The Internet Engineering Task Force

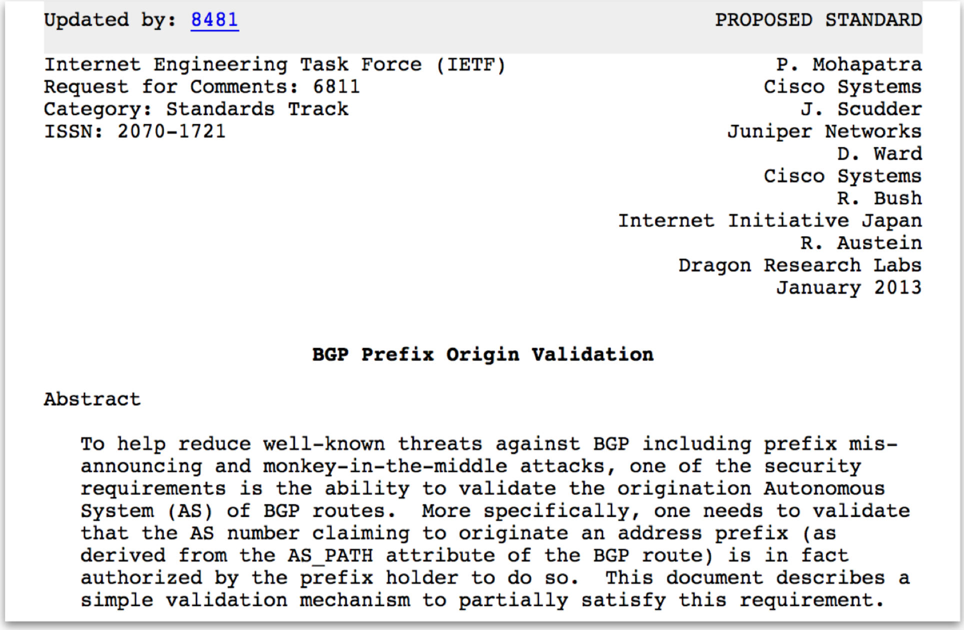
Alissa Cooper
IETF Chair

Making the Internet work better

I E T F®

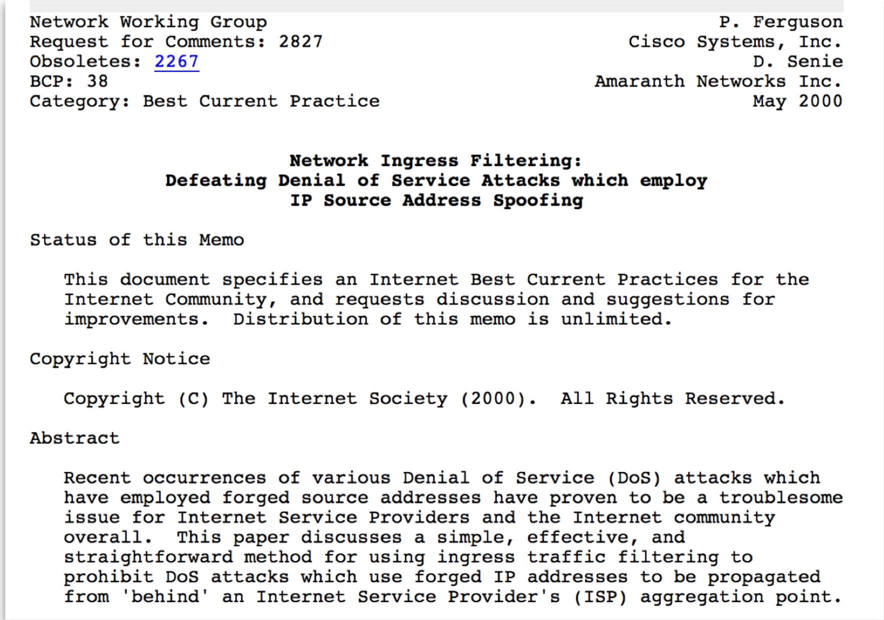
What does the IETF do? Some examples …

RFC 6811



```
Updated by: 8481                                       PROPOSED STANDARD

Internet Engineering Task Force (IETF)                      P. Mohapatra
Request for Comments: 6811                                 Cisco Systems
Category: Standards Track                                     J. Scudder
ISSN: 2070-1721                                         Juniper Networks
                                                                 D. Ward
                                                           Cisco Systems
                                                                 R. Bush
                                               Internet Initiative Japan
                                                              R. Austein
                                                    Dragon Research Labs
                                                            January 2013


                     BGP Prefix Origin Validation

Abstract

   To help reduce well-known threats against BGP including prefix mis-
   announcing and monkey-in-the-middle attacks, one of the security
   requirements is the ability to validate the origination Autonomous
   System (AS) of BGP routes.  More specifically, one needs to validate
   that the AS number claiming to originate an address prefix (as
   derived from the AS_PATH attribute of the BGP route) is in fact
   authorized by the prefix holder to do so.  This document describes a
   simple validation mechanism to partially satisfy this requirement.
```

BCP 38



```
Network Working Group                                        P. Ferguson
Request for Comments: 2827                           Cisco Systems, Inc.
Obsoletes: 2267                                                 D. Senie
BCP: 38                                           Amaranth Networks Inc.
Category: Best Current Practice                                 May 2000


                      Network Ingress Filtering:
           Defeating Denial of Service Attacks which employ
                      IP Source Address Spoofing

Status of this Memo

   This document specifies an Internet Best Current Practices for the
   Internet Community, and requests discussion and suggestions for
   improvements.  Distribution of this memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2000).  All Rights Reserved.

Abstract

   Recent occurrences of various Denial of Service (DoS) attacks which
   have employed forged source addresses have proven to be a troublesome
   issue for Internet Service Providers and the Internet community
   overall.  This paper discusses a simple, effective, and
   straightforward method for using ingress traffic filtering to
   prohibit DoS attacks which use forged IP addresses to be propagated
   from 'behind' an Internet Service Provider's (ISP) aggregation point.
```

IETF Areas

Internet

IPv4, IPv6
DNS, DHCP
6LoWPAN, LPWAN

Routing

BGP, OSPF, IS-IS
MPLS, pseudowire
SFC, NVO3, DETNET

Operations & Management

IPFIX, SNMP
YANG, NETCONF
AAA

Transport

TCP, UDP
QUIC

Applications & Real-Time

HTTP
SMTP, IMAP
SIP, RTP, WebRTC

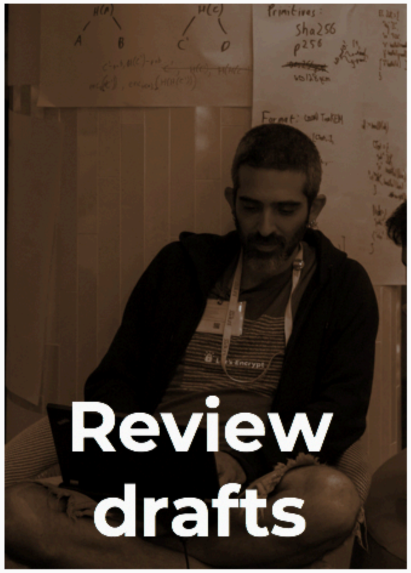
Security

TLS, IPSec, EAP, PKIX

~115 working groups in total

Ways to participate in the IETF

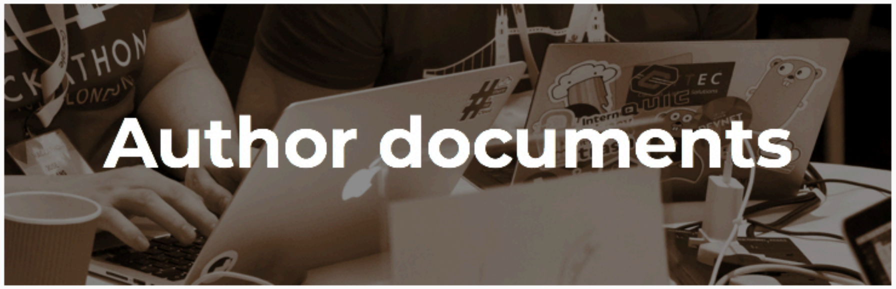
Join mailing lists



Review drafts

Write code

Attend meetings

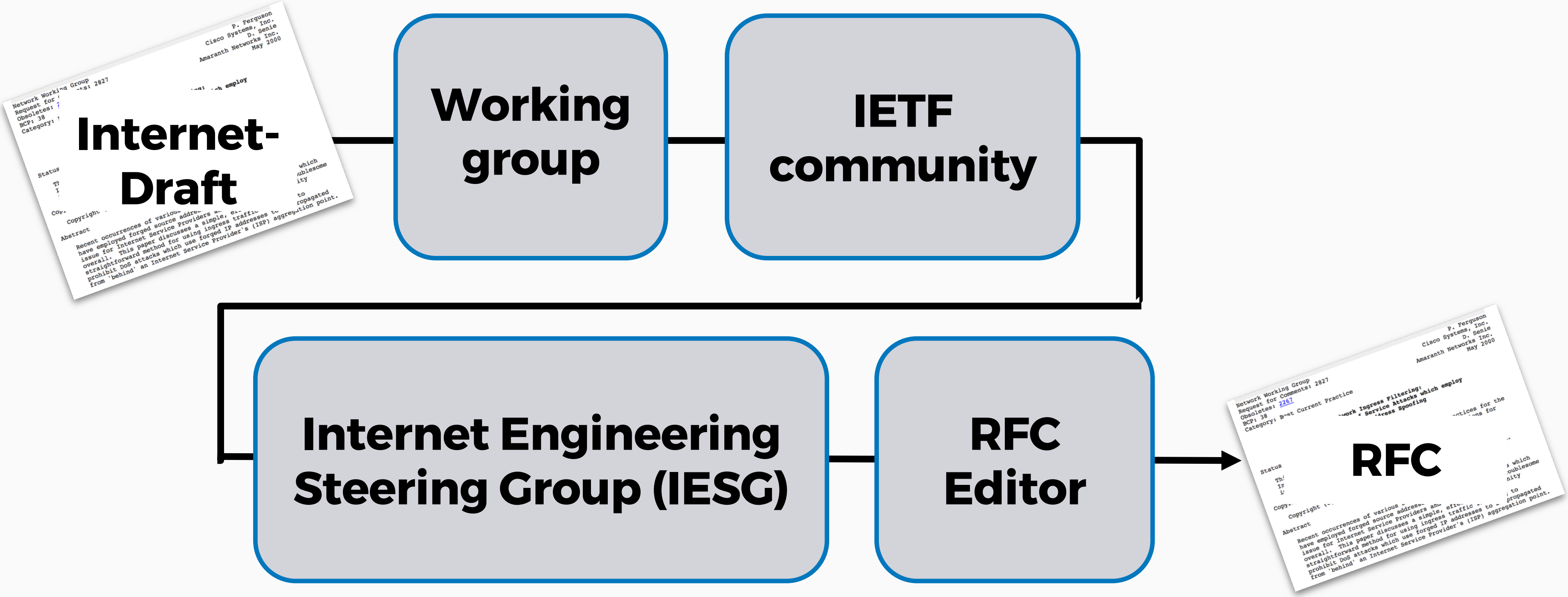


Author documents

Authoring an Internet-Draft in 6 simple steps

1. **Write down your idea.**
2. **Talk to some others about it.**
3. **Get it into Internet-Draft format.**
4. **Submit it to the IETF repository.**
5. **Send a note about it to the relevant mailing list.**
6. **Nurture the draft and its discussion.**

Typical path to RFC



Internet-Draft

Working group

IETF community

Internet Engineering Steering Group (IESG)

RFC Editor

RFC

Resources

- IETF web site: https://www.ietf.org/
- Getting started in the IETF: https://www.ietf.org/about/participate/
- Tao of the IETF: https://www.ietf.org/about/participate/tao/
- Newcomers' tutorials: https://www.ietf.org/about/participate/tutorials/newcomers/
- Working groups (includes chairs' contact information): https://datatracker.ietf.org/wg/
- RFC and Internet-draft search: https://datatracker.ietf.org/

Thank you!

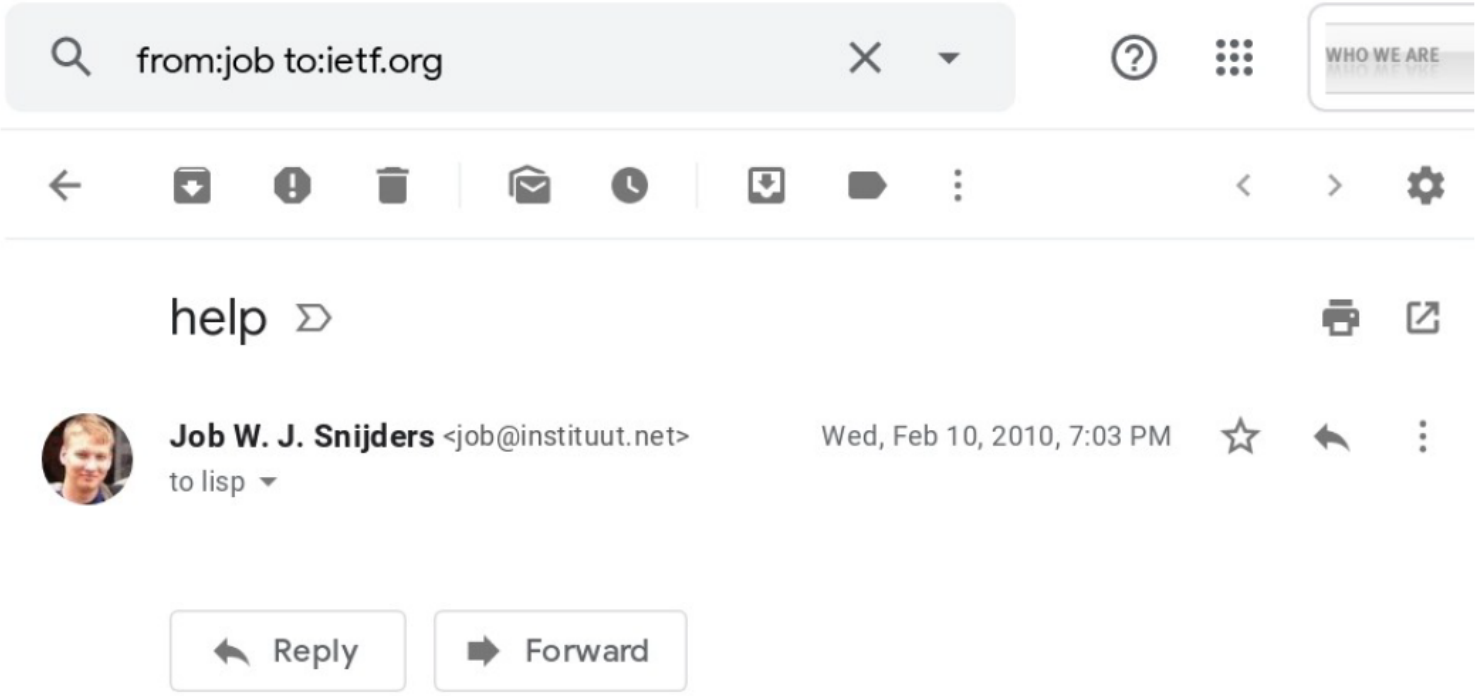
Alissa Cooper
alissa@cooperw.in

Dabbling in IETF

Job Snijders
NTT

LiSP

We all start somewhere



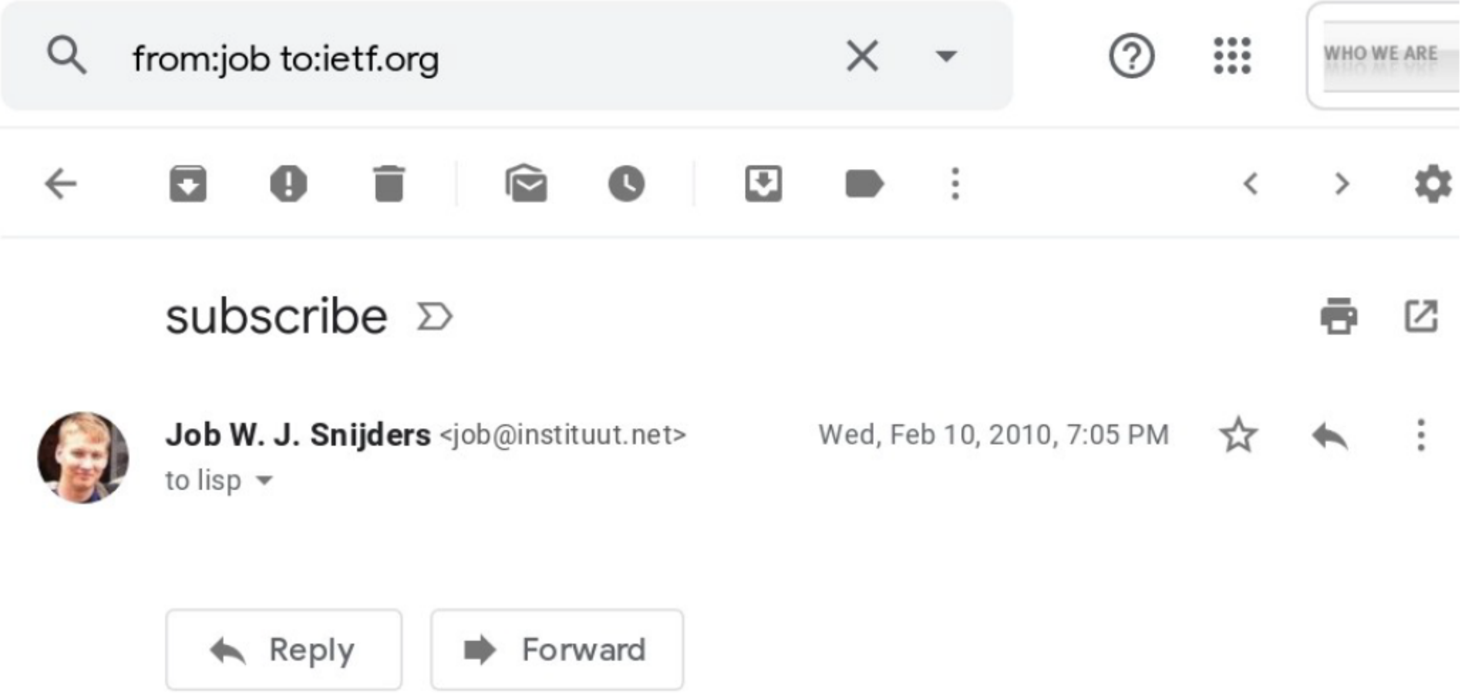
from:job to:ietf.org

help

Job W. J. Snijders <job@instituut.net>
to lisp

Wed, Feb 10, 2010, 7:03 PM

Attempt #2



from:job to:ietf.org

subscribe

Job W. J. Snijders <job@instituut.net>
to lisp

Wed, Feb 10, 2010, 7:05 PM

Second go at IETF: Large BGP Communities

- Identified an operational need (Early 2016), 4 byte ASNs in trouble
- Came up with a fix: Make BGP communities larger
- Implemented this fix in numerous open source projects
- Called all our friends who had $$$ spend with J, C, A, N

http://largebgpcommunities.net/2016/where-did-large-communities-start/

Mr Volk predicted 5 years "if we'd go at full speed". We are now at 2,000 prefixes in DFZ from 500 different origin ASNs!

Personal process take away points

- Perhaps there wasn’t a need to become so upset
- IETF participation definitely helped kick start my career
- It is possible to collaborate with folks who were ‘the enemy’
- IETF has many “products”, some more successful than others: BGP, DNS, IPv4, IPv6, DHCP, HTTP, NTP, etc.

The IETF process actually worked as designed!

Now – taking on responsibility for IETF myself

- Took on chair duties for GROW working group
- Volunteered as member of the 2019-2020 NOMCOM
- …. and happy to talk about mentorship!

If you want things to improve, consider joining!

Internet (INT) Area Intro and Update

IETF Breakout Session

NANOG 77

Introduction

INT is responsible for "IP layer (both IPv4 and IPv6), implications of IPv4 address depletion, co-existence between the IP versions, DNS, DHCP, host and router configuration, mobility, multihoming, identifier-locator separation, VPNs and pseudowires along with related MPLS issues, and various link layer technologies. The Internet Area is also responsible for specifying how IP will run over new link layer protocols."

Area Directors: Suresh Krishnan, Eric Vyncke

https://datatracker.ietf.org/wg/#int
https://trac.ietf.org/trac/int/wiki

- INTAREA
- 6MAN/6LO/6TISCH
- HOMENET
- NTP
- DHC (DHCP)
- DPRIVE/DNSSD
- SOFTWIRE
- Many many many others.

Informal Charter

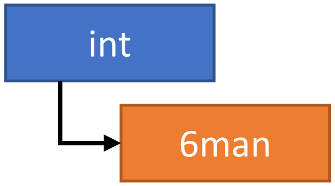
- Responsible for the forwarding plane
  - IP
  - ICMP
- Responsible for a few applications that live close to the forwarding plane
  - DHCP
  - DNS
  - NTP
- Dabble in IP architecture
  - INTAREA WG

Active Working Groups

Abbreviation	Name	Abbreviation	Name
6LO	IPv6 over Networks of Resource-constrained Nodes	HOMENET	Home Networking
6MAN	IPv6 Maintenance	INTAREA	Internet Area Working Group
6TISCH	IPv6 over the TSCH mode of IEEE 802.15.4e	IPWAVE	IP Wireless Access in Vehicular Environments
DHC	Dynamic Host Configuration	LPWAN	IPv6 over Low Power Wide-Area Networks
DMM	Distributed Mobility Management	LWIG	Light-Weight Implementation Guidance
DNSSD	Extensions for Scalable DNS Service Discovery	NTP	Network Time Protocol
PDRIVE	DNS PRIVate Exchange	SOFTWIRES	Softwires
HIP	Host Identity Protocol	TICTOC	Timing over IP Connection and Transfer of Clock

DISCLAIMER

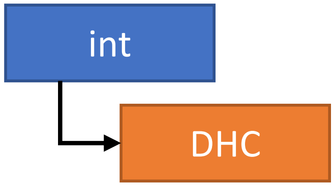
- The INTAREA covers a huge problem space
- Each part of that problem space is of interest to a unique community
  - Wireline, mobile, cloud and enterprise operators
  - Constrained network operators
    - Low power and lossy
  - Special purpose network developers
    - Vehicular networks
- The following slides introduce a few working groups that might be of interest to the NANOG community
  - Non-exhaustive sampling



IPv6 Maintenance

Ongoing work of NANOG interest

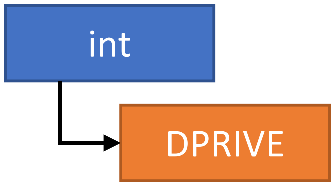
- Working on an IPv6 data plane for SR
  - Draft-ietf-6man-segment-routing-header
  - Draft-ietf-6man-spring-srv6-oam
- Extension Header limits
  - Draft-ietf-6man-icmp-limits
- MTU Discovery
  - Draft-ietf-6man-mtu-option



Dynamic Host Configuration

Ongoing work of NANOG interest

- Work on informational documents providing operational or implementation advice about DHCPv6, as well as documents specifying standard mechanisms for operating, administering and managing DHCPv6 servers, clients, and relay agents
- Assist other WGs and independent submissions in defining options (that follow RFC 7227 guidelines) and to assure DHCP operational considerations are properly documented
- Issue an updated version of the DHCPv6 base specification, and after an appropriate interval following publication, advance to Internet standard



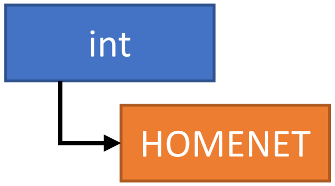
int

DPRIVE

DNS Private Exchange

Ongoing work of NANOG interest

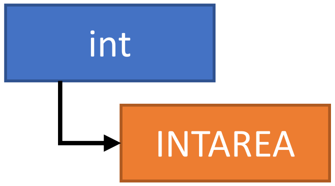
- The DNS PRIVate Exchange (DPRIVE) Working Group develops mechanisms to provide confidentiality to DNS transactions in order to address concerns surrounding pervasive monitoring (RFC 7258).
- Work items
  - Develop requirements for adding confidentiality to DNS exchanges between recursive resolvers and authoritative servers
  - Investigate potential solutions for adding confidentiality to DNS exchanges involving authoritative servers
  - Define, collect and publish performance data measuring effectiveness of DPRIVE-published technologies against pervasive monitoring attacks
  - Document Best Current Practices for operating DNS Privacy services



HOMENET

Ongoing work of NANOG interest

- This working group focuses on the evolving networking technology within and among relatively small "residential home" networks
- Frequent correspondent with Routing Area Babel WG


int

INTAREA

INTAREA

Ongoing work of NANOG interest

- Operational and Architectural Advice
  - Fragmentation Considered Fragile
  - IP Tunnels and The Internet Architecture
- Encapsulations
  - GUE
- ICMP-based OAM Enhancements
  - ICMP PROBE [RFC 8335]
  - ICMP Extensions for Unnumbered Interfaces [RFC 5837]

Summary

- This has been a very small selection of work going on in the IETF.
- Links again:
  https://tools.ietf.org/area/int/
  https://trac.ietf.org/trac/int/wiki

Operations & Management (ops) Area Intro and Update

IETF Breakout Session

NANOG 77

OPS Introduction

Operations and Management Area functions closer to a model of two sub-areas – Operations and Management. Each of the two ADs primarily cover their own sub-area.

OPS part deals with operational and deployment aspects of IETF protocols and technologies.

MGT part deals with evolution of network management architecture and corresponding protocols and models.

Area Directors: Ignas Bagdonas (MGT), Warren Kumari (OPS)

https://datatracker.ietf.org/wg/#ops
https://trac.ietf.org/trac/ops/wiki

- ANIMA
- BMWG
- DIME
- DNSOP
- GROW
- MBONED
- NETCONF
- NETMOD
- OPSAWG
- OPSEC
- RADEXT
- SIDROPS
- V6OPS

OPS area active working groups

ANIMA	Autonomic networking, secure bootstrap, zero touch provisioning.
BMWG	Benchmarking methodology – not the benchmarking itself.
DIME	Diameter protocol maintenance.
DNSOP	DNS deployment and operations practices and methodologies.
GROW	Routing operations, BMP.
MBONED	Multicast deployment.
NETCONF	Model-based manageability – protocols and languages part.
NETMOD	Model-based manageability – modelling part.
OPSAWG	Catch-all group for remaining topics related to operations. Telemetry.
OPSEC	Operational security aspects. RPF, filtering, blackholing.
RADEXT	RADIUS protocol maintenance.
SIDROPS	Secure routing ecosystem deployment aspects.
V6OPS	IPv6 deployment practices and operational aspects.

The Evolution of Network Manageability

- Manageability is essential and yet often overlooked.
- Feature and feature’s manageability parity.
- Configuration vs state vs statistics.
- Manageability and automation.
- Separation and correlation of configuration and state.
- Focus broader than just on a single network element.
- A common schema for networks and network services.
- Focus on software components and not on human operator.
- Feedback loops.
- Intent – what to do vs how to do.

- Models
- Tooling
- Education

Summary

- Operational feedback from the field.
- Modelling work is spread across almost all WGs. The coordination and interworking of resulting models is a problem.
- Practical acceptance by the industry.
- Staying realistic – not possible to represent every technology, service, component, and their interworking as a model.

IETF STATUS UPDATE: ENCRYPTED DNS

DOT, DOH, ADD, & ABCD

David Lawrence <tale.lawrence@oracle.com>
NANOG 77, Austin TX, 29 Oct 2019

TL;DR

- **May 2016**: RFC 7858, Specification for DNS over Transport Layer Security (TLS)
- **Oct 2018:** RFC 8484, DNS Queries over HTTPS (DoH)
- **Jun 2019: add,** Applications Doing DNS -- a Birds-of-a-Feather session, non-working-group-forming
- **Nov 2019:** abcd, Application Behavior Considering DNS **--** a Birds-of-a-Feather session, wg-forming

Pretty straightforward stuff, not much to see here.

I yield the remainder of my time.

A NEARLY NEUTRAL STATUS REPORT

Not evangelizing for the adoption of any particular technology

- I personally do not agree with everything that’s happened in the space
- The IETF leadership do not all agree on what’s happened or should happen next
- External communities also do not agree
- Some of this talk might sound like advocacy, but the devil is in the details

HOW DID WE GET HERE?

We have to go back a ways for the full context

- **4 Billion BCE:** Life appears on earth
- **240 Million BCE:** Then there were dinosaurs
- **200 Thousand BCE:** *Homo sapiens sapiens* appears

… and that’s when things really got complicated

FAST FORWARDING A BIT

Insert 200,000 years of wooshing noise here.

- April 2003: RFC 3514, The Security Flag in the IPv4 Header
  - Steve Bellovin proposed the Evil Bit for signalling good and evil Internet traffic
  - IETF Fun Fact: this RFC has published errata as recently as 2018
- June 2013: Edward Snowden leaks information about global surveillance of the Internet
- November 2013: IETF response to the Snowden revelations starts taking shape

MAY 2014: RFC 7258

PERVASIVE MONITORING IS AN ATTACK

The IETF community's technical assessment is that PM [Pervasive Monitoring] is an attack on the privacy of Internet users and organisations … that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible.

[W]e cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider them to be, since the actions required of the attacker are indistinguishable from other attacks. The motivation for PM is, therefore, not relevant for how PM is mitigated in IETF protocols.

OCTOBER 2014: DPRIVE

DNS PRIVATE EXCHANGE WORKING GROUP

The initial focus of this Working Group was the development of mechanisms that provide confidentiality and authentication between DNS Clients and Iterative Resolvers (published as RFCs 7858 [DNS over TLS] and
8094 [DNS over DTLS])

- To date there has been trivial uptake of 7858 and, as far as I know, none of 8094
- Group re-chartered to work on securing the resolver to authoritative channel
- DNS over QUIC would also be in scope

SEPT 2017: DOH

DNS-OVER-HTTPS WORKING GROUP

- Limited charter scope, intended partly as a new model of “pop-up” working group
- Focused on the technical aspects of tunneling DNS requests in HTTPS
- Discovery mechanisms potentially in-scope, but orthogonal to tunneling
- Published RFC 8484, DNS Queries over HTTPS, to universal acclaim
    - … no wait, that’s not right
- Currently dormant awaiting IETF consensus about how to proceed in this space

JUNE 2018: ADD

APPLICATIONS DOING DNS, A BOF

- DoH immediately triggered broader discussion of DNS client/resolver architecture
- Vendor experiments – yes, mostly Mozilla and Cloudflare – provoked strong reaction
- As some declared the Death of DNS, the “anger and bargaining” stage came on quickly
- BoF sought to identify what technical work the IETF might be able to reach consensus on

This brings us up-to-date with what’s happened so far

WHY DID THE IETF ADOPT DOH?

- The process for bringing new work was followed
- Proponents had multiple motivations, at least some consistent with IETF goals
- The general idea of it was already in the wild
- The IETF not working on a protocol is not equivalent to it not being worked on
- IETF processes tend to bring about better engineering results

POINTS TO REMEMBER

DoT and DoH only provide encrypted channels, they do not fundamentally change the DNS

Some deployment models **DO** significantly change the DNS architecture but are not intrinsic to the protocols

WHAT’S NEXT FOR THE IETF?

- Continue to embrace the multistakeholder process
- abcd (Application Behavior Considering DNS) BoF in a few weeks to plan the next steps for technical standards, including:
  - Resolver discovery
  - Resolver policy expression / characterization
  - Operations in an environment of expanded resolver choice
  - Other general operational recommendations
- Make clear what aspects the IETF can’t address as a technical standards organization
  - Especially that the deployment choices of individual companies is outside our control

If the outcome of this process is important to you, **PLEASE PARTICIPATE**