IETF Report

CATHY ARONSON
ARIN 46 VIRTUAL OCT. 2020

About This Presentation

This presentation is NOT an official IETF report

- **This report covers Virtual IETF 107, and 108, and several interim meetings.**

- **This is not an in-depth IETF report lots of exercise for the reader. Even less in depth this time because of time limit**

- 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.
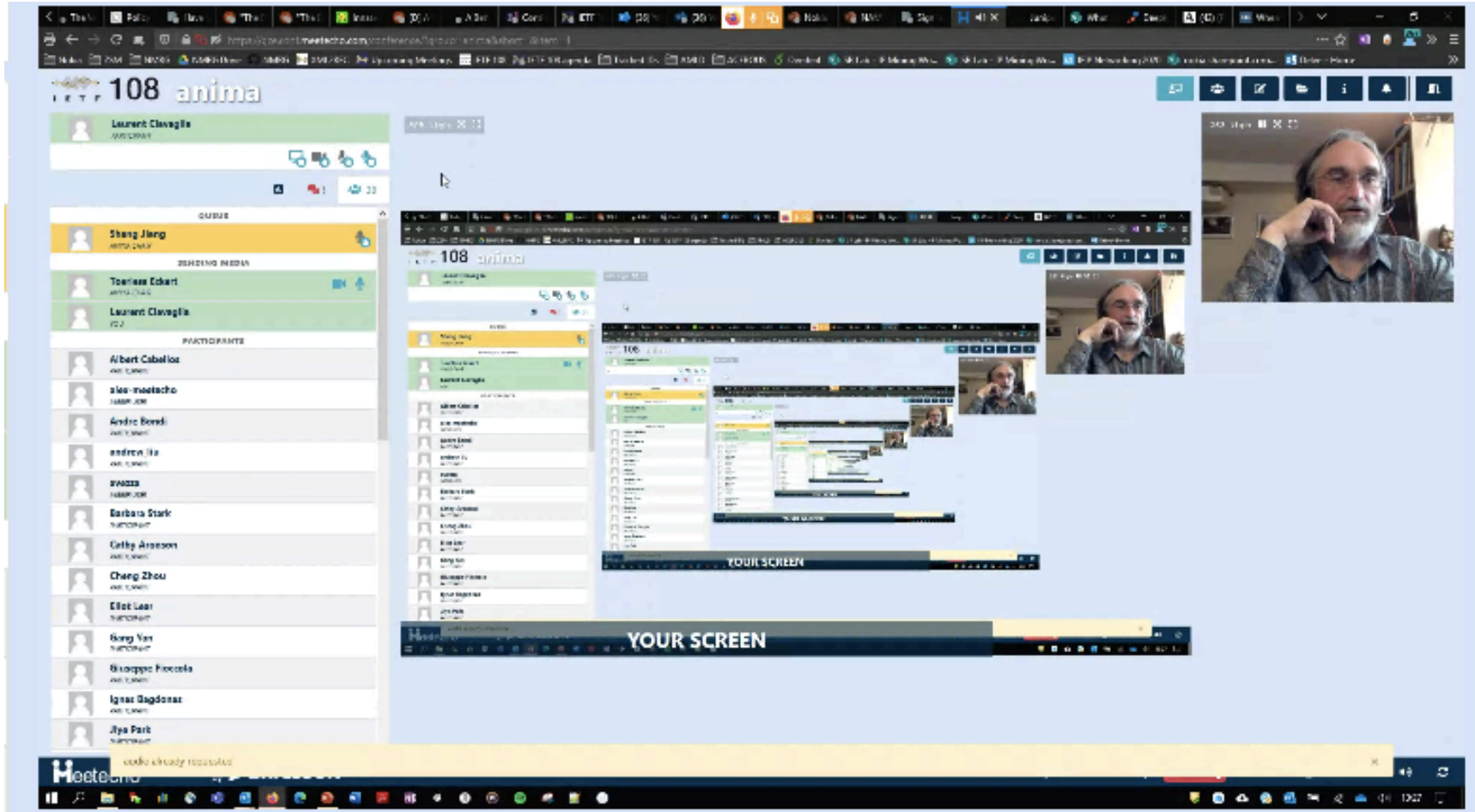
Highlights

- First ever totally virtual IETF was 107.
- That means only a few crazy photos of people, shoes, etc.
- I did take extra photos at IETF 106 and those are mixed in with the other slides
- There is a virtual hum tool.

Is your meeting over yet?
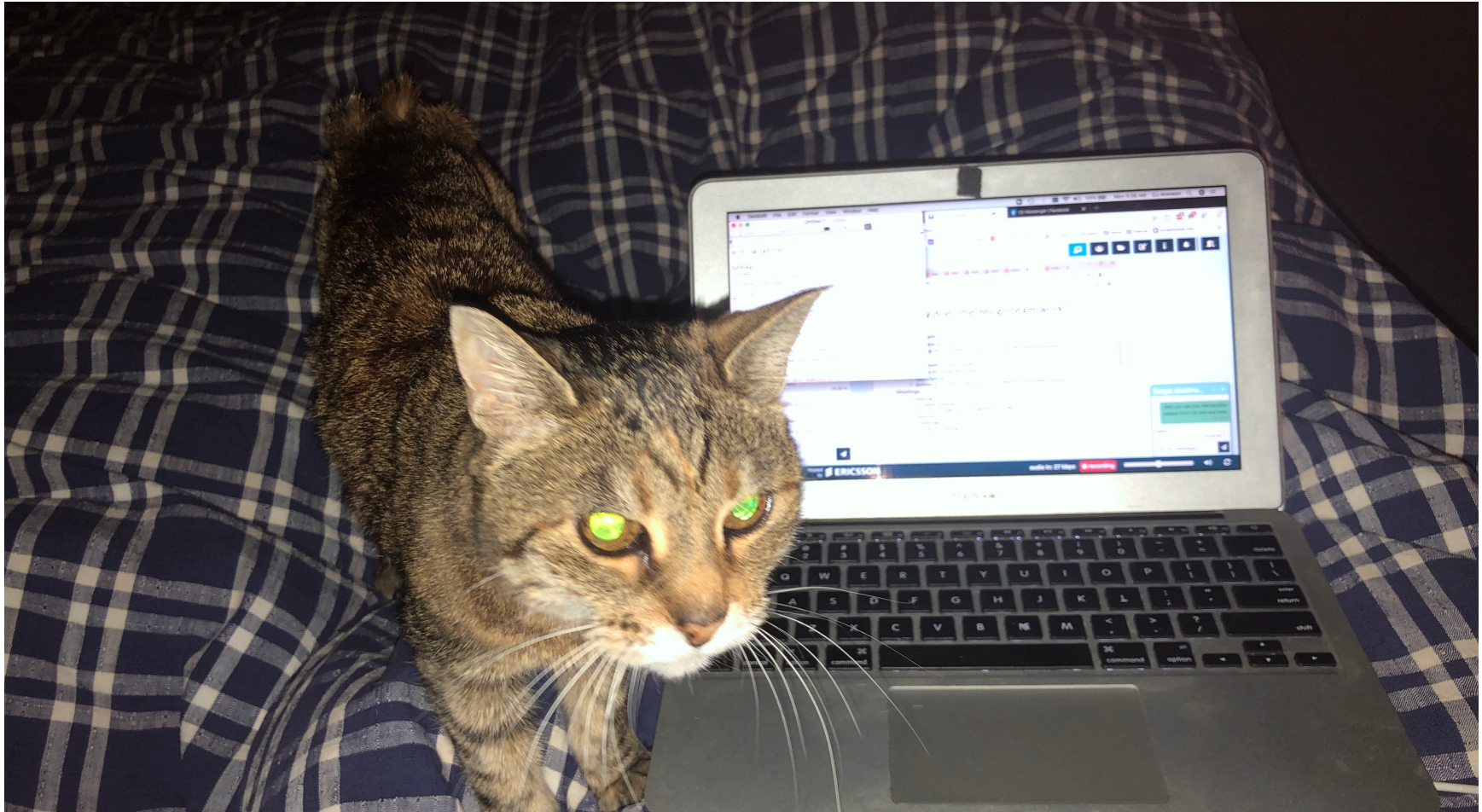
Meetecho

Data on Virtual IETF 107

- Interesting stats about the first virtual IETF
  - 701 unique individuals participated in the virtual sessions over the week
  - Participants from at least 39 distinct countries
  - Between 82 and 235 people participated in each of the working group sessions and 282 at the plenary.
  - Several sessions (I think all of them) had more participation than would have happened in person.
  - IETF 108 had 1372 attendees from 56 distinct countries.

IEPG – What is it?

- There was no IEPG at either of the virtual IETF meetings
- 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

- FORT Project – a LACNIC Initiative
  - FORT validator is an open source RPKI validator. This solution allows operators to validate BGP routing information against the RPKI repository for use in router configuration and resolution.
  - FORT Monitoring - open access tool used to document routing incidents in Latin America and the Caribbean and identify regional trends
  - FORT Report - analyzes routing incidents and looks at how routing security impacts end users in the region
  - Fortproject.net

IEPG

- What part of "NO" is so hard to understand?
  - Experiment where they used a DNS name that did not exist from a signed zone.
  - They ended up seeing more queries for non-existent names than they expected
  - The average was 2.37 queries per non-existent name.
  - So NO apparently does not mean no.
  - The re-query rate was higher for signed then unsigned because the signed one has a little more delay.

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

- The day I broke the treadmills
  - Had a v6 only SSID from June 2018-March 2019
  - Had a raffle for folks who found bugs using v6 only SSID.
  - Only 5% of users went back to v4
  - What was broken
    - Treadmills
    - Spotify app on laptops
    - 3rd Party VPN system
    - StarCraft II – cannot log in with v6 only
    - MacOS internet recovery image

V6 Operations

- The day I broke the treadmills – cont
  - Lessons learned
    - "just disable v6" is never a good work around
    - You only get the experience when you turn off v4
    - Need to be specific about what you need when you say "I need IPv6"
    - Folks don't care which SSID unless it doesn't work.
    - Draft-ietf-dhc-v6only

V6 Operations

- IPv6 development and current status of China Telecom/China
    - One of three major providers in China
    - 163 million households and 308 million mobile users. Now 213.7 million users of which 160.3 active are all v6!
    - 450+ data centers are v6 enabled
    - Challenges
        - Home CPUs a problem
        - Transition of content and services (CDNs and IDCs)
        - Content providers concerned about end to end performance
    - Outside measurements are lower than what China reports internally

I wish I knew who drives this

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

- Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events
  - Improve reaction time of SLAAC
  - Appropriate lifetimes PIO (prefix information lifetimes) now is 1 day preferred 1 month valid - change timers preferred = router lifetime valid should be multiple (3x maybe)
  - Need a condition that triggers detection of stale info and what do you do to deprecate it

6MAN

- Self-configuring Stub Networks: Problem Statement
  - Automatically connect a stub network to the infrastructure?
  - Needs to work with existing v4 and v6 networks
  - This wouldn't exist if you could buy a homenet router.

6MAN

- IPv6 Minimum Path MTU Hop-by-Hop Option
  - More extension headers
- Attribution Option for Extension Header Insertion
  - This was not popular.
  - want to be able to Enable extension header removal and insertion in flight.
  - Insertion breaks
    - Fundamental attribution model of IP
    - Breaks PMTU discovery
    - Breaks ICMP (host gets ICMP errors for problems it didn't create
    - Breaks Authentication Header if applied to inserted headers

6MAN

- IPv6 host detection
  - Not possible to scan and find all IPv6 hosts on a network. This scanning is used to determine the hosts that exist and detect security risk.
  - We know from an old draft that scanning a whole IPv6 address range can be DOS attack.
  - This document proposes a way that the online IPv6 node information can be collected.

SPAM

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 the SIDR 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

- RPKI validated cache Update in SLURM over HTTPs
    - RPKI validated cache update information in JSON object format over HTTPs.
    - This requires RIRs to publish assertions with origin AS0 for all unallocated and unassigned space (v4 and v6) for which it is the current adminstrator. RUSH delivers those assertions to RPKI RPs using the AS0 SLURM file generated by the RIRs.
    - "AS0 is a red herring not a use case"
    - Concerns about the security of this

SIDR Operations

- AS Hijack Detection and Mitigation
  - June and July 2020 real AS hijacking events happened. (One ISP uses another ISP's AS as origin)
  - Origin validation not sufficient.
  - Proposing a new RPKI object REAP (Roas Exist for All Prefixes) REAP contains only ASN and is digitally signed by the AS.
  - Then when the origin validation is NotFound and there is a REAP object then NotFound becomes Invalid and should be rejected by the operator.

SIDR Operations

- Relying Party Measurements
  - This was not presented but the slides are interesting
  - RPs do not fetch from all CAs which results in incomplete view
  - Synchronization can take from 1 minute to 1 hour
  - Significant portion of RPs do not obtain a complete or timely view
  - Migration between RRDP and rsync does not work as defined

Lost in Translation

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

- As I like to say this is where the community networks hang out.
- Challenges in the rural communities: access to reliable, relevant information, and mobilization to build resilience
  - Rural South Africa
  - Zenzeleni Community Networks
  - Network owned and operated by the community it serves started in 2012.
  - 100000 people, 93% unemployed, 90% not completed school
  - most live on $1 USD/day
  - Unlicensed frequencies
  - COVID response - reliable info was a problem. Lots of fake news. no info in isiXhosa (local language). "our stories our internet" People submitting info on how they deal with COVID.

GAIA

- Energy and connectivity
  - SEEU North Macedonia
  - Goal is to manage carbon and energy efficiently
  - 6000 students.
  - 28% energy provided by solar PV
  - Green energy supported community network
  - Sustainable campus testbed
- The environmental sustainability of the Internet for all and everything
  - Looking at the energy required for all aspects of networking from the manufacture of the device to the network

Human Rights on the Internet RG

- The Human Rights Protocol Considerations Research Group 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, but not limited to the right to freedom of expression and the right to freedom of assembly.

HRPC

- Apps for COVID-19 Tracing An EU Data Rights View digital rights Ireland…
  - Covid tracing apps while adhering to EU data rights
  - Making the distance between notifying folks and knowledge of infection as short as possible. So mandatory tracking app not reasonable. Consent is what the EU is using. What does it mean under EU law? Freely given, specific, informed, unambiguous. Consent freely given? - power imbalance invalidates consent. Downloading the app there is no power imbalance. have to be able to agree to parts and disagree to other parts or it's not valid. The options added were "how are your symptoms today?" No feature creep allowed. Ability to withdraw consent. 1,000,000 downloads in about 1 day. 60% of iphone and andriod users. (Ireland).

SHMOO

- Stay Home Meet Only Online
  - The meeting planning activities that the IESG and the IETF LLC engage in would benefit from IETF community consensus guidance concerning novel aspects raised by these developments. The SHMOO working group is therefore chartered to document high-level guidance and principles to the IESG and the IETF LLC. The guidance and principles will concern the following:
    - Determinations of when a previously scheduled in-person meeting should be canceled and replaced with a fully online meeting.
    - Meeting planning in the event that a previously scheduled in-person meeting needs to be canceled and replaced with a fully online meeting.
    - Functional requirements for the technologies the IETF uses to support fully online meetings.
    - Determinations about the meeting fee for fully online meetings. Since remote participation in in-person meetings has historically been at zero cost to participants, LLC and IESG decisions about meeting fees for fully online meetings need to be informed by community consensus guidelines about whether and how to set a registration fee for fully online meetings.
    - The cadence of meeting scheduling and the mix of in-person versus fully online meetings going forward once the disruptions caused by the pandemic have subsided.

SHMOO

- The mailing list is manycouches@ietf.org and that always makes me smile.
- Meeting Planning
  - Mostly asking if we should have an IETF week or spread it out etc.
  - So arguments for and against meeting over a week.
  - "this is going to be miraculously brief"
  - "what is a meeting? do we even need a meeting? how do you make it welcoming to newcomers?"
  - "how do we enable interactions/relationships/etc"

SHMOO

- Technology requirements
  - Should we use jabber?
  - So all the stuff about technology and IETF values etc.
  - "we should be clear about our opinion of dog food"
  - "we didn't agree with the community on our opinion of dog food"
  - Should we reconsider chat and chat clients? Jabber is old.

DNS Deep Dive

- Huge number of DNS requests to accomplish a simple query. Wes just talked about the basics of how DNS works in general
- Geoff talked about DNS and how it scales or not.
  - Resilience using replication
  - Resilience engineering
    - Balance between freshness and effectiveness (caching)
    - Balance between cache time and update times
- Joao Damas
  - Talked about different implementations and solutions software for resolvers, root, etc.

Dispatch

- Overarching group for Applications and Real-Time Area (art)
  - Looks at if there is new work needed in this area
  - Discussed whether there is a group needed for email
    - Should there be a new group on email security?
    - Email is #1 used service on the Internet and hacks at an all time high

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/

Questions?

Additional Materials

- There was no time to talk about these slides but I'll leave them here for folks who are interested to review.

V6 Operations

- IPv6 Point-to-Point Links
  - We have talked about this draft before.
  - Info about what prefixes are being used for P2P links
  - 62% are using /64 instead of /127
- Reaction of Stateless Address Auto-configuration (SLAAC) to Flash-Renumbering Events
  - What happens when IPv6 prefixes become invalid without any signaling that it happened. When a CPE crashes and reboots nodes on the network may continue using stale prefixes resulting in connectivity problems.

V6 Operations

- Neighbor Cache Entries on First-Hop Routers: Operational Considerations
  - This talks about operational issues with neighbor discovery.
  - Neighbor discovery expects bi-directional traffic and if a host comes up for the first time and is communicating with an off-link destination this breaks that model

V6 Operations

- Default IPv6 Local Only Addressing for Non-Internet Devices
  - This is about devices that are not supposed to be reachable on the Internet but are connected to a globally reachable network. Like printers.
  - This document was not well received. The address you use does not make a device more secure. Propagates the "lie" that NAT is more secure.

6MAN

- Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers
  - We have talked about this draft before
  - WGLC
  - Routers and hosts should send unsolicited NA when it gets a new address makes multiple operator domains look like one network.
- Transmission of IPv6 Packets over Overlay Multilink Network (OMNI) Interfaces
  - Streamlining address assignment for airplanes

Adaptive DNS Discovery

- The **Adaptive DNS Discovery** (ADD) working group will work on the following deliverables:
  - Define a mechanism that allows clients to discover **DNS** resolvers that support encryption and that are available to the client either on the public Internet or on private or local networks.

Adaptive DNS Discovery

- CJ - So all these drafts about how to have multiple resolvers and discover and secure them. There are pushes and there are timers. It seems like it's all solving the same problem
  - draft-arkko-abcd-distributed-resolver-selection
    - what you do with multiple resolvers.
  - discovery-selection directions
    - discover that resolvers are there and whether they can do DoH or DoT
    - special capabilities etc. advertise their existence within DNS itself?

Adaptive DNS Discovery

- DNS-over-HTTPS and DNS-over-TLS Server Discovery and Deployment Considerations for Home Networks
  - DoT/DoH deployment considerations for home networks. It particularly sketches the required steps to use DoT/DoH capabilities provided by local networks.

Adaptive DNS Discovery

- Other drafts
  - draft-reddy-add-server-policy-selection
  - draft-mglt-add-rdp

Other Virtual Meetings

- ## MASQUE BoF
  - MASQUE is a mechanism that allows co-locating and obfuscating networking applications behind an HTTPS web server.

- ## WPACK Working group
  - The WPACK working group will develop a specification for a web packaging format that efficiently bundles multiple HTTP representations. It will also specify a way for the publisher to authenticate these resources such that a user agent can trust that they came from their claimed web origins.

Other Virtual Meetings

- PRIVACYPASS BoF
  - The objective of the Privacy Pass effort is to standardize a performance mechanism for providing privacy-preserving attestation of a previous successful authorization between a human and a server. The idea is to support use cases where it may be necessary to check that a client has been previously authorized by a service without learning any other information. Such lightweight authorization mechanisms can be useful in quickly assessing the reputation of a client in latency-sensitive communication.
- Other virtual BoF info is here https://www.ietf.org/blog/ietf107-bofs/

SPRING WG

- The Source Packet Routing in Networking (SPRING) Working Group is the
  home of Segment Routing (SR) using MPLS (SR-MPLS) and IPv6 (SRv6).
  SPRING WG serves as a forum to discuss SPRING networks operations,
  define new applications of, and specify extensions of Segment Routing technologies.

SPRING WG

- Segment Routing Policy Architecture
  - This draft was started at IETF 98. Still working out issues
- Seamless Segment Routing
  - Based on seamless MPLS
  - Large networks. This is a way to make smaller IGP domains
- Enhanced Performance Delay and Liveness Monitoring in Segment Routing Networks
  - Looking at delay and liveness in SR
- Sending probe messages along the path to know if there is a failure monitoring proactively.

SPRING WG

- Other drafts
  - Performance Measurement Using STAMP for Segment Routing Networks
  - Performance Measurement Using TWAMP Light for Segment Routing Networks
  - Service Programming with Segment Routing

GROW – What is it?

- The purpose of the GROW is to consider the operational problems associated with the IPv4 and IPv6 global routing systems, including but not limited to routing table growth, the effects of the interactions between interior and exterior routing protocols, and the effect of address allocation policies and practices on the global routing system. Finally, where appropriate, the GROW documents the operational aspects of measurement, policy, security, and VPN infrastructures.
- charter-ietf-grow-03

GROW

- BGP Monitoring Protocol (BMP) at the Hackathon
  - Hackathon analysis of CPU and memory usage of BMP
  - In some cases it added 10-20 seconds to convergence times. Used more memory.
  - Slides here
    - https://www.ietf.org/proceedings/108/slides/slides-108-grow-ietf-108-hackathon-bmp-00

GROW

- AS-Path Prepend BCP
  - Prepending is used to make an AS path longer and the route less favorable
  - Excessive prepending has caused problems on the Internet
  - Recommendations
    - Only prepend when absolutely necessary
    - Prepending more than a couple of times buys you nothing
    - Prepending-to-all is a self-inflicted and needless risk.
    - Operators should consider limiting the maximum number of prepends accepted

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 <u>charter-ietf-dnsop-04</u>

DNS Operations

- Fragmentation Avoidance in DNS
  - We have talked about this draft before
  - Fragments are bad
  - Working on ways to prevent them
- Service binding and parameter specification via the DNS
  - Designated type to deliver encrypted keys for TLS
- The DELEGATION_ONLY DNSKEY flag
  - You only delegate but you don't sign anything in your domain

DNS Operations

- Parameterized Nameserver Delegation with NS2 and NS2T
  - Two new resource types NS2 and NS2T to facilitate transport method negotiation. Signals how authoritative servers in a zone accept queries.
- Initializing a DNS Resolver with Priming Queries
  - How to start a recursive nameserver with an empty cache
  - Historically this is started with a flat file of root servers that is used to find the info. That file can be out of date (IP addresses of the servers change over time)

DNS Operations

- Revised IANA Considerations for DNSSEC
  - Review requirements needed to add DNSSEC algorithms and resource records into the IANA registries.
- DNS Access Denied Error page
  - So stuff like malware, parental controls, etc. block DNS
  - User does not know why the domain is being blocked.
  - So better errors to users about why the DNS is blocked.
  - Not compliant with DNSSEC.

Autonomic Networks

- The Autonomic Networking Integrated Model and Approach (ANIMA) working group develops and maintains specifications and documentation for interoperable protocols and procedures for automated network management and control of professionally-managed networks.

- The vision is a network that configures, heals, optimizes and protects itself. The strategy is the incremental introduction of components to smoothly evolve existing and new networks accordingly.

Autonomic Networks

- An Autonomic Control Plane
  - Autonomic functions need a control plane to communicate, which depends on some addressing and routing. This Autonomic Control Plane should ideally be self-managing, and as independent as possible of configuration.
  - They need reviewers. I'd say if you run a network at some point this may happen and you might want to know about it.

Autonomic Networks

- BRSKI Cloud Registrar
  - "gets on the Internet via magic"
  - So this is now a random device gets automatically connected
  - You put a device on the network and then it talks to some
  - registry to get a voucher to get connected to where you're
  - located. SO send a cert to the manufacturer and it redirectsyou ? So weird
  - "Cloud is so cloudy"
  - "looking at your draft it still looks like magic to me"

LSVR

- The Link-State Vector Routing (LSVR) Working Group is chartered to develop and document a hybrid routing protocol utilizing a combination of link-state and path-vector routing mechanisms. The LSVR WG will utilize existing IPv4/IPv6 transport, packet formats and error handling of BGP-4 consistent with BGP-LS NLRI encoding mechanisms (RFC7752) to facilitate Link-State Vector (LSV) routing information distribution. An LSV is intended to be specified as a data structure comprised of link attributes, neighbor information, and other and other potential attributes that can be utilized to make routing decisions.

LSVR

- A lot of this work is moving along. There are multiple implementations of BGP SPF and even an open source implementation

- Layer 3 Discovery and Liveness
  - discovery of layer 3 ip topology and liveness
  - not a routing protocol just discover the link

- Layer 3 Discovery and Liveness Signing
  - The Layer 3 Discovery and Liveness protocol OPEN PDU may contain a key and a certificate, which can be used to verify signatures on subsequent PDUs.

LSVR

- L3DL Upper Layer Protocol Configuration
  - being able to discover the BGP attributes of a neighbor PDU exchanged at L2. Hey there is an upper layer protocol (bgp) that has the following attributes. Minimal config parameters
  - "multiple sources of truth are a recipe for complexity and pain"

LSR

- The Link-State Routing (LSR) Working Group is chartered to document current protocol implementation practices and improvements, protocol usage scenarios, maintenance and extensions of the link-state interior gateway routing protocols (IGPs) - specifically IS-IS, OSPFv2, and OSPFv3. The LSR Working Group was formed by merging the isis and ospf WGs and assigning all their existing adopted work at the time of chartering to LSR.
- IS-IS is an IGP specified and standardized by ISO through ISO 10589:2002 and additional RFC standards with extensions to support IP that has been deployed in the Internet for decades. For the IS-IS protocol, LSR-WG's work is focused on IP routing, currently based on the agreement in RFC 3563 with ISO/JTC1/SC6. The LSR-WG will interact with other standards bodies that have responsibility for standardizing IS-IS. LSR-WG will continue to support Layer 2 routing (for example TRILL work) as needed.
- OSPFv2 [RFC 2328 and extensions], is an IGP that has been deployed in the Internet for decades. OSPFv3 [RFC5340 and extensions] provides OSPF for IPv6 and IPv4 [RFC5838] which can be delivered over IPv6 or IPv4 [RFC 7949].

LSR

- IGP Flex Algorithm
  - Allows IGPs to navigate constraint base paths themselves without the use of RSVP or Segment routing.

- OSPF Prefix Originator Extensions
  - Mechanism for inclusion of originator router information.

- IS-IS Topology-Transparent Zone
  - A routing abstraction where part of the network (nodes and links) are just known as a single virtual node to the rest of the network.

LSR

- Experimental Results in IS-IS flooding
  - Looking at flooding and how it can be improved
  - She tried all sorts of parameters that are in various drafts and then saw the result of using and changing them
  - Partial Sequence Numbers Protocol Data Unit (PSNP) how fast?
    - Too slow causes retransmissions
    - Too fast wastes bandwidth, queue space, etc.
    - Reducing PSNP interval can reduce LSP retransmissions and flooding duration.
  - https://www.ietf.org/proceedings/108/slides/slides-108-lsr-04-isisfloodingstudy-00

LSR

- Flooding Topology Minimum Degree Algorithm
  – Data centers are very dense and Link State flooding is not efficient. This is an abstraction that allows only part of the topology to be smaller.
- Other drafts
  – Using IS-IS MT for SR based Virtual Transport Network
  – IGP Extensions for Segment Routing Service Segment
  – IS-IS Extensions to Support Packet Network Slicing using SR
  – ISIS Extension to Support Network Slicing over IPv6 Dataplane
  – IGP Flexible Algorithm with L2bundles