opportunities for additional sharing
  - Mechanisms to enhance enforcement and compliance
    - Using interference measurements to detect devices operating outside defined rules
    - Technologies to aid in restricting devices to compliant modes of operation

RF Model City

- WG has reviewed the PCAST report and discuss the earlier concept of the proposed RF Model/Test City
- WG understands that the FCC/NTIA are planning to announce how to advance the PCAST recommendations on the RF Model City
- WG will engage in various discussions and provide its contributions once the further details are announced

Next Steps

- September TAC Meeting
  - Further analysis/investigation
  - Updates from sub-groups
  - Identify sharing opportunities specific to bands identified by working group

- December TAC Meeting
  - Refine the recommendations on sharing opportunities, including specific bands with suggested enabling technology and database application
  - Provide recommendations on the RF Model City per FCC/NTIA announcement

Cybersecurity Working Group

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

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
  - Mike McNamara TWTelecom
  - Lynn Merrill, Monte R. Lee
  - Vish Nandlall, Ericsson
  - 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

Our progress since the March 10th meeting

- We moved forward on the direction provided by our FCC liaisons, Jeffery Goldthorp and Lauren Kravetz
- Initial focus was around 1) **security metrics** and 2) **insider threats**, with reports due by the end of July
  - The 1st topic has evolved away from reporting on metrics, and toward **cyber security process and function**, with Renato Delatorre leading this topic
  - We continue to move forward with topic #2, **insider threats**, with Mike McNamara leading this sub-group
  - Adam Drobot is driving a forward leaning effort assessing the current industry landscape around **insider threat mitigation technologies**
  - These topic areas will be delivered by the **end of July**

Process and Function progress

- Group Members:
  - Lead: Renato Delatorre - Verizon Wireless
  - Ramani Pandurangan – XO Communications
  - Scott Shepard – Motorola Solutions
  - Martin Dolly – AT&T
  - Rao Vasireddy – Alcatel Lucent
  - George Popovich – Motorola Solutions

Process and Function progress (cont.)

- Team met and discussed the things out there that can be used to "think like the board"
- Focus on what processes and functions should be considered as part of a cyber security program
  - Security Risk Management
  - Vulnerability Management
  - Identity and Access Management
  - Security Monitoring and Response
- Working on developing recommendations from the group

Insider threat sub-team progress

- Established Sub Group focusing on Insider Threat Risk Reduction
  - Leader: Harold Teets
  - Members: Brian Daly, Martin Dolly, Mike McNamara, George Popovich
- Developed best-practice documentation/playbook for Instant Response process execution & mitigation against the Insider Threat
  - Defined “Insider” as Disgruntled, Former, Compromised/Coerced Employees, Paid Informants, Business Associates , Consultants/Contractors, Supply Chain & BYOD
  - Identifying the Insider “motivation” and removing this, where possible, helps to proactively reduce the possibility of the Threat
  - Modeled the playbook after NIST CyberSecurity Framework to highlight actions in each area of : Identify, Protect, Detect, Respond, and Recover

Insider threat sub-team progress (cont.)

- Discussions with Industry experts / volunteers from TAC-based companies on how industry exposure is growing at a rapid pace
  - Focus of foreign countries has shifted from looking to compromise the US Gov't to the penetration of Corporate America
  - Need to be responsible for not only the corporation but also the supply chain
  - Tools used to observe "PRIs – Potential Risk Indicators" of employees/insiders at an individual level and not a group level – proactive communication & daily monitoring of activity essential
- Issues to Address
  - Can the FCC help with Information Sharing across the industry during real-time events?
  - How can smaller enterprises that cannot afford specific tools still be informed / protected?
- Next Steps
  - Additional industry-expert discussions to gather best-practices / technology benefits
  - Formalization of white paper or presentation to the FCC by 7/31 with recommendations on tools & best practices

State of Insider Threat Mitigation

- "The Insider Threat" is a mature area of cyber security but grappling with:
  - Well publicized incidents with significant implications for regulations and policy
  - Growth in the nations dependence on cyber infrastructure and evolution of ICT deployment architectures (Cloud, Mobility, Internet of Things, BYOD, …..)
  - Explosion of new attack vectors that have long term impact on both government and commercial enterprises (Proliferation of Apps, Open Source, Outsourcing, …..)
  - Many new mitigation technologies and practices – many of which still need vetting!
- Key Technology areas
  - User authentication (Multi-component data fusion to provide user, location, positive id, and level of access)
  - Information protection (End-end encryption at rest and in motion, access control, watermarking, ….)
  - Anomaly detection (Big data, fusion/mash-up of structured and unstructured data, pattern and behavioral analysis, ……)
  - Physical access protection (Compartmented execution and storage, tamper proof devices, keyed connectivity, video analytics, ….)
  - Resource Access Management (White lists, analysis on connection, software scanning, …..)

State of Insider Threat Mitigation (cont.)

- Research Federal
  - Incidence Response and Best Practices US-CERT
  - Major Responsibilities – ODNI, DHS, and NIST
    - Ongoing activities in almost all US Departments and Agencies
  - Research Activities coordinated by NITRD
    - Involve major research funding agencies, NSF, DoE, DARPA, IARPA, ….
- NFP Organizations and Academic Centers
  - Identified over 20 Organizations and 20 Academic centers focusing on the "Insider Threat " space
  - Found over 30 Start-ups working on advanced technologies and methods mostly in Big Data and Analytics.
- Commercial Offerings
  - Almost all ICT majors have an offering in this space (Accenture, Cisco, HP, IBM, Intel, Microsoft, Oracle, …)
  - Major Federal Contractors (CSC, Mantech, Lockheed Martin, Boeing, Raytheon, …….)
  - And hundreds of smaller players
- A very crowded field!

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

State of Insider Threat Mitigation Work Plan

- Re-examine technical approaches to insider threat – mitigation, response, and recovery
- Look at specific technology areas
  - Resilient Architectures for Cyber Defense
  - Trusted Computing
  - Access Control
  - Big Data and Analytics for risk and anomaly detection
  - Social Network Analysis
  - Formal Methods
- Examine implications and challenges for critical infrastructure
- Engage with academic, commercial and government experts and ongoing initiatives

Moving forward: Feedback from Admiral Simpson

- The Admiral recommended the following topics for consideration
  - Advancing collective knowledge around graceful degradation of systems
  - Convening function across the security ecosystem
  - Application of big data to improve threat response
- We investigated the government/industry landscape to better understand how to incorporate the Admiral's feedback
  - We found comparable and advanced activity among other agencies
  - We have been making those connections with the FCC and other agencies
- Looking forward, we must keep our key objectives in mind
  - Propose technology focused recommendations to incentivize industry to reduce vulnerabilities during the product development process
  - Example 1: How software and hardware are designed/developed to reduce the # of security patches
  - Example 2: New or modified procedures highlighting and addressing software and hardware security concerns in the design and development process

Proposed direction for the 2nd half of 2014

- We recommend a forward leaning focus on technical aspects of cyber security that are of interest to the FCC
  - We have very strong technical representation in our Working Group: leveraging this strength will bring about the greatest value to the FCC
  - This direction was reinforced by our discussions with Admiral Simpson
- Technical topic candidates *(we would select a subset from this list)*
  - Use of big data and analytics to identify risks, vulnerabilities, and anomalies
  - Re-examination of technical approaches to insider threats - mitigation, response, and recovery
  - Resilient Architectures for Cyber Defense, including operation in a degraded network
  - Distributed Denial of Service (DDoS) mitigation techniques
  - Access control, including user authentication trends and moving beyond passwords
  - Trusted computing
  - Social Network Analysis
  - Formal methods
  - An analysis of implications and challenges for critical infrastructure
  - Investigation of other government/industry/academic initiatives with relevance to these topics

Technological Advisory Council

Supporting the Transition to IP

Working Group

10 June 2014

Working Group Members

- Mark Bregman and Tom McGarry (Neustar)
- Theresa Hennesy (Comcast)
- Kevin Kahn (Intel)
- Fred Kemmerer and John Barnhill (Genband)
- Steve Lanning (Viasat)
- Jack Nasielski (Qualcomm)
- Marvin Sirbu (SGE)
- Doug Jones (VZ)
- Russ Gyurek (Cisco)
- Dale Hatfield (UCol)
- Harold Teets and Mike McNamara (TW Telecom)
- Lynn Merrill (NTCA & Monte R. Lee)
- Peter Bloom (General Atlantic)
- Vish Nindlall (Ericsson)
- Dick Green (Liberty)
- Nomi Bergman, John Dickinson (Bright House)

Special thanks to the FCC members: Walter Johnston, Henning Schulzrinne, Kalpak Gude and William Layton for their contributions.

Today's Discussion

- Review our original mission
- Update on work effort to date
- Share our reference architecture plan
- Receive feedback from the rest of the TAC

2014 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

Rural Operator Findings

Interviewed several rural companies about broadband deployment.
Companies serve population within one mile of town and serve Midwest farmland, moderate rock western plains, and mountainous regions with construction costs that range between $15K and $85K per mile
Interviewed companies: Hamilton; Panhandle and Silverstar.

Common Themes:

- Service Provider in tune with the community
- If community fails, so does the company.
- Employees live in communities they serve: see and hear from the customers and react quickly
- There were sufficient last mile access solutions, once a middle mile solution is in place
- Aggressively adopted new and hybrid solutions which solved geographical challenges and fit investment profiles.

Rural Operator Findings: Last mile access

- These companies innovate by embracing diverse technologies available to provide broadband service, including video/IPTV
- Interviewees started with DSL. Two of them then added HFC.
- Majority of their networks are Fiber-to-the-node, the node being a transition point to copper or coax
- Deployment of FTTH in new build situations
- These operators have extended copper life by reaching customers with higher speeds near town with VDSL
- Creative deployment of wireless solutions (LTE or WiMAX)
- Some areas unreachable with terrestrial wireless due to terrain. Some distances too far and required multiple repeaters to reach down canyons

Rural Operator Findings: Construction methods

- Use existing facilities as long as possible to support fastest broadband services; move to newer technology as ROI allows.
- Survey requirements for construction along state HWY vary greatly by state
- Some states require multi duct placement along R/W to resell at future date
- Environmental review process protracted and expensive
- Plan new subdivision builds with other utilities to share costs
- Place conduit with water and gas
- All employees spot and act on opportunities to share construction costs with utilities and roads.

Rural Operator Findings: Broadband Speeds

- Serve towns with broadband speeds above 10 Mbps
- In low cost construction areas: serve all customers with broadband speeds above 10 Mbps
- High cost construction areas:
  - Serve as many customers possible outside town with broadband speeds over 10 Mbps based on ROI.
  - Serve remaining customers with ADSL or Wireless services. 4Mbps/1Mbps, but below 10 Mbps (downstream).

Rural Operator Findings: Voice Services

- Companies have varying stages of VoIP in network but not complete through all architecture segments
- Access to a soft switch seems to be a key turning point for fully deploying VoIP. For them, the transition point has not yet arrived:
  - Companies without soft switches are reviewing options for purchase or leasing services from hosted parties.
  - Companies with soft switches are hosting services for others.
  - Interestingly, two companies host third party soft switches. Yet they have not yet transitioned their own legacy circuit switched voice customers.

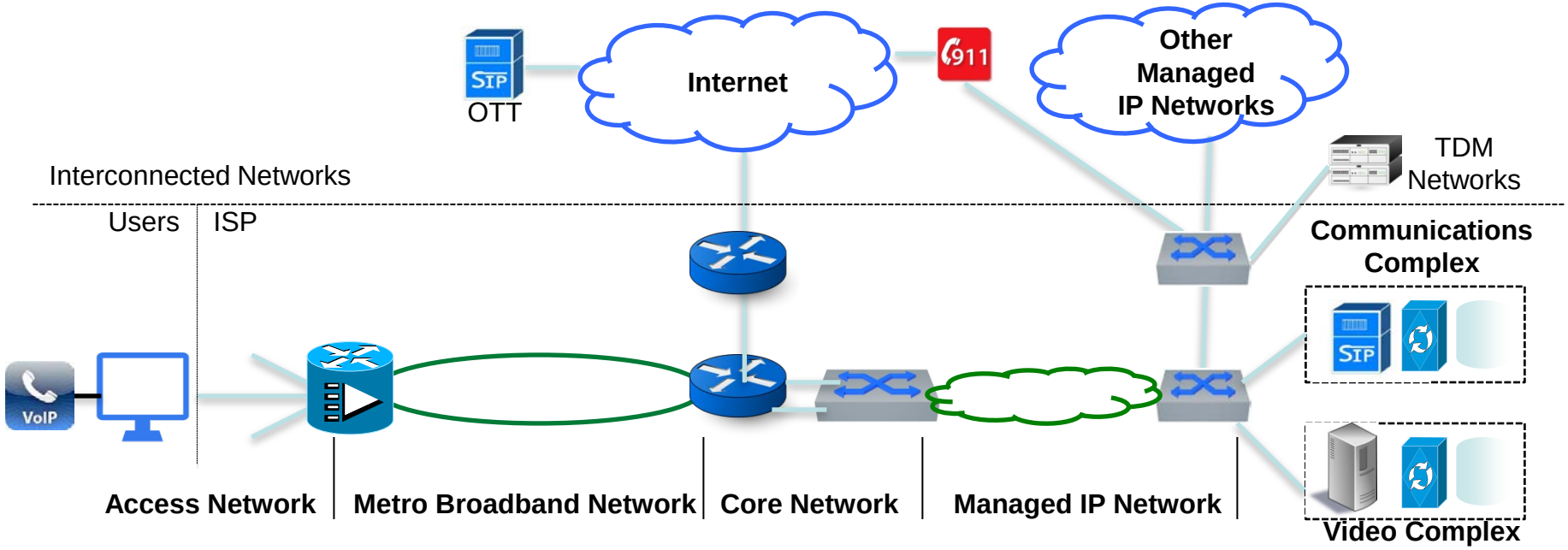
Rural Operator Findings: Middle Mile, or Backhaul to Internet

- Installed larger fiber networks or joined a consortium to form statewide networks to reduce cost
- Built redundant connection points over several years, as investments in their 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 therefore price. These companies have adopted regional interconnect solutions, where they offer regional hosting and transit service to mitigate high middle-mile transition costs.

Reference Architecture Plan

- Develop a reference architecture to frame how we see the broadband network, and its access and backbone technology solutions, evolving.
- Our specific mission: To develop a reference architecture for the broadband network that provides users access to Internet and communication services. The reference architecture will include the possibility that the user's ISP also provides communication and video services. It will also show the ISP's interconnection to other networks for the purposes of providing Internet, communications and video services.
- We hope to use this framework to share a technical view as to how solutions are evolving, how this brings the customer forward, and to examine impacts to advanced communications capabilities
- Marvin Sirbu is leading the access piece, and Tom McGarry the backbone piece.

Reference Architecture



Reference Architecture

- The reference architecture provides a high-level view of the ISP network that provides broadband and other services to users
- It divides the ISP network into six components;
  1) access network,
  2) metro broadband network,
  3) core network,
  4) managed IP network,
  5) communications complex, and
  6) video complex
- It includes connections to other networks; 1) the Internet via the core network; and 2) TDM networks, 3) 911 service, and 4) other managed IP networks via the managed IP network
- The reference architecture will provide further detail on all of these components

Next Steps for TAC 2014 Work

- Between now and September, working sessions to create a draft of a high level reference architecture for early review at our 9/23 meeting. Refine and publish for the December meeting.
- Continued surveys (access vendors, HFC service providers, service providers of larger size) and comparison of results to other broadband survey findings.
- Industry is moving forward with trials, as directed by the Commission. The TAC continues to identify additional technical areas for consideration, and is seeking input from industry advocates in those areas.
- Continued work to review and consider “corner cases” in aggregate

THANK YOU