

Independent Submission
Request for Comments: 8962
Category: Informational
ISSN: 2070-1721

G. Grover
N. ten Oever
C. Cath
S. Sahib
1 April 2021

Establishing the Protocol Police

Abstract

One mantra of the IETF is, "We are not the Protocol Police." However, to ensure that protocols are implemented and deployed in full compliance with the IETF's standards, it is important to set up a body that is responsible for assessing and enforcing correct protocol behavior.

This document formally establishes the Protocol Police. It defines the body and sets out what aspects of IETF protocols they will police. This document acts as a point of reference for networking engineers, law enforcement officials, government representatives, and others. It also provides advice on how to report issues to the Protocol Police.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see 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/rfc8962>.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction
2. Definitions
3. Composition of the Protocol Police
 - 3.1. Recognizing the Protocol Police
 - 3.2. Recruitment

4.	Support for the Protocol Police
5.	Punishable Offenses
5.1.	Protocol-Layer Violations
5.2.	Deliberate Non-Interoperability
5.3.	Disobeying RFCs
6.	Reporting Offenses
7.	Punishment
7.1.	Traffic Imprisonment
8.	Morality Considerations
8.1.	Oversight
9.	IANA Considerations
10.	Security Considerations
11.	Privacy Considerations
12.	Human Rights Considerations
13.	Conclusion
14.	Informative References
	Acknowledgments
	Authors' Addresses

1. Introduction

IETF participants are often confronted with circumstances where developers or deployers choose to not obey the sacrosanct words of an RFC. This can lead to outcomes that are widely agreed to be unexpected, unwarranted, or undesirable.

Some are of the opinion that IETF participants should come to a consensus and declare what protocol behavior is unacceptable, and that the maintainers and developers of non-compliant protocols should be chastised. Others (especially working group chairs) non-gracefully fall back on the undocumented mantra, "We [or the IETF] are not the Protocol Police." Understandably, this has led to confusion about who should make judgments about proper interpretation of protocol specifications.

This document formally establishes the Protocol Police, hitherto undocumented at the IETF. It defines the body and sets out what aspects of IETF protocols they will police. This document acts as a point of reference for networking engineers, law enforcement officials, government representatives, and others. It also provides advice on how to report issues to the Protocol Police.

The Protocol Police, as defined in this document, are responsible for enforcing all IETF standards and best practices.

2. Definitions

For possibly the first time in IETF history, words like "SHALL" and "MAY" are used in this document in their real and enforceable sense.

3. Composition of the Protocol Police

The Protocol Police shall be selected by the IETF Nominating Committee (NomCom) as laid out in [RFC3797] in a manner similar to that used to select the IAB and IESG [RFC8713].

However, the members of the Protocol Police shall not be publicly named. This will enable them to operate more effectively and without interference or unwarranted pressure from members of the community. The first rule of the Protocol Police is \$CIPHERTEXT.

3.1. Recognizing the Protocol Police

When more than one person says, "We are not the Protocol Police," at least one of them is not telling the truth.

The Protocol Police love company and are never alone.

You are not the Protocol Police: we are. We are not the Protocol Police: you are.

3.2. Recruitment

If you are interested in joining the Protocol Police, contact your localhost. Your behavior will be monitored, and your implementation will be analyzed for full RFC compliance. If your deeds, both now and in the past, are recognized to be true to the scripture, NomCom will of course be instructed to induct you to the ranks. But if you have transgressed, any information the investigation produces MAY be used against you in future proceedings.

In making an assessment of your suitability for membership of the Protocol Police, contact may be made on your behalf with the Internet Moral Majority [RFC4041].

If you have nothing to hide, you have nothing to fear.

4. Support for the Protocol Police

Support for the existence and operation of the Protocol Police is essential to the concept of "policing by consent." Fortunately, the IETF community and all stakeholders may now consider themselves served by this document which, by dint of its existence, warrants adherence.

5. Punishable Offenses

5.1. Protocol-Layer Violations

Some boundaries must not be crossed. There are no acceptable layer violations. Even though layers, like borders, are ambiguous abstractions only serving to uphold the legitimacy and identity of the institutions that produce them, they shall be observed and defended because the Protocol Police exist to defend them.

5.2. Deliberate Non-Interoperability

The Protocol Police are sanctioned to gain access to any walled garden that undermines interoperability. At the same time, the Protocol Police will defend legacy interoperability options in all NTP eras (see Section 6 of [RFC5905]), and will be reachable via the Extensible Messaging and Presence Protocol (XMPP) until at least era 2147483649.

5.3. Disobeying RFCs

In the beginning was the RFC, and the network was with the RFC, and the RFC was with the network. Through the RFC all things were made; without the RFC nothing was made that has been made. In the network was life, and that life was the light of all the INTERNET. Thou shalt not deviate from the path set out in the RFCs or else thou shall be scattered over the data plane.

6. Reporting Offenses

Send all your reports of possible violations and all tips about wrongdoing to /dev/null. The Protocol Police are listening and will take care of it.

7. Punishment

7.1. Traffic Imprisonment

The Protocol Police will maintain a list of hosts and clients that have demonstrated their inability to comprehend simple commandments contained in RFCs, which all IETF participants know to be precise and accessible even to a general audience.

If this work is standardized, IANA is requested to register the list of addresses (see Section 9). For a period specified in an official notification, all other networks SHALL drop all network packets originating from or intended for such addresses. This will result in effective and forced confinement of criminal networks.

Using powerful machine-learning mechanisms for threat analysis, the Protocol Police will identify networks that are likely to fail to comply with this requirement. This process is known as Heuristic Internet Policing (HIP). Networks identified in this way will be disciplined by the Protocol Police with TCP RSTs. Let it be known: the Protocol Police always shoot from the HIP.

8. Morality Considerations

This section contains morality considerations consistent with the demands of [RFC4041].

```
| We reject: kings, presidents and voting.  
| We believe in: rough consensus and running code.  
| We only bow down to: the Protocol Police.  
|  
| -- My friend Dave  
  
| Woop-woop! This is the Protocol Police!  
| Woop-woop! That's the packet of the beast!  
|  
| -- KRS-ZERO (after spotting an evil bit [RFC3514])
```

8.1. Oversight

All police forces must be accountable and subject to oversight. The Protocol Police take full responsibility for oversight of their actions and promise to overlook all activities.

9. IANA Considerations

If this work is standardized, IANA shall set up a registry for criminal networks and addresses. If the IANA does not comply with these orders, the Protocol Police shall go and cry to ICANN before becoming lost in its bureaucracy.

10. Security Considerations

Before the Protocol Police, there was no security. The Police have arrived. All your networks are belong to us.

11. Privacy Considerations

None.

12. Human Rights Considerations

There are none for you to worry about. The Police will see to it.

13. Conclusion

Case closed.

14. Informative References

- [RFC3514] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, DOI 10.17487/RFC3514, April 2003, <<https://www.rfc-editor.org/info/rfc3514>>.
- [RFC3797] Eastlake 3rd, D., "Publicly Verifiable Nominations Committee (NomCom) Random Selection", RFC 3797, DOI 10.17487/RFC3797, June 2004, <<https://www.rfc-editor.org/info/rfc3797>>.
- [RFC4041] Farrel, A., "Requirements for Morality Sections in Routing Area Drafts", RFC 4041, DOI 10.17487/RFC4041, April 2005, <<https://www.rfc-editor.org/info/rfc4041>>.
- [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.
- [RFC8713] Kucherawy, M., Ed., Hinden, R., Ed., and J. Livingood, Ed., "IAB, IESG, IETF Trust, and IETF LLC Selection, Confirmation, and Recall Process: Operation of the IETF Nominating and Recall Committees", BCP 10, RFC 8713, DOI 10.17487/RFC8713, February 2020, <<https://www.rfc-editor.org/info/rfc8713>>.

Acknowledgments

Members of the Protocol Police MUST salute and ACK all network traffic from Daniel Kahn Gillmor, Mallory Knodel, and Adrian Farrel.

Authors' Addresses

Gurshabad Grover

Email: gurshabad@cis-india.org

Niels ten Oever

Email: mail@nielstenoever.net

Corinne Cath

Email: corinnecath@gmail.com

Shivan Kaul Sahib

Email: shivankaulsahib@gmail.com