IETF Report

CATHY ARONSON
ARIN 43, BARBADOS

About This Presentation

This presentation is an official IETF report

- **This report covers IETF 103 (Bangkok) and 104 (Prague)**
- **This is not an in-depth IETF report lots of exercise for the reader**
- I am officially the ARIN IETF Reporter for 2019
- 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

- I found out that ".horse" exists.
  - Traceroute to bad.horse is really funny
  - Someone clearly had way too much time on their hands..
- PechaKucha
  - Is a presentation style in which 20 slides are shown for 20 seconds each (6 minutes and 40 seconds in total).
  - http://bapk-videos.mamadrum.net/IETF-104-Prague-videos/

Drafts I've Recently Read

- **IPv6 Address Assignment to End-Sites**
  - "This document reviews the architectural and operational considerations of end-site assignments, and reiterates that assignment policy and guidelines belong to the RIR community."
  - "23% of the responders (generally in more advanced countries, in terms of IPv6 deployment) assign a /48, 35% assign a /56 and 33% assign a single /64"
  - "Math's show that even assuming 32 billion of humans (2^35), and assigning each of them 4 /48's, with a 50% routing efficiency, we can repeat that 2^10 times, so if average life span of each human is 100 years, and we don't recover back the /48's, we will be able to use IPv6 addressing space for over 102.400 years."

Drafts I've Recently Read

- Simple Internet Protocol (SIP) Specification
  - This was one of the proposals to replace IPv4 and it has been re-published as Historic.
- 464XLAT: Combination of Stateful and Stateless Translation
  - Provides limited IPv4 connectivity across an IPv6-only network by combining existing and well-known stateful protocol translation
  - Allows v4 only hosts to work on a v6 only network

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

- I wasn't at IEPG in Bangkok…
- QUIC Observations
  - https://blog.apnic.net/2018/01/29/measuring-quic-vs-tcp-mobile-desktop/
  - there may need to be operational changes to effectively replace TCP with QUIC
  - Middleboxes looking at the headers (need to avoid this)
  - 3% page load time (PLT) improvement on Google search and 18% reduction in buffer time on YouTube
  - Worse than TCP when packets are reordered

IEPG

- BGP Blackholing Reconsidered
  - Make it so victim IP address of DDOS attack doesn't get traffic anymore. Tell other providers not to send traffic to it.
  - NTT has a 57MB router config because of this
- Proposing a black hole validation process
- Working on black hole validator software open source

IEPG

- Reaction of Stateless Address Autoconfiguration (SLAAC) to Renumbering Events
  - The router reboots or is rebooted the device gets a new prefix but the old addresses are maintained and preferred
    - This causes a lot of problems. No connectivity to new owner of prefix. IPv6 connectivity may fail.
  - "There is no spoon. The network must be resilient!"

Technology Deep Dive - Modern Router Architecture (WGTLGO)

- This is something new the IETF is trying.
- IESG sees contentious cross-area/late IETF Last Call discussions on related topics
- IPv6 extension header issues are still **late surprises** for too many working groups

WGTLGO

- "Assume a spherical router at zero gravity and zero degrees temperature"
- Forwarding Plane Realities
- Summarizing implications for protocol designers
- There is a lot that I think needs to be done. IETF is doing stuff that may not be doable in hardware.

WGTLGO

- A couple of quotes that sum it up
- "We specifically asked the ASIC folks and they said no to 128 bits. They said no and the IETF gave us them anyway. Specifically asked for variable addresses."
- "just because the IETF decides to do it doesn't mean a chip designer has to like it right?
- **It seems like there is a push and pull between what we're doing at the IETF and how that ends up in hardware/software on a router.**

KSK Side Meeting -Bangkok

- This was a meeting in Bangkok about the KSK roll and soon the old KSK was going to be revoked.

- The wanted to start the discussion about when and how often to roll the key.

KSK Side Meeting - Bangkok

- Some thoughts
  - Maybe a bunch of folks don't validate
  - Need to discuss when/if to roll the key again
  - Folks surprised how little data we have
  - Folks going out and looking for stories after the fact
  - Suggestion that we roll the keys regularly so we know how to do it?
  - Need a recommendation that keys not be hardcoded.
  - A couple of quotes
    - "Engineering done by gut feeling is often a bad thing"
    - "is it possible to design so we have more info?"

KSK Futures BoF

- The key signing key (KSK) for the DNS root was changed for the first time on 11 October 2018. During the lead-up to the change, members of the DNS operations and security communities started discussing how the KSK should change in the future. Some of the topics of this discussion have included how often to change the KSK, requirements before making the next change, adding additional standby KSKs to the root zone, changing the signing algorithm, and so on.

KSK Futures BoF

- www.icann.org/review-2018-dnnsec-ksk-rollover.pdf
- "250 million users were affected negatively"
- "Some ISPs turned off validation and didn't turn it back on"
- "System is not reliable and the DNS is so opaque that we don't know where the issues are"
- "Need to protect the root system against DNSsec"

DHC – What is it?

- 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 generally outside of scope for the DHC WG. Such options should be defined within their respective WGs or sponsored by an appropriate AD 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.

DHC

- **DHC group was started in 1989.**
- **RFC8415 (DHCPv6) was made proposed standard in November of 2018 so maybe full standard in November 2019**

DHC

- Link-Layer Addresses Assignment Mechanism for DHCPv6
  – This is emerging IEEE work
  – **Assigning MAC addresses dynamically.**
  – **This work is being done because so many devices are short lived like VMs, etc.**
  – Hypervisor would get a block of MAC addresses that it hands out.

DHC

- Half of the 48-Bit MAC address space was reserved for local use.
  - **IEEE has broken them up into 4 quadrants**
  - **draft-bernardos-dhc-slap-quadrant**
    - Standard Assigned Identifier quadrant
    - Extensions to DHCPv6 protocols to enable a DHCPv6 client or a DHCPv6 relay to indicate a preferred SLAP quadrant to the server, so that the server allocates the MAC address to the given client out of the quadrant requested by relay or client.

Link State Routing (LSR) – What is it?

- Link State Routing
  - 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.

LSR

- My thoughts, "I can't help but think this is like softwires all over again. A lot of drafts that are all trying to solve the same thing. "
- Update on dynamic flooding
  - Dynamic flooding regardless of topology
  - OSPF and IS-IS
  - so this appears to be a flooding mechanism that is efficient and gives you two links to everywhere. solves flooding on dense graphs.. It doesnt work great if the network isn't dense but it doesn't hurt

LSR

- IS-IS Sparse Link-State Flooding
  - Want something simple
  - Fully distributed any topology
  - Sparse flooding tree.. use an anchor or two.
- OSPF Flooding Reduction
  - Another draft to reduce and compute flooding topology

LSR

- Distributed Algorithm for Constrained IGP Flooding
  - Another draft for the same stuff.
  - "visual representation of the results diagram"
  - "everyone is bi-connected to the flooding topology"

LSR

- Hierarchal IS-IS
  - In IS-IS levels 3-8 are not defined
    - There are 6 reserved bits become levels 3-8
    - So this is all we need to make this happen. Giant request to iANA for new code points.
    - "I am not proposing anyone do any stupid stuff"
    - Need deployment cases..

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-ietf-dnsop-serve-stale**
  - This draft defines a method for recursive resolvers to use stale DNS data to avoid outages when authoritative nameservers cannot be reached to refresh expired data.

DNS Operations

- draft-ietf-dnsop-aname
  - This document defines the "ANAME" DNS RR type, to provide similar functionality to CNAME, but only for type A and AAAA queries. **Unlike CNAME, an ANAME can coexist with other record types**. The ANAME RR allows zone owners to make an apex domain name into an alias in a standards compliant manner.
  - This fixes the problems with CNAME but allows the same desired functionality.

DNS Operations

- draft-mayrhofer-did-dns
  - Decentralized Identifiers (DIDs) [W3C-DID] use a Uniform Resource Identifier (URI) scheme [RFC3986] to identify persons, organizations, or things in decentralized infrastructure, such as blockchains and distributed ledgers.
    - **Yup Blockchain in the DNS.. Fun**

DNS Operations

- **Other drafts**
  - draft-ietf-dnsop-rfc7816bis
    - QNAME minimization?
  - draft-ietf-dnsop-7706bis
    - rewriting to match current reality.
  - draft-hoffman-dns-special-labels, Hofmann
  - draft-lhotka-dnsop-iana-class-type-yang, lhotka

Plenary

Since 17th century, there has been a house in which nothing memorable has ever happened.

May Czech history continue to avoid this place!

Computing in the Network Proposed Research Group

- The COIN proposed research group (COINRG) will explore existing research and foster investigation of "Compute In the Network" and resultant impacts to the data plane. The goal is to investigate how to harness and to benefit from this emerging disruption to the Internet architecture to improve network and application performance as well as user experience. COIN will encourage scrutiny of research solutions that comprehend the re-imagining of the network to be a place where routing, compute, and storage blend.

COINRG

- Edge data discovery
  - The edge is no longer data centers
  - The edge is ambiguous .. proliferation of edges

COINRG

- Industrial Networks
  - Talked about how computing could happen closer to the robots, etc so that they function better. If more than 1 second delay problems occur.
  - robots - network - edge cloud/ control
  - **use in-network processing to move control functions into switches. reduces latency**
  - **real world examples - arc welding robot**
  - another - mobile cooperating robots

COINRG

- Computing Service Providers
  - CAN Computing As a Network
  - Even if you're doing in-network computing you still need more resources than a switch would have
  - **Neighborhood clouds**
  - Basically try to move as much into the network as we can ?

OPSEC – What is it?

- Operational Security Capabilities for IP Network Infrastructure
- The OPSEC WG will document operational issues and best current practices
with regard to network security. In particular, the working group will
clarify the rationale of supporting current operational practice,
addressing gaps in currently understood best practices and clarifying
liabilities inherent in security practices where they exist.

OPSEC

- Operational Security Considerations for IPv6 Networks
  - This draft was started in 2012.
  - There are still references to things that aren't security issues like using **PI address** space. Those are supposed to be removed

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

- Discovering PREF64 in Router Advertisements
  - **This document specifies a Router Advertisement option to configure the NAT64 prefix.**
  - IPv4 access on IPv6-only networks
  - Including the NAT64 prefix in the Router Advertisement minimizes the number of packets required to configure a host.

V6 Operations

- **CERNET2 IPv6-only Practice: Backbone, Servers, Clients and 4aaS**
  - China Education and research network
  - 25 PoPs and 1000+ Universities
  - V6 only NOT dual stack, even upstream is v6 only.
  - V6 only with single translation is optimum

V6 Operations

- NAT64/464XLAT Deployment Guidelines in Operator and Enterprise Networks
  - This is an analysis that covers most of the combinations of these services
    - DNS 64 may break DNSSEC
    - NAT64 doesn't work with IPv4-only hosts/apps
    - NAT64/DNS64 will not work with some literals

V6 Operations

- Pros and Cons of IPv6 Translation Technologies for IPv4-as-a-Service (IPv4aaS)

    – **Comparison of 464XLAT, Dual Stack Lite, lw4o6, MAP-E, and MAP-T to help service providers pick the best mechanism for a particular deployment.**

V6 Operations

- 464XLAT Optimization for CDNs/Caches
  - Looks like there is a problem with IP/ICMP Translation Algorithm (SIIT) where v4 only device gets translated multiple times.

IRTF Open

- ANRP Awardees
  - Engineering Egress with Edge Fabric: Steering Oceans of Content to the World
    - Very interesting presentation/paper about Facebook's edge fabric that manipulates BGP routes to ease congestion and get the best performance

IRTF Open

- ANRP Awardees
  - BGP Communities: Even more Worms in the Routing Can
    - Talk/paper about BGP communities, what they're used for and how far do they propagate.
    - Some info about how easy it would be to do malicious things with communities.

IRTF Open

- Taking a Long Look at QUIC: An Approach for Rigorous Evaluation of Rapidly Evolving Transport Protocols
  - An analysis of the performance of QUIC and performance of QUIC vs TCP
  - Also does the presence of QUIC on the network affect TCP performance.

Measurement and Analsys of Protocols (MAPRG)

- The Measurement and Analysis for Protocols Research Group Research Group (MAPRG) aims to provide a forum for interchange between these two (IETF, IRTF) communities, supporting:
  - exchange of measurement-derived insight; discussion of techniques and best practices for measurement relevant to protocol
  - engineering and network operations;
  - collaborations to share data supporting these measurements; and
  - a "landing pad" for the Internet measurement community to introduce its efforts to the * IETF.

MAPRG

- Heads-up talk: Privacy and Security Issues in IPv6 Deployment
  - Interesting talk about different ways to track people and discover topology in IPv6.
- A Tale of Two Checksums
  - QUIC performance over a satellite public Internet access

MAPRG

- Other measurements
  - Evaluating the Performance of CoAP, MQTT, and HTTP in Vehicular Scenarios
  - The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem
  - Is the Web Ready for OCSP Must Staple?

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

- HOMENET marketing slides? Trying to figure out why there aren't more implementations of HOMENET
- Homenet Naming and Service Discovery Architecture
  - how names are published and resolved on homenets, and how hosts are configured to use these names to discover services on homenets. It presents the complete architecture, and describes a simple subset of that architecture that can be used in low-cost homenet routers.
  - A lot has to happen automatically since a HOMENET does not have an "operator".
- Securing the Home Network
  - This is not all there yet.

HOMENET

- SecureHomeGateway project
  - everything comes with a name?
  - allows for mitigation of weaponizing the IoT devices.
  - you scan the code on the device and it verifies it and adds config to the router to filter the device

HOMENET

- draft-ietf-homenet-babel-profile-07
  - **How do keys and creds get distributed in a HOMENET context? Seems like a huge question that needs to be answered.**
- Outsourcing Home Network Authoritative Naming Service
  - drafts on front-end-naming-delegation and naming-architecture-dhc-options, and their implementation

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

- Node requirements will be RFC soon
- IPv6 Segment Routing Header (SRH)
  - First presented 6 years ago
  - 5 years since the first implementation
  - This will probably move forward.

6MAN

- IPv6 Router Advertisement IPv6-Only Flag
  - **This tells a host that the network is v6 only and not to wait for v4 response.**
  - There is one current implementation of this
  - Added gorp to make it hard to do this maliciously

6MAN

- Path MTU Hop-by-Hop Option
  - **This is different than the packet too big message solution we have talked about before**
  - **Bigger packets as the links get faster really helps.**
  - Changed to experimental because we need real data to see what to do
  - So this is an experiment to figure out what mechanism(s) work
  - Can we start moving to jumbo frames?
  - "make sure it's silicon friendly"

6MAN

- Privacy Extensions for Stateless Address Autoconfiguration in IPv6
  - large discussion about generating these addresses and how they generate them
- Discovering PREF64 in Router Advertisements
  - Nat64 prefix detection in RAs
  - The problem is secure prefix discovery in SLAAC-only networks.

6MAN

- IPv6 Segment Routing Header (SRH)
  - This is version 17! Wow
  - running code update - a number of them.
    - cisco has shipping code, Linux and others
    - Huawei has code too
    - Barefoot, Spirent, Ixia all have code.
  - Applications with support too

6MAN

- Packet Too Big (PTB) Messages, draft-leddy-6man-truncate
  - This is a way to do PMTU discovery. The initial packet gets sent with a truncate bit set. If the MTU is too small the packet gets truncated and at the destination an ICMP message is sent to the source to say the appropriate MTU.

6MAN

- Other drafts
  - Path MTU Solution Space
  - Destination Originates Internet Control Message Protocol (ICMP) Packet Too Big (PTB) Messages
  - In-situ OAM IPv6 Options
  - OAM in Segment Routing Networks with IPv6 Data plane

Global Routing Ops – 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.

Global Routing Operations

- Solution for Route Leaks Using BGP Communities
- Communities Are Everywhere
  - 14% transit ASNs propagate communities
    - Doesn't seem like a lot but they're heavily interconnected.
  - 50% of communities travel more than 4 ASNs
  - Longest seen 11 ASNs
  - Did some experiments
    - Interesting that an attacker injects a blackhole prefix that gets black holed but shouldn't be. Basically all the off path communities are causing hacks to succeed.

Global Routing Operations

- draft-gu-grow-bmp-route-leak-detection
  - Akamai also using BMP to validate to make sure that internal prefixes that you don't want to go out. (BGP Monitoring Protocol)
  - This is detection not prevention.
- There is no document on how to roll out bgp security.   Maybe create a living document that can change and publish it quicker?

SUIT WG – What is it?

- Software Updates for Internet of Things
  - Vulnerabilities in Internet of Things (IoT) devices have raised the need for a secure firmware update mechanism that is also suitable for constrained devices. Security experts, researchers, and regulators recommend that all IoT devices be equipped with such a mechanism. While there are many proprietary firmware update mechanisms in use today, there is no modern interoperable approach allowing secure updates to firmware in IoT devices. In June of 2016 the Internet Architecture Board organized a workshop on 'Internet of Things (IoT) Software Update (IOTSU)', and RFC 8240 documents various requirements and challenges that are specific to IoT devices.

SUIT WG

- Current Documents
  - SUIT Architecture
  - SUIT Information Model
  - SUIT Manifest Format
  - SUIT Hackathon Report
    - Many folks came to the hackathon for this but not to IETF.

IRTF QIRG – What is it?

- Quantum Internet Proposed Research Group
  - A Quantum Internet, if developed and deployed, will bring new communication and remote computation capabilities, as well as improving the accuracy of physical sensor systems (e.g., for interferometry for long-baseline telescopes). One key area will be cryptographic functions including quantum key distribution and quantum byzantine agreement.

QIRG

- Six stages of evolution of a quantum network
  - I keep pondering.. What in the world is the quantum Internet? Apparently I am not alone.
  - entanglement – completely coordinated and inherently private can produce entanglement with teleportation?? Huh? Or quantum repeater??
  - Need quantum network stack?
- Advertising Entanglement Capabilities in Quantum Networks
  - Modifying IS-IS and OSPF for quantum networks

QIRG

- The first session in Prague was a Quantum Internet Tutorial. I decided it's a Quantum Bafflement ™

- Basically at least for now most of the "Quantum Internet" is distributed computing over the existing Internet

- Long term it will be something else. Maybe if we have a physicist in the room you can help me with this.

Parting Thoughts

- IPv6 and White Sand Beach in Jamaica

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?