IETF Report

CATHY ARONSON
ARIN 44, AUSTIN TX

About This Presentation

This presentation is an official IETF report

- **This report covers IETF 105 (Montreal)**
- **This is not an in-depth IETF report lots of exercise for the reader**
- I am officially the ARIN IETF Reporter until June 2020
- 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

- RFC 8651 on Dynamic Link Exchange Protocol (DLEP) Control-Plane-Based Pause Extension
  - October 7, 2019
  - Why is this important?

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

- “How Big Was That”
  - Based on these vulnerabilities
    - CVE-2019-11477 – 11479
  - These were denial of service attacks that exploited a bug in a not frequently used code path for TCP Maximum Segment Size (MSS)
- The details “Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service.”

IEPG

- Cache Me If You Can: Effects of DNS Time-to-Live
  - This is an analysis of DNS TTL values and how the affect performance of the DNS.
  - Found that longer caching produced faster responses, lower DNS traffic and more robust to DDoS attacks on the DNS.
  - Found that shorter caching supports operational changes, can help with DNS-based response to DDoS attacks, can cope better with DNS-based load balancing

IEPG

- DNS Transparency
  - This is a new way for changes in the DNS to be sent to the folks who run the servers
    - Visible and auditable
  - There have been attacks where changes were made sort term and changed back before folks noticed.

IEPG

- Sea Turtle..
  - A cyber threat campaign targeting public and private entities, including national security organizations, located primarily in the Middle East and North Africa. January 2017-2019
  - The actors behind this campaign have focused on using DNS hijacking as a mechanism for achieving their ultimate objectives.
  - There is concern that this could be used more widely and causing more damage.
  - https://blog.talosintelligence.com/2019/04/seaturtle.html

IEPG

- Sea Turtle
  - It is estimated that 40 different organizations across 13 different countries were compromised during this campaign
  - “The actors are responsible for the first publicly confirmed case against an organizations that manages a root server zone, highlighting the attacker's sophistication.”

IEPG

- “Routing in 2018”
  - Still the same as before. Even though we have reached IPv4 address exhaustion.
    - Shorter prefixes being added but the rate is unchanged
  - IPv4 52,000 prefixes and 3400 ASNs / Year
  - IPv6 15,000 prefixes and 2000 ASNs / year
  - IPv6 is way less stable. Maybe because of tunnels and old software

Technical Plenary

- If you get a chance to watch this you should.
  - Current Thinking About Privacy on the Internet
    - Steve Bellovin and Arvind Narayanan
    - Good talks on network measurement and privacy.
    - 90% of users have a unique browser fingerprint and you can look at yours.
    - The House that Spied on me: need a debug mode for IoT devices because we can't look because it's encrypted. Nests with microphones.. Interesting
    - In the 1960s we had "notice and consent" notice and consent is dead now because we just have no idea who is collecting what and how they're using it.

Transport Area WG (TSVWG)

- The Transport Area receives occasional proposals for the development and publication of RFCs dealing with transport topics that are not in scope of an existing working group or do not justify the formation of a new working group. TSVWG will serve as the forum for developing such work items in the IETF.

TSVWG

- Transport Encryption: Impact of Transport Header confidentiality on network operation and the evolution of the internet / Impact of Transport Header Encryption
  - This looks at end-to-end transport protocol encryption and the impact on network protocol design and network operation. Transport measurements have been important to the design of current protocols.
  - Some things that we lose with this encryption
    - Network Operations and Research
    - Protection from DoS
    - Network troubleshooting and diagnostics
    - Network traffic analysis
    - Open and verifiable network data.

TSVWG

- Loss Signaling for Encrypted Protocols
  - Uses 2 bits to allow endpoints to signal packet loss in a way that can be used to measure and locate the source of the loss.
  - This is particularly helpful with encrypted transport headers.

Security Area Directorate (SAAG)

- The Security Area Directorate provides support to the IETF Security Area Directors. The group consists of the Working Group Chairs of the Security Area and selected individuals chosen for their technical knowledge in security and their willingness to work with other groups within the IETF to help provide security throughout IETF protocols.

SAAG

- Privacy Issues in Identifier Locator Separation Protocols
  - In LISP participating nodes can share their current ID to locator info with their peers.
  - This document looks at the possible privacy issues with that sharing
    - Location and movement privacy?

SAAG

- Do we need an expanded Internet Threat Model?
  - #1 " we assume that the attacker has nearly complete control of the communications channel over which the end-systems communicate"
  - #2 "we assume that the end-systems engaging in a protocol exchange have not themselves been compromised"
  - The belief is that #1 is still necessary for protocol design but is #2 still sufficient?
  - They're looking for feedback

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 Ops

- https://datatracker.ietf.org/doc/draft-ietf-dnsop-aname/
  - ANAME is like CNAME but fixes problems with CNAME existing with other record types.
- Considerations for Large Authoritative DNS Servers Operators
  - Considerations for operators configuring authoritative servers
    - Mostly about how to configure Anycast to get a robust set up that's less affected by attacks.

DNS Ops

- draft-fujiwara-dnsop-avoid-fragmentation
  - Fragmentation is problematic in the DNS and elsewhere.
  - Proposes max/min payload sizes.
- draft-nygren-httpbis-httpssvc/
  - This draft seems to solve the same problem as ANAME as well as allowing an HTTPS origin hostname to be served from multiple network services, each with associated parameters

DNS Ops

- draft-brotman-rdbd
  - Related Domains By DNS
    - A mechanism by which a DNS domain can publicly document the existence or absence of a relationship with a different domain, called "Related Domains By DNS", or "RDBD".
    - Hard to know if example.com and dept-example.com are related or if one might be an attacker impersonating the example.com domain.
- draft-woodworth-bulk-rr
  - A bulk format that allows for easy sharing between primary and secondary nameservers for a zone

Applications Doing DNS BoF

- Snowden revelations lead to the securing of the DNS, encrypting DNS traffic. Thus DNS over TLS (DoT)
- Then came DNS over HTTP (DoH)
- Mozilla's perspective
  - "Individuals' security and privacy on the Internet are fundamental and must not be treated as optional"

Applications Doing DNS BoF

- DoH BCP
  - The DoH protocol creates technical challenges for operators/providers intending to deploy DoH (and DoT) resolvers
  - IETF should consider a BCP which documents concerns and provides guidance.
  - The slides have a long list of potential topics
    - Seems to me like this is a good idea.

Applications Doing DNS BoF

- List of DoH BCP Topics
  - How operator and enterprise networks can offer local DoH (and DoT) servers?
  - How operator and enterprise DoH servers can be used across home, mobile and enterprise (BYOD) networks?
  - Network & server performance, load testing, capacity & resilience planning
  - Impact on existing infrastructure –load balancers, captive portals, NAT, proxies, CDNs, etc.
  - Impact to CPE –connection set-up and DoH (and DoT) proxies and certificates
  - Providing DoH and DoT servers in split DNS environments
  - Interactions between applications and OS / Kernel DNS settings
  - How DoH clients will handle policy negotiation with servers and manage conflicts
  - Protection of application-specific DoH and DoT resolver configuration
  - Authentication requirements for DoH and DoT resolvers
  - Management of TLS sessions at DNS query rates –ticket duration, restarts, etc.
  - Options to minimise TLS overheads for DoT and DoH traffic

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 OPs

- Autonomous System Provider Authorization in the Resource Public Key Infrastructure
  - An Autonomous System Provider Authorization is a digitally signed **object that provides a means of verifying that a Customer Autonomous System holder has authorized a Provider Autonomous System to be its upstream provider** and for the Provider to send prefixes received from the Customer Autonomous System in all directions including providers and peers.
  - new RPKI project can detect hijacks etc
  - Treat hijacks and route leaks differently?

SIDR Ops

- Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers
  - It can be a large operational burden to do prefix origin validation so this new mechanism to facilitate validation.
  - The result of this prefix origin validation is signaled to peers by using the EBGP Prefix Origin Validation State Large Community as introduced in this document.

SIDR Ops

- BGP Prefix Origin Validation State Extended Community
  - BGP extended community to carry the origination AS validation state inside an autonomous system.
  - Allows IBGP speakers to know the state and configure local policies

SIDR Ops

- RPKI Signed Object for Trust Anchor Keys
  - This could facilitate key rolls in RPKI
  - An RPKI signed object for Trust Anchor Keys (TAK), that can be used by Trust Anchors to signal their set of current keys and the location(s) of the accompanying CA certificates to Relying Parties, as well as changes to this set in the form of revoked keys and new keys, in order to support both planned and unplanned key rolls without impacting RPKI validation.
  - Tim will be doing a proof of concept on this.

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

- **IPv6 Deployment at Liquid Telecom**
  - Africa's largest fiber network (16 countries)
  - Enterprise centric customer base. Not easy to get them to switch. NAT also works as a security mechanism.
  - Folks often bring their own CPE and that's often a problem. Often CPEs have different transition mechanisms
  - Problem with different countries' AUP
    - This country will not allow X traffic (X = whatsapp, Facebook, or whatever)

V6 Operations

- 464XLAT Optimization
  - Useful for 4 to 6 translation
  - If the devices or applications in the customer LAN are IPv6-capable, then the access to the CDNs, caches or other resources, will be made in an optimized way, by means of IPv6-only, not using the NAT64
  - if the devices or applications are IPv4-only, for example, most of the SmartTVs and Set-Top-Boxes available today, a non-optimal double translation will occur
  - This document tries to eliminate this double translation when possible.

V6 Operations

- Neighbor Cache Entries on First-Hop Routers: Operational Considerations draft-linkova-v6ops-nd-cache-init-01
  - Neighbor Discovery (RFC4861) is used by IPv6 nodes to determine the link-layer addresses of neighboring nodes as well as to discover and maintain reachability information. There is a problem when a host that has never been seen before is added.
  - The current standard assumes communications are bi-directional and they are not always that way. A valid neighbor advertisement is not used because the protocol assumes that it should already be in the neighbor cache. This is a problem when a host is communicating off-link via it's first-hop router.

V6 Operations

- Operational Security Considerations for IPv6 Networks draft-ietf-opsec-v6-17
  - This has been worked on since 2012. Folks think it's time to move the document forward
- IS-IS Multi Topology Deployment Considerations draft-chunduri-lsr-isis-mt-deployment-cons-02
  - This covers scenarios using IS-IS with v4, v6 and v4/v6.

V6 Operations

- IPv6 Point-to-Point Links draft-palet-v6ops-p2p-links-03
  - different alternatives for configuring IPv6 point-to-point links, considering the prefix size, numbering choices and prefix pool to be used.
  - Covers /64, /127, /126, GUAs, ULAs, unnumbered.

V6 Operations

- draft-palet-v6ops-ipv6-only
  - Terminology regarding the usage of expressions such as "IPv6-only", in order to avoid confusions when using them in IETF and other documents. The goal is that the reference to "IPv6-only" describes the actual native functionality being used, not the actual protocol support.
  - If a link is only natively forwarding v6 but v4 is encapsulated then it is considered v6-only

Technology Deep Dive

- Technology Deep Dive: How Network Interface Cards (NICs) Work Today
  - This session started with a description of how a basic network interface card (NIC) operates and led into NIC feature evolution.

ANRW

- Advanced Networking Research Workshop
  - Securing IPv6 Neighbor Discovery and SLAAC in Access Networks through SDN.
    - This paper proposes and evaluates a new approach, based on Software Defined Networking (SDN), to secure the IPv6 Neighbor Discovery Protocol (NDP) message exchange and make the Stateless Address Auto-configuration safer.
      - Slaac is the default
      - dhcpv6 is not as wide spread even if it's there you have to still do some of the slaac. SLAAC uses NDP.
      - NDP has been diagnosed as a security risk for switched Ethernet networks, because routers and hosts implicitly trust all other nodes on the local network.
      - Does IPsec fix this? yes if you have a valid IP address.

ANRW

- What time is it? Managing Time in the Internet.
  - This is all about how time is managed around the world.
  - Sometimes I am amazed by how hokey some of these things are.
  - Time Zone Database (TXDB) is operated by IANA. A historical repository that reflects time zones established by governments around the world, Coordinated Universal Time (UTC)
  - There were 2283 updates in the last 26 years.

ANRW

- Limitless HTTP in an HTTPS World: Inferring the Semantics of the HTTPS Protocol without Decryption
  - Can you infer things about the network without decrypting the data?
  - Goal: Given a stream of encrypted TLS applications records, infer:
    - the underlying HTTP frames, and
    - for HEADERS frames, identify fields/values
  - Higher level goals: Use these techniques to improve the detection of
    - Defender: malicious communication/websites, data exfiltration
    - Attacker: blocked domains

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

- "IPv6 Segment Routing Header (SRH)"
  - Last call completed
  - Going over comments
- ICMPv6 errors for discarding packets due to processing limits
  - Most of the errors deal with extension headers. (too long, too many, too many options, etc)

6MAN

- Path MTU Hop-by-Hop Option
  - Another solution because path MTU discovery doesn't work
  - Alternative to sending packet too big message
  - Geoff says there is a 30% failure rate with extension headers.

6MAN

- IPv6 Neighbor Discovery on Wireless Networks
  - Since broadcast can be unreliable over wireless media, DAD often fails to discover duplications
  - The address space is huge so there aren't usually conflicts because of that but not because they're detected.
  - This draft attempts to clean up the chattiness of the IPv6 ND announcements and clean up DAD using abstractions of wireless media.

6MAN

- RFC8200 Fragmentation Errata
  - This has changes to fragmentation to make it better. The header is in the first fragment.
  - How to create the first fragment.
  - Clarification document (hopefully)

6MAN

- Discovering PREF64 in Router Advertisements
  - RA option that allows routers to tell hosts which nat64 prefix to use.
- Change Status of RFC 2675 to Historic
  - Moves IPv6 Jumbograms from proposed standard to historic
  - 65,536 and 4,294,967,295 octets in length
  - Some argument that Jumbograms are optional so who cares?
  - “can we unhistorisize it ?”

6MAN

- IPv6 Support for Segment Routing: SRv6+
  - Traceroute and ping for SR
  - Draft of tools for SR

Network Management RG

- The Network Management Research Group (NMRG) provides a forum for researchers to explore new technologies for the management of the Internet. In particular, the NMRG will work on solutions for problems that are not yet considered well understood enough for engineering work within the IETF.
- The initial focus of the NMRG will be on higher-layer management services that interface with the current Internet management framework. This includes communication services between management systems, which may belong to different management domains, as well as customer-oriented management services. The NMRG is expected to identify and document requirements, to survey possible approaches, to provide specifications for proposed solutions, and to prove concepts with prototype implementations that can be tested in large-scale real-world environments.

NMRG

- Refining Network Intents for Self-Driving Networks
  - Network that runs itself.
  - Intent-based networking (IBN) allows operators to specify high-level policies that dictate how the network should behave without worrying how they are translated into configuration commands in the network devices.
  - https://ccronline.sigcomm.org/wp-content/uploads/2019/02/sigcomm-ccr-final263.pdf

NMRG

- Update on Intent Classification
  - Intent management system has an interface for users to input their requests and the engine translates them into network configuration.
  - Commonly agreed definition, interface, and model of intent

NMRG

- Considerations for intent-based management architecture(s)
  - simplicity, flexibility, extensibility and integrability ?
  - “Not sure the emperor had clothes” – me
- An intent-driven management framework
  - intent- driven management architecture, its key elements, and interfaces.

Source Packet Routing in Networking - ?

- The SPRING working group will define procedures that will allow a node to steer a packet along an explicit route using information attached to the packet and without the need for per-path state information to be held at transit nodes. Full explicit control (through loose or strict path specification) can be achieved in a network comprising only SPRING nodes, however SPRING must inter-operate through loose routing in existing networks and may find it advantageous to use loose routing for other network applications.

- charter-ietf-spring-01

SPRING

- draft-ietf-spring-srv6-network-programming-01
  - Defines the SRv6 Network Programming concept and aims at standardizing the main segment routing functions to enable the creation of interoperable overlays with underlay optimization and service programming.
  - Uses another code point even with other RFCs saying you can't. Lots of folks against this
  - **Their example uses a /32 per router which prompted, "I thought the draft may have confused v4 and v6 because it used a /32 per loopback" I think the authors used a /32 for ease of subnetting v6 but of course that's a crazy example.**

SPRING

- Using DHCP to Manage Node and Ring SID Assignment
  - There are two types of Node and ring segment identifiers (SIDs): those that are locally assigned by the advertising node, such as adjacency and binding SIDs; and those that are globally unique within a given SPRING domain, such as node and ring SIDs. Node SIDs are often manually configured on routers today; this is not only tedious, but error-prone as well; the addition of ring SIDs which must be managed per ring makes manual assignment even more fraught.

SPRING

- Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)
  - All about how to operate and manage segment routing in IPv6.

SPRING

- Other segment routing drafts
  - IPv6 Support for Segment Routing: SRv6+
    - SRv6+ is a Segment Routing (SR) solution that leverages IPv6.
  - TTL Procedures for SR-TE Paths in Label Switched
  - Network Programming Extension: SRv6 uSID Instruction
  - Segment Routing with MPLS Data Plane Encapsulation for In-Situ OAM Data
  - PMS/Head-end based MPLS Ping and Traceroute in Inter-AS SR Networks

NetRqmts BoF – what is it?

- IETF Meeting network requirements
  - What do we really need on the IETF network vs. what we think we need or what we'd like to have because we're geeks?
  - draft-odonoghue-netrqmts
  - Interesting discussion. Even whether IPv6 was on the table.

NetRqmts BoF

- The network for IETF 105
  - Sometimes there are location related challenges
  - Sometimes there are community driven experiments
  - They ship a “scout” ahead of time that advertises the network and straightens out geo-location, etc.
  - Joe’s Magic – automatically configures the switches
  - “access points in elevators”

Inter-Domain Routing (IDR)

The Inter-Domain Routing Working Group is chartered to standardize, develop, and support the Border Gateway Protocol Version 4 (BGP-4) [RFC 4271] capable of supporting policy based routing for TCP/IP internets.

The main objective of the working group is to support the use of BGP-4 by IP version 4 and IP version 6 networks. The working group will also continue to work on improving the robustness and scalability of BGP.

IDR will review extensions made to BGP in other working groups at least at WG document adoption and during working group last calls. The IDR working group will also provide advice and guidance on BGP to other working groups as requested.

IDR

- An Update to BGP-LS Specification (RFC7752bis)
  - This is an update from the many implementations of BGP-LS
  - They are looking for feedback from folks using this code.

IDR

- BGP Path MTU
  - Problems with path MTU and packets too long.
  - Extensions for BGP to carry MTU info

IDR

- BGP based VPN Services over SRv6+ enabled IPv6 networks
  - In pure IPv6 deployments where there may be non-MPLS capable routers, it would be desirable to have alternate mechanism to provide VPN connectivity. This document describes BGP extensions and procedures applicable for SRv6+ enabled IPv6 networks, to provide VPN services over BGP.
- Inter-Domain Traffic Steering with BGP Labeled Colored Unicast (BGP-LCU)
  - Technology that enables signaling of existence of E2E path that satisfy high-level traffic treatment behavior intent.
  - trivial mechanism for passing on colored labeled routes.
  - Simple case of color coordination among ASNs

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.

GROW

- leak-detection-mitigation
  - A new well-known Large Community that provides a way for route leak prevention, detection, and mitigation.
- Support for Local RIB Monitoring Protocol
  - updates the BGP Monitoring Protocol (BMP) RFC 7854 by adding access to the BGP instance Local-RIB, as defined in RFC 4271 the routes that have been selected by the local BGP speaker's Decision Process. These are the routes over all peers, locally originated, and after best-path selection.

GROW

- Other drafts
  - BMP for BGP Route Leak Detection
  - BGP Route policy and Attribute Trace using BMP
  - draft-xu-grow-bmp-route-policy-attr-trace / draft-gu-grow-bmp-route-leak-detection
    - This has codes that will say why a route is not accepted. It was mentioned that this is very costly.

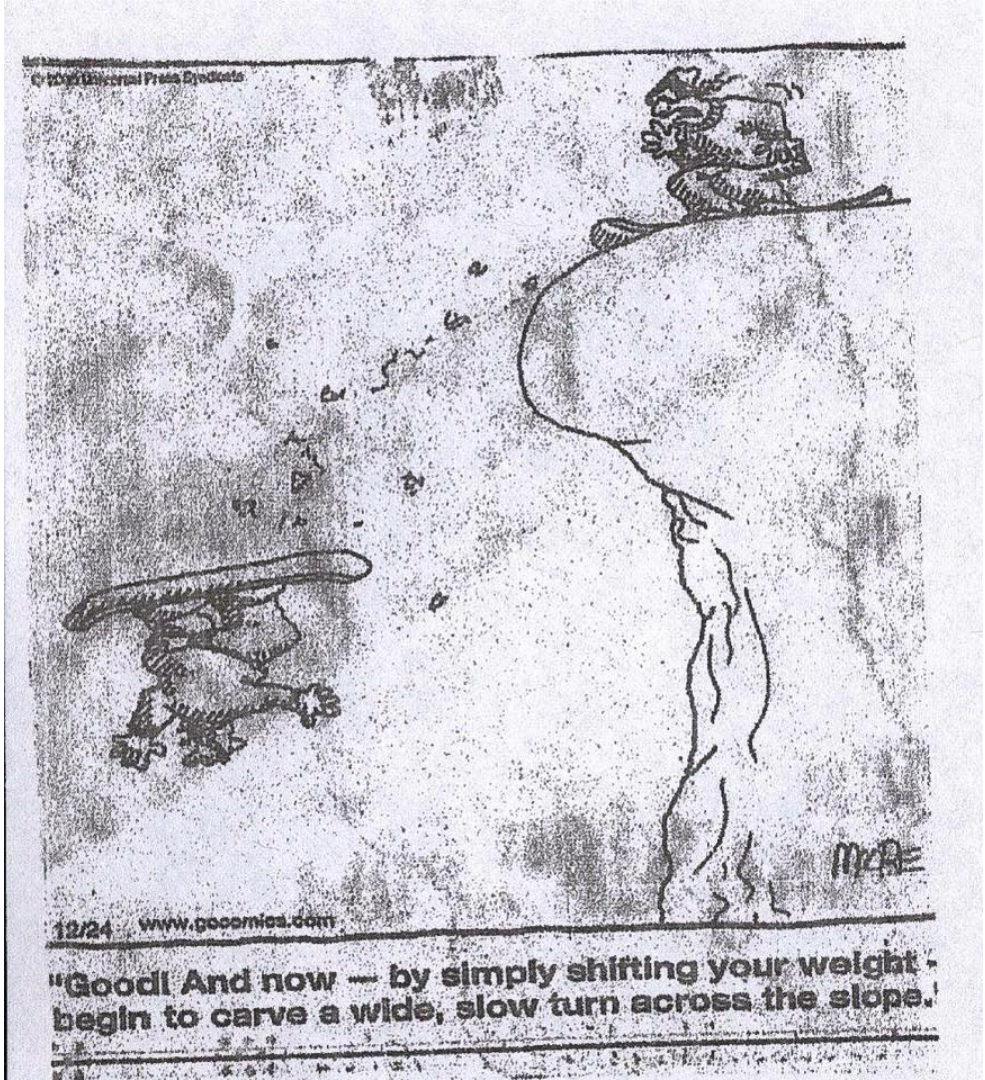
References

- 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?


12/24 www.pocornics.com
"Good! And now — by simply shifting your weight - begin to carve a wide, slow turn across the slope."