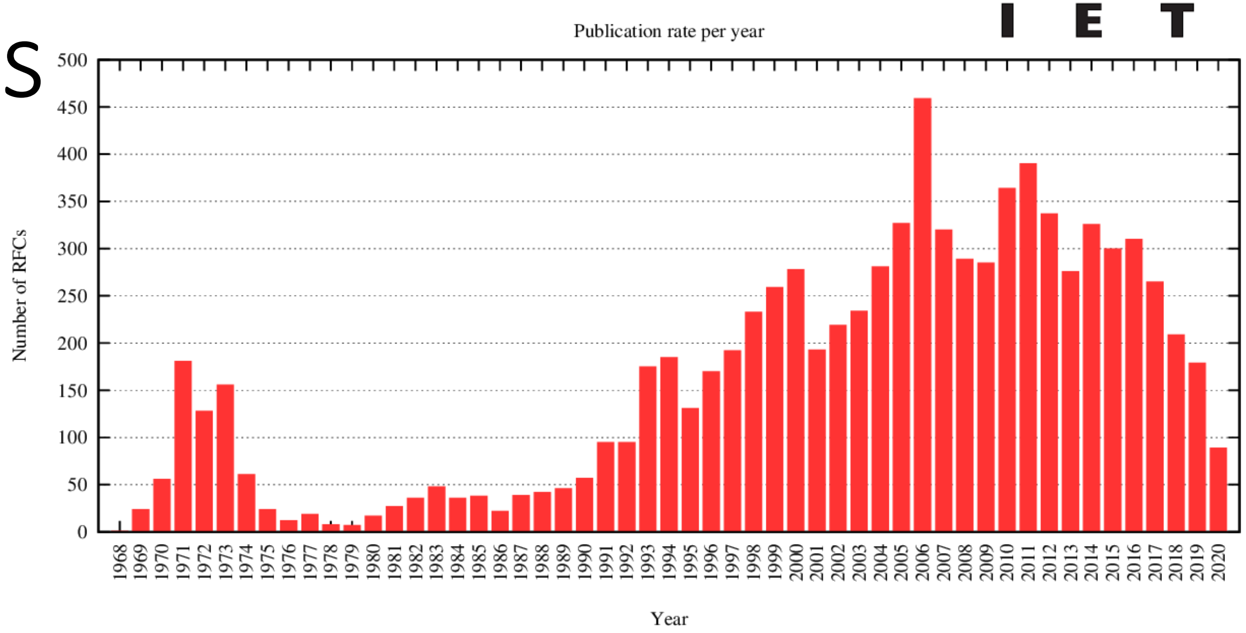
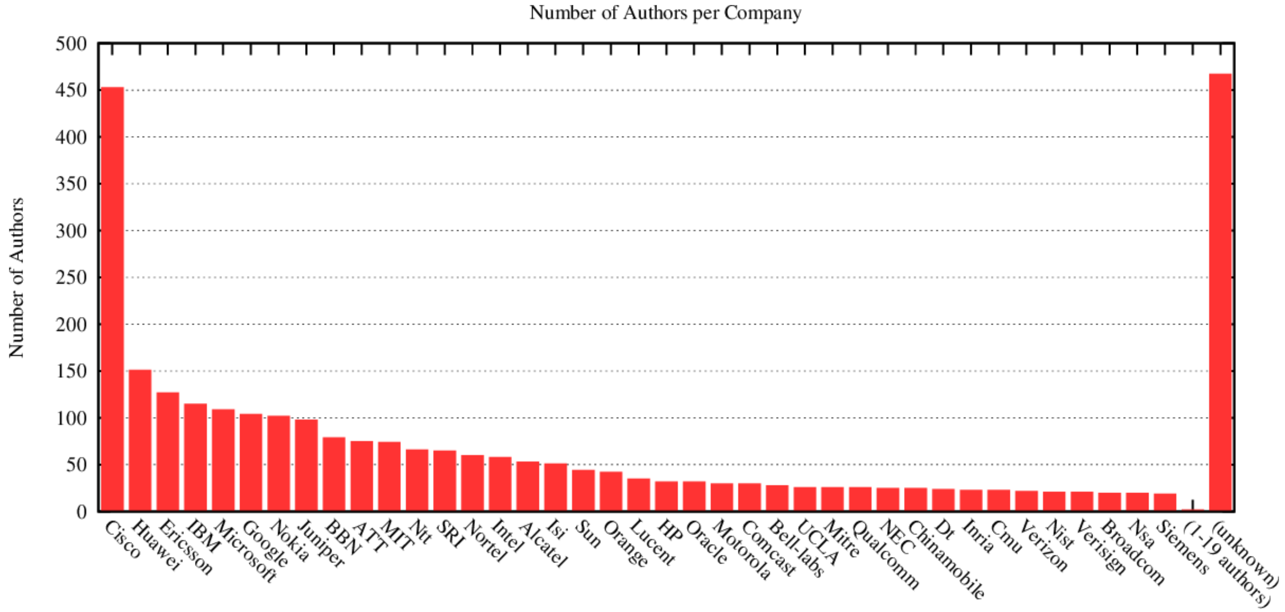
# Request For Comments

- RFCs cover many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, and sometimes humor.
- RFCs area associated with an active IETF Working Group.
- Published RFCs never change. Technical & Editorial Errata are provided.
- Started 7 Apr 1969, by Steve Crocker

- **RFC 1**: Host Software
- **RFC 2555**: 30 Years of RFCs

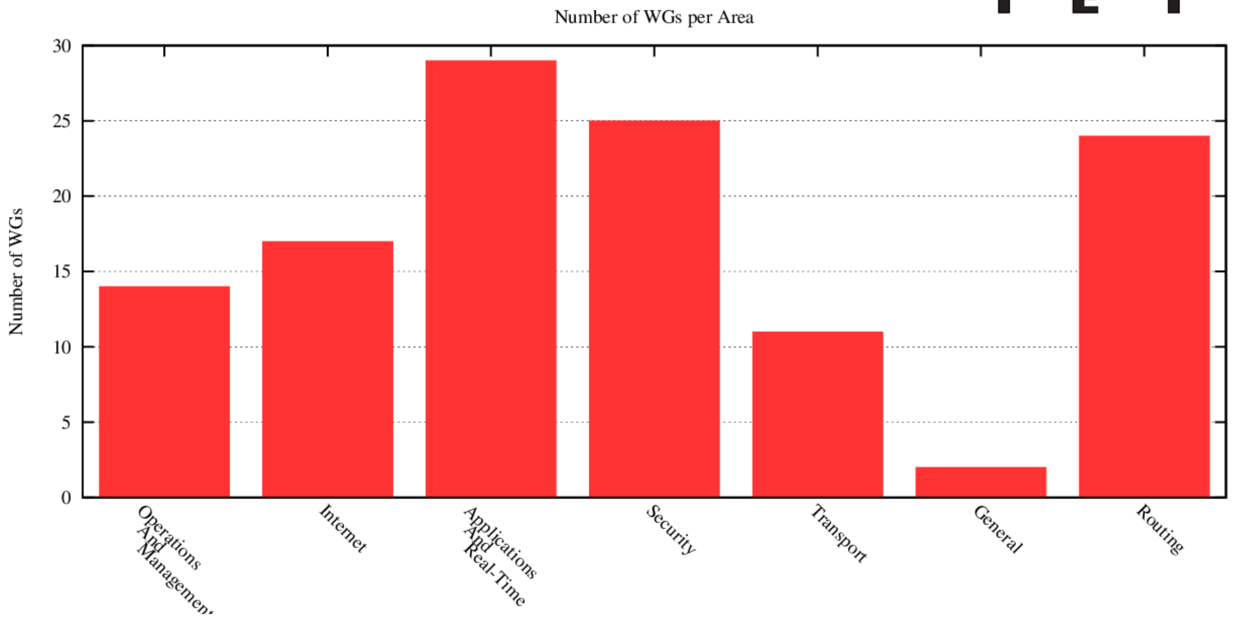


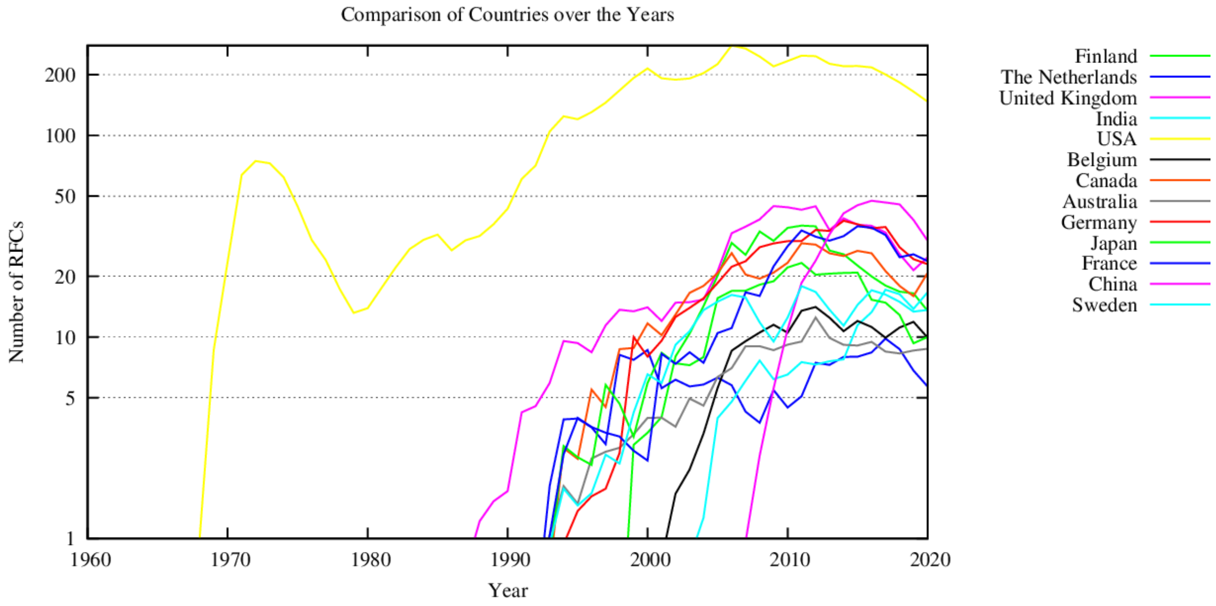


https://ietf.org/standards/rfcs/
www.arkko.com/tools/rfcstats/

# IETF Working Groups

- Applications & Real-Time area (29)
- General area (2)
- Internet area (17)
- Operations & Management area (14)
- Routing area (24)
- Secutiry area (25)
- Transport area (11)





https://ietf.org/standards/rfcs/
https://datatracker.ietf.org/wg/
www.arkko.com/tools/rfcstats/

# April RFCs

- **RFC527: ARPAWOCKY (1973)**
  Beware the ARPANET, my son;
  The bits that byte, the heads that scratch;
  Beware the NCP, and shun
  the frumious system patch,
- **RFC7511: Scenic Routing for IPv6 (2015)**
  This document specifies a new routing scheme for the current version of the Internet Protocol version 6 (IPv6) in the spirit of "Green IT", whereby packets will be routed to get as much fresh-air time as possible.
- **RFC2549: IP over Avian Carriers with Quality of Service (1999)**
  The following quality of service levels are available: Concorde, First, Business, and Coach.  Concorde class offers expedited data delivery.  One major benefit to using Avian Carriers is that this is the only networking technology that earns frequent flyer miles, plus the Concorde and First classes of service earn 50% bonus miles per packet.  Ostriches are an alternate carrier that have much greater bulk transfer capability but provide slower delivery, and require the use of bridges between domains.

IPoAC: IP over Avian Carriers

```
RFC 3514          The Security Flag in the IPv4 Header      1 April 2003

   The bit field is laid out as follows:

            0
           +-+
           |E|
           +-+

   Currently-assigned values are defined as follows:

   0x0  If the bit is set to 0, the packet has no evil intent.  Hosts,
        network elements, etc., SHOULD assume that the packet is
        harmless, and SHOULD NOT take any defensive measures.  (We note
        that this part of the spec is already implemented by many common
        desktop operating systems.)

   0x1  If the bit is set to 1, the packet has evil intent.  Secure
        systems SHOULD try to defend themselves against such packets.
        Insecure systems MAY chose to crash, be penetrated, etc.
```