INTRAREDE 2021

"Novos padrões, tecnologias e desafios na Internet: o que vem acontecendo no IETF e fóruns técnicos internacionais?"

Raphael Vicente Rosa

15 de Dezembro de 2021

Internet Engineering Task Force (IETF) - Quick Highlights

- "*The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications.*"
- Final document: Request For Comments (RFC) - "Internet Standard"
  - IPv4, IPv6, DNS, etc
- The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force
  - https://www.ietf.org/about/participate/tao/
- Internet Research Task Force (IRTF)
- Hackathon ("running code")

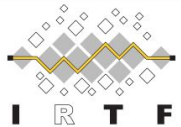
IETF Areas and Working Groups

Area	Description
Applications and Real-Time Area (art)	Protocols seen by user programs, such as email and the web and delay-sensitive interpersonal communications
General (gen)	IETF process, and catch-all for WGs that don't fit in other Areas (which is very few)
Internet (int)	Different ways of moving IP packets and DNS information
Operations and Management (ops)	Network management, AAA, and various operational issues facing the Internet
Routing (rtg)	Getting packets to their destinations
Security (sec)	Privacy, integrity, authentication, non-repudiation, confidentiality, and access control
Transport (tsv)	Transport for large volumes of traffic at potentially high bandwidths

IRTF Research Groups

IRTF Research Groups Workshops and Prizes People Policies

IRTF Research Groups



Current Research Groups

These 14 Research Groups are currently chartered:

CFRG
Crypto Forum Research Group

COINRG
Computation in the Network Research Group

DINRG
Decentralized Internet Infrastructure Research Group

GAIA
Global Access to the Internet for All Research Group

HRPC
Human Rights Protocol Considerations Research Group

ICCRG
Internet Congestion Control Research Group

ICNRG
Information-Centric Networking Research Group

MAPRG
Measurement and Analysis for Protocols Research Group

NMRG
Network Management Research Group

NWCRG
NetWork Coding for Efficient Network Communications Research Group

PANRG
Path Aware Networking Research Group

PEARG
Privacy Enhancements and Assessments Research Group

QIRG
Quantum Internet Research Group

T2TRG
Thing-to-Thing Research Group

New Proposed Research Groups

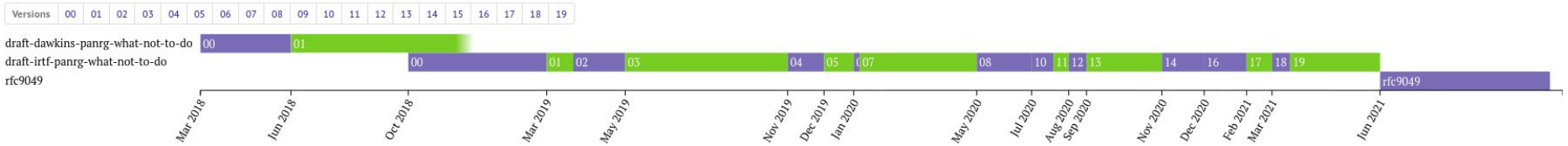
Life Cycle of a I-D Towards an RFC

1. Publish the document as an Internet-Draft.
2. Receive comments on the draft.
3. Edit your draft based on the comments.
4. Repeat steps 1 through 3 a few times.
5. Ask an Area Director to take the draft to the IESG (if it's an individual submission). If the draft is an official Working Group product, the WG chair asks the AD to take it to the IESG.
6. If the Area Director accepts the submission, they will do their own initial review, and maybe ask for updates before they move it forward.
7. Get reviews from the wider IETF membership. In particular, some of the Areas in the IETF have formed review teams to look over drafts that are ready to go to the IESG.
8. Discuss concerns with the IESG members. Their concerns might be resolved with a simple answer, or they might require additions or changes to the document.
9. Wait for the document to be published by the RFC Editor.

Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)

RFC 9049

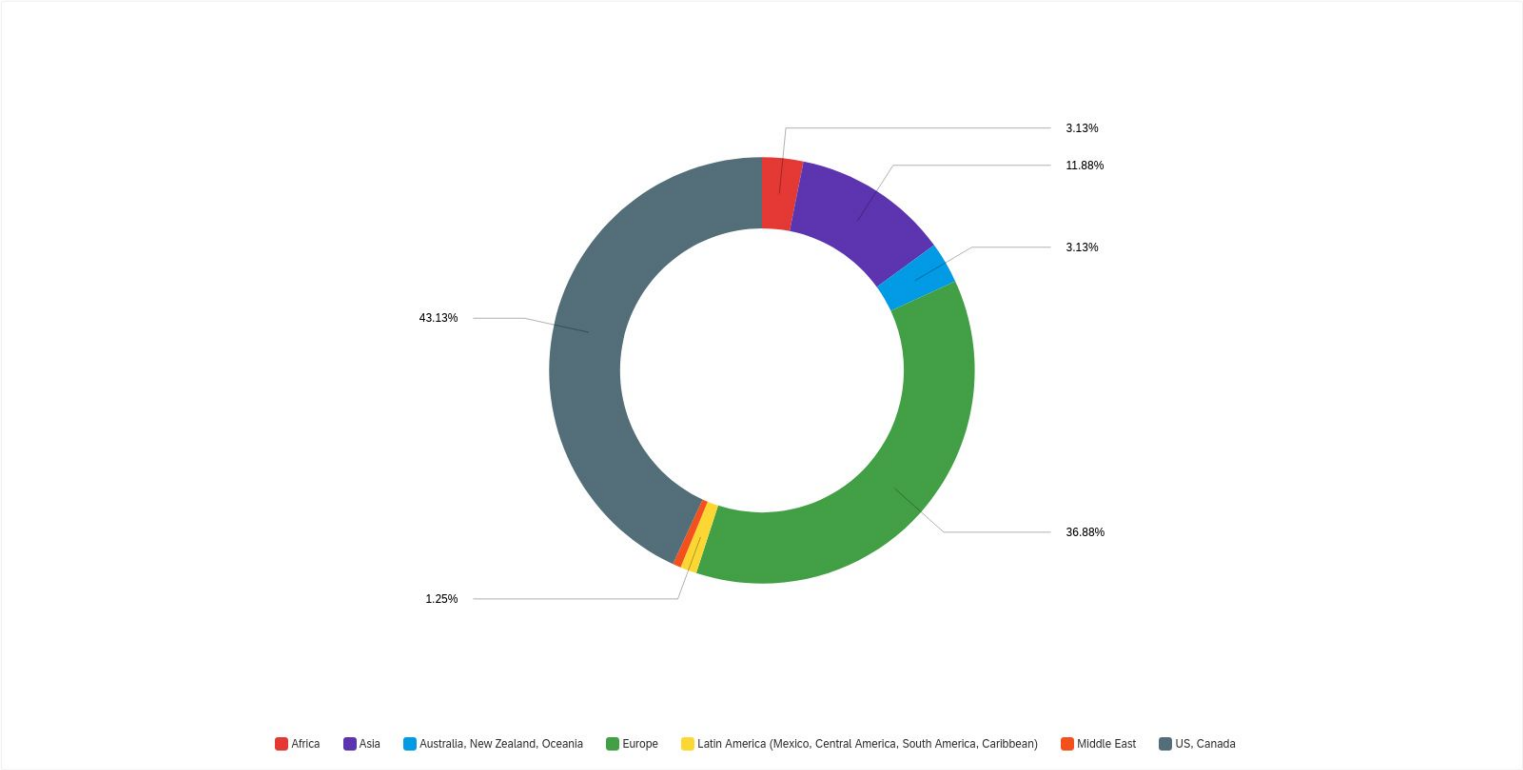
Status | IRSG evaluation record | IESG evaluation record | IESG writeups | Email expansions | History



Document	**Type**	RFC - Informational (June 2021; No errata) Was draft-irtf-panrg-what-not-to-do (panrg RG)
	Author	Spencer Dawkins
	Last updated	2021-06-25
	Replaces	draft-dawkins-panrg-what-not-to-do
	Stream	Internet Research Task Force (IRTF)
	Formats	plain text, html, xml, pdf, htmlized, bibtex
	IETF conflict review	conflict-review-irtf-panrg-what-not-to-do
Stream	**IRTF state**	Published RFC
	Consensus Boilerplate	Yes
	Document shepherd	Jen Linkova
	Shepherd write-up	Show (last changed 2020-08-23)
IESG	**IESG state**	RFC 9049 (Informational)
	Telechat date	
	Responsible AD	(None)
	Send notices to	Jen Linkova <furry13@gmail.com>
IANA	**IANA review**	Version Changed - Review Needed

IETF #112 Survey

Q1 - In what region do you live?



IETF 112 Survey

Q4 - How many IETF Meetings have you participated in? (including this meeting)

Field	Choice Count
1	4.38% 7
2-5	14.37% 23
6-10	15.00% 24
11+	66.25% 106
	160

Showing rows 1 - 5 of 5

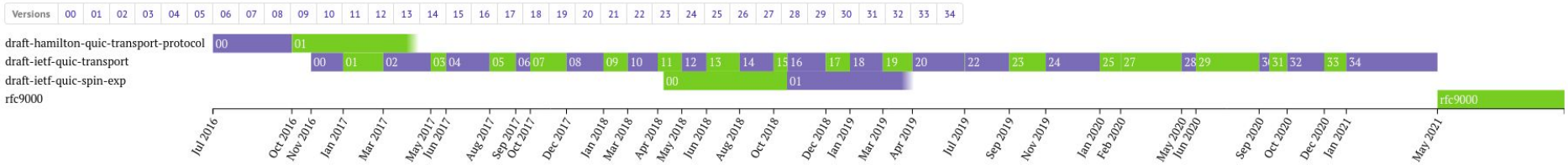
Interesting IETF Activities

- QUIC: A UDP-Based Multiplexed and Secure Transport (RFC 9000)
- Security & privacy (e.g., TLS 1.3)
- Automated network management
- Internet of Things
- Deterministic Networks

QUIC: A UDP-Based Multiplexed and Secure Transport

RFC 9000

Status | IESG evaluation record | IESG writeups | Email expansions | History



Document	**Type**	RFC - Proposed Standard (May 2021; No errata) Was draft-ietf-quic-transport (quic WG)
	Authors	Jana Iyengar, Martin Thomson
	Last updated	2021-05-27
	Replaces	draft-hamilton-quic-transport-protocol, draft-ietf-quic-spin-exp
	Stream	Internet Engineering Task Force (IETF)
	Formats	plain text, html, xml, pdf, htmlized, bibtex
	Reviews	GENART Telechat Review (of -33): Ready INTDIR Telechat Review (of -33): Ready OPSDIR Last Call Review (of -32): Ready GENART Last Call Review (of -32): Ready with Issues
Stream	**WG state**	Submitted to IESG for Publication
	Document shepherd	Lars Eggert
	Shepherd write-up	Show (last changed 2020-09-25)
IESG	**IESG state**	RFC 9000 (Proposed Standard)
	Action Holders	(None)
	Consensus Boilerplate	Yes

Transport Layer Security (tls)

Document	Date	Status	IPR	AD / Shepherd
Active Internet-Drafts (16 hits)				
draft-ietf-tls-cross-sni-resumption-02 **Transport Layer Security (TLS) Resumption across Server Names**	2021-12-05 6 pages New	I-D Exists Waiting for WG Chair Go-Ahead		Christopher Wood
draft-ietf-tls-ctls-04 **Compact TLS 1.3**	2021-10-25 17 pages	I-D Exists WG Document		Christopher Wood
draft-ietf-tls-dtls-connection-id-13 **Connection Identifiers for DTLS 1.2**	2021-06-22 18 pages	RFC Ed Queue : AUTH48 AUTH48 for 175 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir		Benjamin Kaduk Joseph Salowey
draft-ietf-tls-dtls-rrc-02 **Return Routability Check for DTLS 1.2 and DTLS 1.3**	2021-11-26 10 pages	I-D Exists WG Document		
draft-ietf-tls-dtls13-43 **The Datagram Transport Layer Security (DTLS) Protocol Version 1.3**	2021-04-30 71 pages	RFC Ed Queue : AUTH48 AUTH48 for 225 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, tsvart		Benjamin Kaduk Sean Turner
draft-ietf-tls-esni-13 **TLS Encrypted Client Hello**	2021-08-12 48 pages	I-D Exists WG Document *Mar 2021*		
draft-ietf-tls-exported-authenticator-14 **Exported Authenticators in TLS**	2021-01-25 14 pages	Approved-announcement to be sent::Revised I-D Needed for 250 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir Action Holders: Nick Sullivan for 250 days		Roman Danyliw Sean Turner
draft-ietf-tls-external-psk-guidance-04 **Guidance for External PSK Usage in TLS**	2021-12-09 16 pages New	IESG Evaluation for 5 days IESG telechat: 2021-12-16 Submitted to IESG for Publication: Informational Reviews: artart, genart, opsdir, secdir Action Holders: Benjamin Kaduk		Benjamin Kaduk Sean Turner
draft-ietf-tls-external-psk-importer-06 **Importing External PSKs for TLS**	2020-12-03 11 pages	Approved-announcement to be sent::Revised I-D Needed for 293 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir *Jan 2021*		Roman Danyliw Joseph Salowey
draft-ietf-tls-hybrid-design-03	2021-07-13	I-D Exists		Christopher Wood

Autonomic Networking Integrated Model and Approach (anima)

“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.”

RFCs (8 hits)			
RFC 8366 *(was draft-ietf-anima-voucher)* **A Voucher Artifact for Bootstrapping Protocols**	Errata	2018-05 23 pages	Proposed Standard RFC
RFC 8368 *(was draft-ietf-anima-stable-connectivity)* **Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)**		2018-05 24 pages	Informational RFC
RFC 8990 *(was draft-ietf-anima-grasp)* **GeneRic Autonomic Signaling Protocol (GRASP)**		2021-05 55 pages	Proposed Standard RFC
RFC 8991 *(was draft-ietf-anima-grasp-api)* **GeneRic Autonomic Signaling Protocol Application Program Interface (GRASP API)**		2021-05 29 pages	Informational RFC
RFC 8992 *(was draft-ietf-anima-prefix-management)* **Autonomic IPv6 Edge Prefix Management in Large-Scale Networks**	Errata	2021-05 19 pages	Informational RFC
RFC 8993 *(was draft-ietf-anima-reference-model)* **A Reference Model for Autonomic Networking**		2021-05 26 pages	Informational RFC
RFC 8994 *(was draft-ietf-anima-autonomic-control-plane)* **An Autonomic Control Plane (ACP)**		2021-05 128 pages	Proposed Standard RFC
RFC 8995 *(was draft-ietf-anima-bootstrapping-keyinfra)* **Bootstrapping Remote Secure Key Infrastructure (BRSKI)**	Errata	2021-05 116 pages	Proposed Standard RFC

IoT Related RFCs

INFORMATIONAL

Internet Research Task Force (IRTF)
Request for Comments: 8576
Category: Informational
ISSN: 2070-1721

O. Garcia-Morchon
Philips
S. Kumar
Signify
M. Sethi
Ericsson

April 2019

Internet of Things (IoT) Security: State of the Art and Challenges

Abstract

The Internet of Things (IoT) concept refers to the usage of standard Internet protocols to allow for human-to-thing and thing-to-thing communication. The security needs for IoT systems are well recognized, and many standardization steps to provide security have been taken -- for example, the specification of the Constrained Application Protocol (CoAP) secured with Datagram Transport Layer Security (DTLS). However, security challenges still exist, not only because there are some use cases that lack a suitable solution, but also because many IoT devices and systems have been designed and deployed with very limited security capabilities. In this document, we first discuss the various stages in the lifecycle of a thing. Next, we document the security threats to a thing and the challenges that one might face to protect against these threats. Lastly, we discuss the next steps needed to facilitate the deployment of secure IoT systems. This document can be used by implementers and authors of IoT specifications as a reference for details about security considerations while documenting their specific security challenges, threat models, and mitigations.

This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).

Internet Engineering Task Force (IETF)
Request for Comments: 8520
Category: Standards Track
ISSN: 2070-1721

E. Lear
Cisco Systems
R. Droms
Google
D. Romascanu

March 2019

Manufacturer Usage Description Specification

Abstract

This memo specifies a component-based architecture for Manufacturer Usage Descriptions (MUDs). The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. Later work can delve into other aspects.

This memo specifies two YANG modules, IPv4 and IPv6 DHCP options, a Link Layer Discovery Protocol (LLDP) TLV, a URL, an X.509 certificate extension, and a means to sign and verify the descriptions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8520.

Birds-of-a-feather (BOF) Groups

Birds-of-a-feather (BOF) groups

Groups in the *BOF* state.

BOF	Name	Date
priv	Privacy Respecting Incorporation of Values	2021-11-08

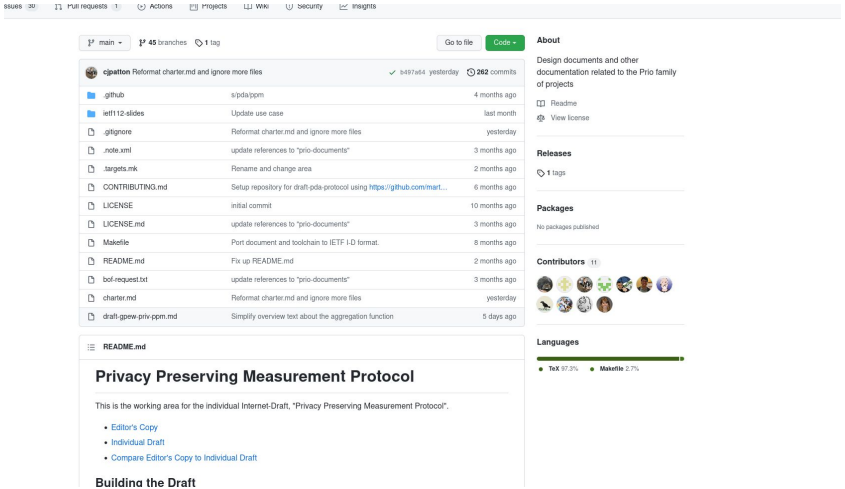
Workgroup: Network Working Group
Internet-Draft: draft-gpew-priv-ppm-00
Published: 25 October 2021
Intended Status: Standards Track
Expires: 28 April 2022
Authors: T. Geoghegan *ISRG*; C. Patton *Cloudflare*; E. Rescorla *Mozilla*; C.A. Wood *Cloudflare*

Privacy Preserving Measurement

Abstract

There are many situations in which it is desirable to take measurements of data which people consider sensitive. In these cases, the entity taking the measurement is usually not interested in people's individual responses but rather in aggregated data. Conventional methods require collecting individual responses and then aggregating them, thus representing a threat to user privacy and rendering many such measurements difficult and impractical. This document describes a multi-party privacy preserving measurement (PPM) protocol which can be used to collect aggregate data without revealing any individual user's data.

Table of Contents



Operator's Perspective

Operations and Management Area (ops)

ops Area Directors (ADs)

Warren Kumari
Robert Wilton

ops area-specific web pages

Issuer Tracker
Mailing List
Wiki

ops active WGs (15)

Group	Responsible AD	Name	Chairs
anima	Robert	Autonomic Networking Integrated Model and Approach	Toerless Eckert, Sheng Jiang
bmwg	Warren	Benchmarking Methodology	Sarah Banks, Al Morton
dime	Robert	Diameter Maintenance and Extensions	Jouni Korhonen, Lionel Morand
dnsop	Warren	Domain Name System Operations	Benno Overeinder, Tim Wicinski, Suzanne Woolf
grow	Warren	Global Routing Operations	Chris Morrow, Job Snijders
iotops	Warren	IOT Operations	Henk Birkholz, Alexey Melnikov
mboned	Warren	MBONE Deployment	Lenny Giuliano, Greg Shepherd
mops	Éric	Media OPerationS	Leslie Daigle, Kyle Rose (Assigned AD: Éric Vyncke)
netconf	Robert	Network Configuration	Mahesh Jethanandani, Kent Watsen
netmod	Robert	Network Modeling	Lou Berger, Joel Jaeggli, Kent Watsen
opsawg	Robert	Operations and Management Area Working Group	Henk Birkholz, Joe Clarke, Tianran Zhou
opsec	Warren	Operational Security Capabilities for IP Network Infrastructure	Ron Bonica, Jen Linkova
radext	Benjamin	RADIUS EXTensions	Lionel Morand, Stefan Winter (Assigned AD: Benjamin Kaduk)
sidrops	Warren	SIDR Operations	Chris Morrow, Keyur Patel
v6ops	Warren	IPv6 Operations	Fred Baker, Ron Bonica

Workgroup: Domain Name System Operations
Internet-Draft: draft-ietf-dnsop-dns-tcp-requirements-14
Updates: 1123, 1536 (if approved)
Published: 7 December 2021
Intended Status: Best Current Practice
Expires: 10 June 2022
Authors: J.T. Kristoff *DataPlane.org*
D. Wessels *Verisign*

DNS Transport over TCP - Operational Requirements

Abstract

This document updates RFC 1123 and RFC 1536. This document requires the operational practice of permitting DNS messages to be carried over TCP on the Internet as a Best Current Practice. This operational requirement is aligned with the implementation requirements in RFC 7766. The use of TCP includes both DNS over unencrypted TCP, as well as over an encrypted TLS session. The document also considers the consequences of this form of DNS communication and the potential operational issues that can arise when this Best Current Practice is not upheld.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 June 2022.

Copyright Notice

Table of Contents

draft-ietf-netconf-udp-notif-04 **UDP-based Transport for Configured Subscriptions**		2021-10-21 22 pages	I-D Exists WG Document	
RFCs (27 hits)				
RFC 4741 *(was draft-ietf-netconf-prot)* **NETCONF Configuration Protocol**	Errata	2006-12 95 pages	Proposed Standard RFC Obsoleted by RFC 6241	Dan Romascanu
RFC 4742 *(was draft-ietf-netconf-ssh)* **Using the NETCONF Configuration Protocol over Secure SHell (SSH)**	Errata	2006-12 10 pages	Proposed Standard RFC Obsoleted by RFC 6242	Dan Romascanu
RFC 4743 *(was draft-ietf-netconf-soap)* **Using NETCONF over the Simple Object Access Protocol (SOAP)**		2006-12 20 pages	Historic RFC Updated by RFC 8996	
RFC 4744 *(was draft-ietf-netconf-beep)* **Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)**		2006-12 10 pages	Historic RFC Updated by RFC 8996	Dan Romascanu
RFC 5277 *(was draft-ietf-netconf-notification)* **NETCONF Event Notifications**		2008-07 35 pages	Proposed Standard RFC	Dan Romascanu
RFC 5539 *(was draft-ietf-netconf-tls)* **NETCONF over Transport Layer Security (TLS)**		2009-05 7 pages	Proposed Standard RFC Obsoleted by RFC 7589	Dan Romascanu
RFC 5717 *(was draft-ietf-netconf-partial-lock)* **Partial Lock Remote Procedure Call (RPC) for NETCONF**	Errata	2009-12 23 pages	Proposed Standard RFC	Dan Romascanu
RFC 6022 *(was draft-ietf-netconf-monitoring)* **YANG Module for NETCONF Monitoring**	Errata	2010-10 28 pages	Proposed Standard RFC	Dan Romascanu
RFC 6241 *(was draft-ietf-netconf-4741bis)* **Network Configuration Protocol (NETCONF)**	Errata	2011-06 113 pages	Proposed Standard RFC Updated by RFC 7803, RFC 8526	1 Dan Romascanu
RFC 6242 *(was draft-ietf-netconf-rfc4742bis)* **Using the NETCONF Protocol over Secure Shell (SSH)**		2011-06 11 pages	Proposed Standard RFC	Dan Romascanu
RFC 6243 *(was draft-ietf-netconf-with-defaults)* **With-defaults Capability for NETCONF**	Errata	2011-06 26 pages	Proposed Standard RFC	Dan Romascanu
RFC 6470 *(was draft-ietf-netconf-system-notifications)* **Network Configuration Protocol (NETCONF) Base Notifications**	Errata	2012-02 15 pages	Proposed Standard RFC	Dan Romascanu
RFC 6536 *(was draft-ietf-netconf-access-control)* **Network Configuration Protocol (NETCONF) Access Control Model**	Errata	2012-03 49 pages	Proposed Standard RFC Obsoleted by RFC 8341	Dan Romascanu
RFC 7589 *(was draft-ietf-netconf-rfc5539bis)* **Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication**		2015-06 11 pages	Proposed Standard RFC	Benoît Claise Mehmet Ersue
RFC 7895 *(was draft-ietf-netconf-yang-library)* **YANG Module Library**		2016-06 13 pages	Proposed Standard RFC Obsoleted by RFC 8525	Benoît Claise Mahesh Jethanandani
RFC 8040 *(was draft-ietf-netconf-restconf)* **RESTCONF Protocol**	Errata	2017-01 137 pages	Proposed Standard RFC Updated by RFC 8527	Benoît Claise Mehmet Ersue

main | 2 branches | 0 tags | Go to file | Code

lllyfeng Update README.md — 16a5c7b on Nov 1 — 48 commits

ansible_gen	update gen_examples.py	last month
.gitignore	init version	3 months ago
LICENSE	init version	3 months ago
MANIFEST.in	update version and README.md,adding templates to dist	2 months ago
README.md	Update README.md	last month
requirements.txt	init version	3 months ago
setup.py	update version	2 months ago

README.md

ansible-gen

Overview

ansible-gen is an automatic code generation tool for ansible modules according to YANG modules and some user-specified files which is designed to managemant the devices through NETCONF.

Installation

Prerequisites

- OS: Windows,Red Hat,Ubuntu,CentOS,OS X,BSD,Suse
- Python: Python2/Python3(greater than python2.7 is preferred)

About

a tool to generate ansible API automatically for huawei net-engine ansible plugin

Readme

View license

Releases

No releases published

Packages

No packages published

Contributors 2

lllyfeng frank feng

QiufangMa Qiufang Ma

Languages

Python 98.0% **HTML** 1.6%

Shell 0.4%

Draft Operators and the IETF

Versions: 00

Network Working Group — C. Grundemann
Internet-Draft — J. Zorz
Intended status: Informational — Internet Society
Expires: May 1, 2015 — October 28, 2014

Operators and the IETF
draft-opsawg-operators-ietf-00

Abstract

Internet Society has launched a new project to address the perceived gap between Operators and the IETF. The objective of this project is ultimately to facilitate communications between the operator community and the IETF to help ensure that operational realities inform the development of key standards. The first phase of this project was a survey of the operator community that was conducted over the first half of 2014. This I-D aims to synthesize the initial survey results, along with information we collected directly from operators during the survey window. The primary purpose of doing this is to start a conversation which we hope will lead to increases in the level of operational input and feedback to the IETF standards making process.

An Overview of the draft Operators and the IETF

- Challenges
  - Time
    - 72% of respondents who do not participate in IETF mailing lists say they don't participate because they don't have enough time
  - Culture
    - "The IETF is not really focused towards operations and, historically, operator input has not been well received."
  - Money
    - "It is too expensive to attend regularly. It is not my primary job to attend IETF meetings, so is secondary to other things."
  - Awareness
    - "No awareness of how I can help, what I can do, and where my goals would align with the IETF."

- Solutions
  - Communication
    - "Quarterly summaries for those that are not able to attend."
    - "Offer communications options other than e-mail."
  - Outreach
    - "More liaisons between the IETF and Operator forums"
    - "Promote the IETF impact and role of standards to large operators
    - (education)."
  - Inclusion
    - "Introduce works in multi language."
    - "Make remote participation easier."

Recommendations

https://www.ietf.org/about/participate/tao/

https://www.ietf.org/how/runningcode/hackathons/

https://blog.apnic.net/2021/11/23/more-notes-from-ietf-112/

Obrigado!

The views and opinions expressed here are those of the author and do not necessarily reflect the official policy or position of his employer.