IETF Report

CATHY ARONSON
ARIN 40, SAN JOSE, CA.

About This Presentation

This presentation is an official IETF report

- I am officially the ARIN IETF Reporter for 2017
- This is all my opinion and my view and I am not covering everything just highlights
- You should know I like funny quotes
- I hope you enjoy it
- Your feedback is greatly appreciated
- If you were there and I missed something interesting please share!
- Opinions expressed are solely my own and I include thoughts that I typed while at the meeting.

Highlights

Highlights

- The Internet as we know it is changing – QUIC
  - "The QUIC WG will provide a standards-track specification for a UDP-based, stream-multiplexing, encrypted transport protocol."
    - BoF in July 2016
    - Already 5 implementations
- The "problem" with TLS (later)
- ANRP Presentations (later)
- RFC Format (later)

Advanced Networking Research Workshop (ANRW)

- A lot of research gets done because of RIPE Atlas.
- Measurement Vantage Point Selection Using A Similarity Metric.
  - Looks at how similar are the RIPE Atlas vantage points
  - How to choose probes to get the best info. Pairwise similarities are here http://sg-pub.ripe.net/emile/probe-similarity/

ANRW

- Characterizing User-to-User Connectivity with RIPE Atlas
  - Estimation of RIPE Atlas coverage in eyeball networks, as well as an approach to measure and visualize user interconnectivity with our Eyeball Jedi tool.
  - Does traffic from one network to another stay within a country?
- CheesePi: Research, Results, and the Regulator
  - CheesePi is a lightweight platform written in Python with the goal of performing multimedia measurements from within users' homes.
- copycat: Testing Differential Treatment of New Transport Protocols in the Wild
  - proof-of-concept case study (UDP vs. TCP) in order to answer questions about the deployability of current transport evolution approaches, and demonstrate the extent of copycat's capabilities and possible applications.
- Implementing IPv6 Segment Routing in the Linux Kernel.
  - There is now a Linux implementation of Segment Routing (SR).
  - Uses the Segment Routing Header (SRH) defined in IPv6

ANRW

- Panel: Internet Health Metrics
  - Interesting discussion about measurement of network from ISP perspective.
  - "Opportunities for optimization"
  - For example trying to measure the before and after of IPv4 and IPv6. Is one better than the other? What happens when v4 starts to degrade?
  - Early examples from JJB – v4 server is close and v6 server (for v6 launch event) is far away. Not broken but not optimal either.

ANRW

- Other papers
  - Tracking transport-layer evolution with PATHspider.
  - Take your own share of the PIE.
  - PPV - Per Packet Value - resource shaping framework marking and measuring classes of flows
  - A NEAT Way to Browse the Web
  - Manage resource-constrained IoT devices through dynamically generated and deployed YANG models.
  - No domain left behind: is Let’s Encrypt democratizing encryption?

IEPG – What is it?

- The IEPG is an informal gathering that meets on the Sunday prior to IETF meetings. The intended theme of these meetings is essentially one of operational relevance in some form or fashion - although the chair will readily admit that he will run with an agenda of whatever is on offer at the time!
- The IEPG has a web page and a mailing list
  - iepg@iepg.org - the usual subscription protocols apply.

IEPG

- Exploring blinded network data for fun and profit - George Michaelson
  - HTTPS everywhere is now a thing
  - Who is left behind?
    - It's not a lot of folks but they exist. Real users who risk being excluded from secure communications.
    - Working to characterize the info. Paper and data are on Arxiv
    - ASN is the strongest predictor of failure – linked to economy.

IEPG

- Fully Automatic DNSSEC
  - Uses RFC7344 – Automating DNSSEC
  - RFC8078 Managing DS records from the parent via CDS/CDNSKEY
  - Implementations
    - FRED, Knot DNS2.5, BIND 9.11, PowerDNS, OpenDNSSEC
  - 1296512 domains
    - 667 815 domains signed by DNSSEC with published DS record
    - 21 156 domains signed by DNSSEC without published DS record. DS = Delegation of Signing

IEPG

- BGP More Specifics
  - 3 kinds
    - Provider aggregatable – Hole punching
    - Traffic engineering
    - More specific overlays
  - 53% are more specifics
    - Not new addresses but more fragmenting of existing space
  - 1% of prefixes generate 40% of updates in v4
  - V6 has 100 times the instability events

IEPG

- Root Canary
  - Timely because we see that ICANN has delayed this rollover
  - Measuring and monitoring the impact of the KSK rollover
  - Monitoring gives immediate insight into which operators have problems
  - Notify operators so they can take action.
  - This is the first time the root KSK is rolled so it will provide insight into issues.
  - 4 Online Perspectives
    - RIPE Atlas
    - Luminati
    - APNIC DNSSEC measurement
  - https://rootcanary.org
  - New key on July 11th has not led to noticeable problems with resolvers.
  - Most RIPE Atlas probes are behind stable validating resolvers
  - Support for ECDSA P-256 and P-384 are at almost the same level as RSA-SHA256

IEPG

- Recursives in the Wild: Engineering Authoritative DNS Servers
  - Analyze how recursives behave in the wild with the goal to better engineer authoritative servers.
  - Recommendation: Use Anycast on all your NS, and peer very well, with multiple sites
  - https://tinyurl.com/y7exc5ts

IRTF – What is it?

- The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organization, the Internet Engineering Task Force (IETF), focuses on the shorter term issues of engineering and standards making.
- The IRTF is a composed of a number of focused and long-term Research Groups. These groups work on topics related to Internet protocols, applications, architecture and technology. Research Groups have the stable long term membership needed to promote the development of research collaboration and teamwork in exploring research issues. Participation is by individual contributors, rather than by representatives of organizations.

IRTF

- A Multi-perspective Analysis of Carrier-Grade NAT Deployment
  - Seems like it would be a yawn but wow good info.
  - 38% of ISPs say they plan to deploy CGN
  - Interesting techniques to find who is using CGN. One of the techniques uses bit torrent.
    - looks for bit torrent peers and then gets address/port numbers, graph the leakage and then use that to see CGNs.
  - Another technique is using a netalyzer from inside.
  - Deployment stats
    - Non-cellular 17%
    - Cellular 94%
  - Found what I talked about before .. Blocks like 25/8 being used as RFC1918 space

IRTF

- A Systematic Analysis of the Juniper Dual EC Incident
  - This was by far the most interesting part of IETF this time.
  - Paper here http://dualec.org/DualECJuniper-draft.pdf
  - Two security issues produced two backdoors.
  - It was a calamity of errors.
  - The fun thing is that IKEv2 nonce size made it less secure.. Anyway it is totally worth the read.

IPv6 Maintenance (6MAN) - ?

- The 6man working group is responsible for the maintenance, upkeep, and advancement of the IPv6 protocol specifications and addressing architecture. It is not chartered to develop major changes or additions to the IPv6 specifications. The working group will address protocol limitations/issues discovered during deployment and operation. It will also serve as a venue for discussing the proper location for working on IPv6-related issues within the IETF.

6Man

- Drum roll please …
  - IPv6 specification is now Internet standard!!! RFC8200
- Update on IPv6 Addressing Architecture
  - no actual need for restriction of /64 for address ids.
  - Never ending argument about what prefixes should be.
  - I have never understood why we have to specify some prefix length.

6Man

- Still working on IPv6 Node Requirements
- Other drafts being worked
  - Route Information Options in Redirect Messages, draft-templin-6man-rio-redirect
    - How to send traffic direct without the router (sort of like proxy ARP)
  - IPv6 Address Usage Recommendations
  - Tweaking Default Address Selection
    - How to solve multihoming
  - Proposals to discover Provisioning Domains
    - Again how to pick your source address
  - The AERO Address
    - Delegated prefixes are imbedded in the link local address.

HOMENET – What is it?

- The purpose of this working group is to focus on this evolution, in particular as it addresses the introduction of IPv6, by developing an architecture addressing this full scope of requirements:
  - prefix configuration for routers
  - managing routing
  - name resolution
  - service discovery
  - network security
- charter-ietf-homenet-03

HOMENET

- Deploying HNCP
  - Ted deployed HNCP and had lots of problems. It ruffled some folks who thought he should have maybe tried harder
    - “the amount of work you need to do to understand how to debug the network is too much”
    - Response “we have 19 year olds who can install this protocol.. “

HOMENET

- draft-ietf-homenet-babel-profile-02
  - The world's biggest fan of BABEL speaks
  - Discussion of interactions between HNCP and BABEL
- Other drafts being worked
  - draft-tldm-simple-homenet-naming-00
    - Continuing saga of home.arpa
  - draft-boutier-babel-source-specific
    - New format for source specific routing
  - draft-tldm-simple-homenet-naming-02
  - draft-ietf-homenet-dot-09 – WGLC
  - draft-ietf-homenet-redact-03 – AD Eval

SIDR Operations – What is it?

- The global deployment of SIDR, consisting of RPKI, Origin Validation of BGP announcements, and BGPSEC, is underway, creating an Internet Routing System consisting of SIDR-aware and non-SIDR-aware networks. This deployment must be properly handled to avoid the division of the Internet into separate networks. Sidrops is responsible for encouraging deployment of theSIDR technologies while ensuring as secure of a global routing system, as possible, during the transition.

The SIDR Operations Working Group (sidrops) develops guidelines for the operation of SIDR-aware networks, and provides operational guidance on how to deploy and operate SIDR technologies in existing and new networks.

SIDR Operations

- Analysis of easy deployment validator
  - 10% wrong ROAs
  - Almost no one enforces Route Origin Validation (ROV) so the wrong ROAs don't have consequences
  - "Smart Validator" - ROAlert.org - this is cool because bad ROAs make ROV not possible. Tells you if ROAs are valid
- draft-paillisse-sidrops-blockchain-00.txt
  - "I know that block chain is all hip and sexy but I fail to see what problem you're trying to solve"

SIDR Operations

- Other drafts
  - Update on Tree-validation
    - There is a RIPE tree validator RPKI Validator.
  - HTTPS in TAL URIs
  - Signed TAL to communicate URI changes
  - draft-ymbk-sidrops-ov-clarify-00.txt
  - draft-madi-sidrops-rp-00.txt
  - Update on BGPsec reference implementation and BGPSEC-IO, a BGPsec testing engine

V6 Operations – What is it?

- The IPv6 Operations Working Group (v6ops) develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides operational guidance on how to deploy IPv6 into existing IPv4-only networks, as well as into new network installations.
- The main focus of the v6ops WG is to look at the immediate deployment issues; more advanced stages of deployment and transition are a lower priority.
- http://datatracker.ietf.org/wg/v6ops/

V6 Operations

- Turning IPv4 off in an Enterprise network Microsoft
  - 775 locations, 1.2m devices Why v6?
    - Out of RFC1918
    - Acquisitions and overlapping rfc1918 as well as interoperating and the fragility of NAT solutions.
    - Operational complexity of dual stack
    - Support of dual stack in firewalls, helpdesk, NOC, etc
- More about this here: https://blog.apnic.net/2017/07/21/ietf99-prague-microsoft-enterprise-looks-barrel-v6-gun/

V6 Operations

- IPv6 deployment status
  - 9 million domain names and 23% of all networks are advertising v6
  - Google reports 37 countries exceeding 5% of traffic. Akamai reports 7 countries whose IPv6 traffic exceeds 15%. In Japan, all three major mobile networks, NTT, KDDI, and Softbank, are deploying IPv6 this year, and in India, Reliance JIO’s deployment has driven measures of IPv6 traffic in the country to exceed 20%. The IPv4 Market Group comments that it expects IPv6 user count to exceed 50% world-wide in 2019, and with that, the start of the decline of the IPv4 address market.
  - More info here https://www.internetsociety.org/doc/state-ipv6-deployment-2017

V6 Operations

- A Longitudinal View of Dual-stacked Websites: Failures, Latency and Happy Eyeballs
  - Has probes measuring v6
  - Looks at v6 performance and deployment
  - Detailed look at performance
  - Alexa top 100 websites with AAAA entries
    - 27% show some rate of failure over IPv6
    - 9% exhibit more than 50% failures over IPv6
  - More info here https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-a-longitudinal-view-of-dual-stacked-websites-failures-latency-and-happy-eyeballs

V6 Operations

- Happy Eyeballs Version 2: Better Connectivity Using Concurrency
  - If you get the AAAA response before the A response why not just start doing v6?
- Incremental Deployment of IPv6-only Wi-Fi for IETF meetings
  - This is actually controversial. Why not have a v6 network with a v4 gateway for IETF? Some folks complained that they have to get work done.

V6 Operations

- IPv6 just works right?
  - – If you buy a box from <insert computer store name here> and you bring it home the IPv4 just works.
  - – The assertion is that this needs to be the case for v6.

V6 Operations

- Using Conditional Router Advertisements for Enterprise Multi-homing
  - Source routing outbound. Need to be able to change the host address based on network changes, interface state, etc
  - This is a change to the host and may be hard to implement
- Considerations For Using Unique Local Addresses
  - IETF doesn’t recommend it
  - We debate a lot at IETF about using these
- Reporting of Happy Eyeballs v2 Failures
  - Requires 192.88.99.0/24
  - To make the syslog happen either use a Network-specific prefix or this /24 for anycast

V6 Operations

- Other drafts
  - Considerations For Using Unique Local Addresses
  - Requirements for a Zero-Configuration IPv6 CPE
  - Using Conditional Router Advertisements for Enterprise Multihoming
  - RFC 7984-bis (Locating Session Initiation Protocol
  - Basic Requirements for IPv6 Customer Edge Routers
  - Transition Requirements for IPv6 Customer Edge Routers
  - Minimum Requirements for IPv6 Only Customer Edge Routers
  - Basic Requirements for IPv6 Customer Edge routers with HNCP
  - Requirements for a Zero-Configuration IPv6 CPE

Ops Area – What is it?

The primary technical areas covered by the Operations & Management (OPS) Area include: Network Management, AAA, and various operational issues facing the Internet such as DNS operations, IPv6 operations, operational security and Routing operations.

Unlike most IETF areas, the Operations & Management area is logically divided into two separate functions: Network Management and Operations.

The Network Management function covers Internet management and AAA, and the related protocols, including but not limited to NETCONF, SNMP, RADIUS, Diameter, and CAPWAP, and of data modeling and data modeling languages used in management such as SMI and YANG. Another important role of the Management function is to identify potential or actual management issues regarding IETF protocols and documents in all areas, and to work with the other areas to resolve those issues.

The Operations function is largely responsible for soliciting operator feedback and input regarding IETF work. Another important role of the Operations function is to identify potential or actual operational issues regarding IETF protocols and documents in all areas, and to work with the other areas to resolve those issues.

The OPS area intersects most often with the Routing, Internet and Security areas.

Ops Area

- How the IETF needs to evolve
  - Semantic Versioning and Structure for IETF Specifications
    - So folks are hating the RFC format and how it makes work difficult. Alternative formats and semantic versioning
    - So YANG models for document revisions?

OPSAWG

- Work being discussed
  - Manufacturer Usage Description Specification
  - Service Models Explained
  - Export BGP community information in IPFIX
  - YANG Data Model for NAT
  - Extending YANG for events, actions, and finite state machine

ISA BoF – what is it?

- Changes to the relationship between ISOC and IETF
- 2nd Option would be new ISOC subsidiary.
- Discussion of changing the org such that there are more staff etc. This may not be good

TLS – What is it?

- The TLS (Transport Layer Security) working group was established in 1996 to standardize a 'transport layer' security protocol. The basis for the work was SSL (Secure Socket Layer) v3.0 [RFC6101]. The TLS working group has completed a series of specifications that describe the TLS protocol v1.0 [RFC2246], v1.1 [RFC4346], and v1.2 [RFC5346] and DTLS (Datagram TLS) v1.0 [RFC4347], v1.2 [RFC6347] as well as extensions to the protocols and ciphersuites.
- The primary purpose of the working group is to develop (D)TLS v1.3.

TLS WG

- Okay so not something I normally attend. It does appear that this is significant and that a lot of enterprises and data center folks are worried that they will no longer be able to debug their networks. They want to be able to decrypt the data stream so that they can solve problems. Of course decrypting by one means potential decryption for the bad guys too

TLS WG

- TLS1.3 is the new version of TLS.
- There is a draft on this new version and it's impact to data center operations
- Data Center use of Static DH
  - why static Diffie-Hellman is important
    - out of band encryption in data centers
    - when a problem hits no one knows where the problem is
    - need to decrypt and then look for user info.
    - without static Diffie-Hellman won't be able to find problems. This is the problem with TLS 1.3. This locks out the troubleshooters.

TLS WG

- National Cybersecurity Center of Excellence (NCCOE) project for visibility within the datacenter with TLS 1.3
  - About deployment of Static DH
  - Mission is about tech transfer and adoption/deployment
  - Take standards and demonstrate how we can manage security and business requirements

Dynamic Host Configuration - ?

- The DHC WG is responsible for defining DHCP protocol extensions. Definitions of new DHCP options that are delivered using standard mechanisms with documented semantics are not considered a protocol extension and thus are outside of scope for the DHC WG. Such options should be defined within their respective WGs and reviewed by DHCP experts in the Internet Area Directorate. However, if such options require protocol extensions or new semantics, the protocol extension work must be done in the DHC WG.
- charter-ietf-dhc-08

DHC

- DHCPv6 deployment at Comcast
  - DHCP primary protocol used to bootstrap devices that are used on cable networks PacketCable, eRouter, etc
  - 99% of 44, 000, 000 cable modems use DHCPv6 and are v6 only
  - eRouters 90% are growing and dual stack extremely stable
  - used for configuring DOCSIS and DSG DHCPv6 options
  - looking at optimizing DHCPv6
- 100 million bindings in DHCP platform
  - every day is a first new record
- Comcast says that v6 has unencumbered them.
  - Plenty of addresses and the ability to use them. No longer bound by re-addressing, re-subnetting, etc.

DHC

- Secure DHCPv6
  - Stalled need to move it forward
- Other work
  - DHCP/DHCPv6 options for LWM2M bootstrapping
  - OnDemand Extensions to DHCPv6 for IP Session Continuity Requests

GAIA – what is it?

- Global Access to the Internet for All
- The Internet Society's Global Internet User Survey 2012 reveals that a large majority of respondents believe that Internet access should be considered a basic human right. However, in the reality of today's Internet, the vision of global access to the Internet faces the challenge of a growing digital divide, i.e., a growing disparity between those with sufficient access to the Internet and those who cannot afford access to the essential services provided by the Internet.

GAIA

- guifi.net
  - community network
  - community clouds as open commons
  - are they feasible and sustainable?
- librem esh
  - Open source DIY router for community networks
- Community networks in Africa
  - Zenzeleni networks
    - Folks here live on < $2.00 / day
    - This network gives them free calls
    - Working together to establish a commons
- Other work
  - Netcommons.au
  - Connectivity in India

Technical Plenary

- IETF has a new website and an new RFC format that no longer requires ascii art.
  - September 14, 2017 RFC Series publishes first RFC with non-ASCII characters - RFC 8187
- More discussion about moving the IETF network forward to IPv6 by default

Human Rights Considerations

- The **Human Rights** Protocol **Considerations** Research Group in the **IRTF** is chartered to research whether standards and protocols can enable, strengthen or threaten **human rights**, as defined in the Universal Declaration of **Human Rights** (UDHR) and the International Covenant on Civil and Political **Rights** (ICCPR), specifically, ...

HRC RG

- Presentation by our own Milton Mueller
  - Requiem for a Dream: on advancing human rights through internet architecture
    - can rights be protected by design or through protocols?
    - connectivity as an enabler of human rights
    - "code is law" (this all happens up front as code is written) or more accurate "technology mediates human rights" (here infrastructure is here and then folks are trying to do things to infringe)
  - "internet press and radio were technologies of freedom not because of their architecture but because the state didn't know how to control them. then they discover new ways to control them.
  - Design happens before the fact and rights violations happen after the fact … ongoing struggle.

HRC RG

- Discussion of draft-tenoever-hrpc-association-01
  - document forms of association and assembly and how the internet architecture enables these
    - Is the Internet itself an association?
    - Forced association? DDOS and ISPs
    - What about the right to be offline?
- draft-tenoever-hrpc-political-00
  - Politics of standards.
  - Are protocols political? Neutral? Inherently political?

HRC RG

- Report back on Hackathon on HTTP status code 451 + HR considerations
  - build tools that crawl and detect censorship online
  - Several apps that do various things to detect or have folks report
  - Want to run it in a number of other countries.
  - https://netblocks.org/dashboard - some results here
  - Maybe anonymize results so that folks don’t stop doing 451 because they’re being monitored

DNS Operations – What is it?

- The DNS Operations Working Group will develop guidelines for the operation of DNS software and services and for the administration of DNS zones. These guidelines will provide technical information relating to the implementation of the DNS protocol by the operators and administrators of DNS zones.
- More at charter-ietf-dnsop-04

DNS Operations

- draft-wkumari-dnsop-extended-error
  - You could have DNSSEC fail and not know why. SO this error code was for that.
- Client ID in Forwarded DNS Queries
  - Carrying client ID info in DNS queries.. This was determined by the group to be the bad idea fairy
- Other drafts
  - draft-edmonds-dnsop-capabilities
  - draft-huque-dnssec-alg-nego

Babel WG – What is it?

- Babel is a loop-avoiding, distance vector routing protocol with good provisions for dynamically computed link metrics. The core of the Babel protocol and security extensions are described in Experimental Independent Stream RFCs 6126, 7557, and 7298.
- The Working Group will focus on moving the Babel protocol to IETF Proposed Standard with IETF review. This includes clarifying RFC 6126 and integrating RFC 7557 and feedback provided by independent implementations, and resolving comments. It is not a requirement that the Babel protocol produced is backwards compatible with RFC 6126. It is a requirement that Babel support at least one profile that is auto-configuring. Other documents that are relevant to the above work can also be produced. Particular emphasis will be placed on work needed for a Proposed Standard routing protocol, such as ensuring manageability and strong security. Link metric measurement or link metric calculation procedures significantly more complex that those currently in Babel are out of scope.

Babel WG

- Drafts being worked
  - Mandatory sub-TLVs in Babel
  - Unicast Hellos
  - Information Model
  - Bit Indexed Explicit Replication (BIER) in Babel
    - I think we need Beer in Babel
  - Source-Specific Routing for Babel

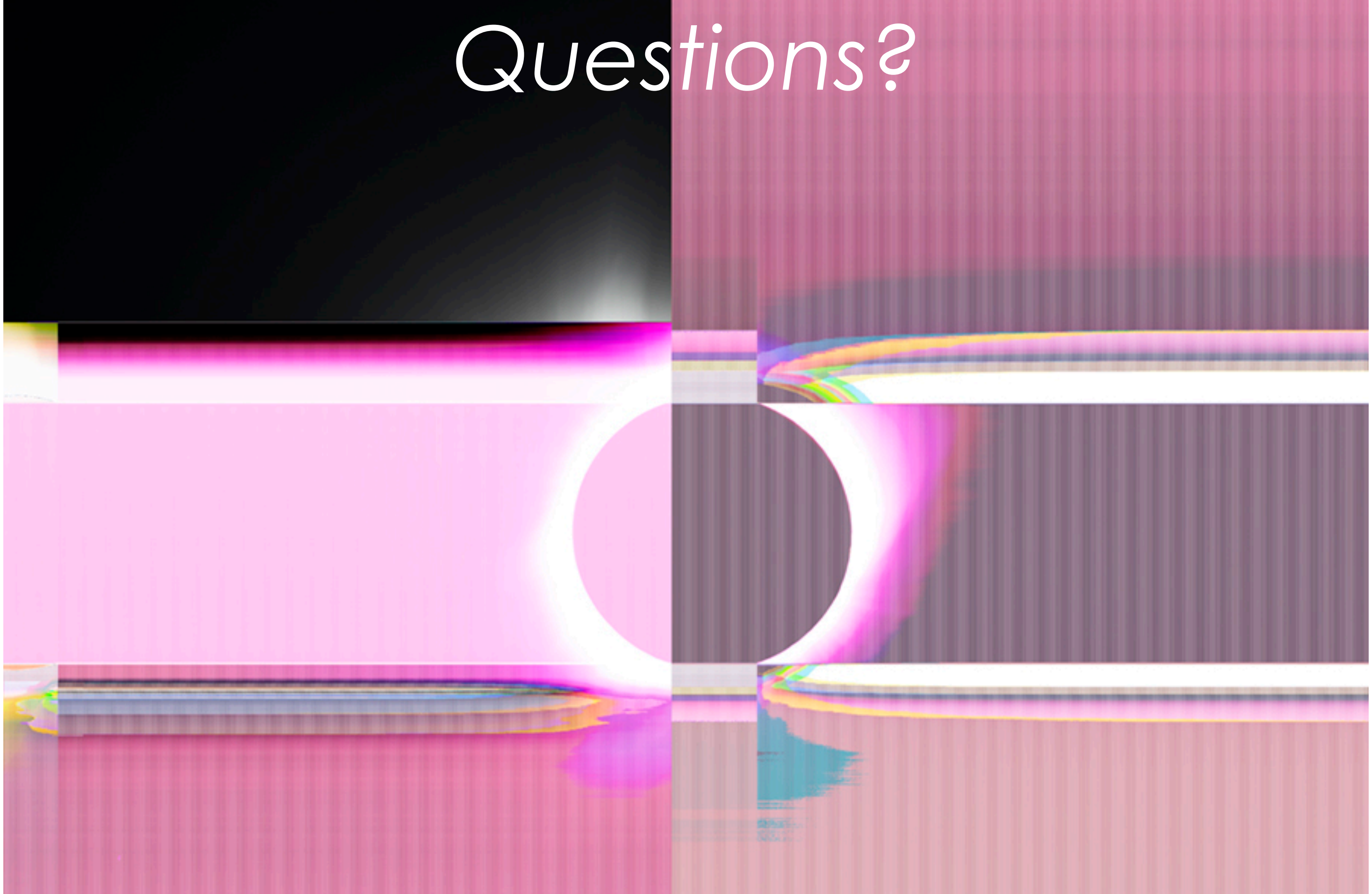
References

- Cool Feed of new documents and what they are
  - http://tools.ietf.org/group/tools/trac/wiki/AtomFeeds
  - It's pretty cool and has info about all new documents, liaisons etc.
- General WG Info:
  - http://datatracker.ietf.org/wg/ (Easiest to use)
- Internet Drafts:
  - http://tools.ietf.org/html
- IETF Daily Dose (quick tool to get an update):
  - http://tools.ietf.org/dailydose/
- Upcoming meeting agenda:
  - http://tools.ietf.org/agenda
- Upcoming BOFs Wiki:
  - http://tools.ietf.org/bof/trac/wiki
- Also IETF drafts now available as ebooks

Going to your first IETF?

- Watch the video
  - https://www.ietf.org/newcomers.html
- Are you a woman attending first IETF?
  - IETF Systers
  - https://www.ietf.org/mailman/listinfo/systers
- Woman involved in NOGs?
  - Net-grrls
  - https://www.facebook.com/groups/netgrrls/
- Men there are lists for you too.. All the meeting lists are mostly men. Have at it ☺

Questions?



Questions?