

Les RFC : mais cé quoi ce poulé ?

Clément PARSSEGNY

24 octobre 2024

1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

C'est quoi une RFC ?

C'est quoi une RFC ?

RFC = Request for Comments

Définit les normes et protocoles qui deviennent les standards de l'Internet Engineering Task Force (IETF).^a

a. <https://datatracker.ietf.org/>

C'est quoi une RFC ?

RFC = Request for Comments

Définit les normes et protocoles qui deviennent les standards de l'Internet Engineering Task Force (IETF). ^a

a. <https://datatracker.ietf.org/>

On y retrouve aussi des brouillons, des traces de discussions instantanées, des diapositives...

Ça ressemble à quoi ?

Note: This is a change from [RFC5246], so in practice many TLS 1.2 clients and servers will not behave as specified above.

A legacy TLS client performing renegotiation with TLS 1.2 or prior and which receives a TLS 1.3 ServerHello during renegotiation MUST abort the handshake with a "protocol_version" alert. Note that renegotiation is not possible when TLS 1.3 has been negotiated.

4.1.4. Hello Retry Request

The server will send this message in response to a ClientHello message if it is able to find an acceptable set of parameters but the ClientHello does not contain sufficient information to proceed with the handshake. As discussed in [Section 4.1.3](#), the HelloRetryRequest has the same format as a ServerHello message, and the legacy_version, legacy_session_id_echo, cipher_suite, and legacy_compression_method fields have the same meaning. However, for convenience we discuss "HelloRetryRequest" throughout this document as if it were a distinct message.

The server's extensions MUST contain "supported_versions". Additionally, it SHOULD contain the minimal set of extensions necessary for the client to generate a correct ClientHello pair. As with the ServerHello, a HelloRetryRequest MUST NOT contain any extensions that were not first offered by the client in its ClientHello, with the exception of optionally the "cookie" (see [Section 4.2.2](#)) extension.

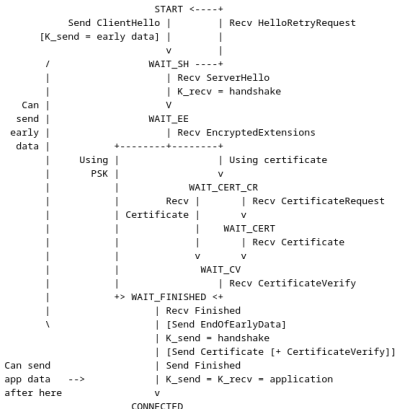
Upon receipt of a HelloRetryRequest, the client MUST check the legacy_version, legacy_session_id_echo, cipher_suite, and legacy_compression_method as specified in [Section 4.1.3](#) and then process the extensions, starting with determining the version using "supported_versions". Clients MUST abort the handshake with an "illegal_parameter" alert if the HelloRetryRequest would not result in any change in the ClientHello. If a client receives a second HelloRetryRequest in the same connection (i.e., where the ClientHello was itself in response to a HelloRetryRequest), it MUST abort the handshake with an "unexpected_message" alert.

Ça ressemble à quoi ?

Appendix A. State Machine

This appendix provides a summary of the legal state transitions for the client and server handshakes. State names (in all capitals, e.g., START) have no formal meaning but are provided for ease of comprehension. Actions which are taken only in certain circumstances are indicated in []. The notation "K_(send,rcv) = foo" means "set the send/rcv key to the given key".

A.1. Client



Pourquoi je dois lire des RFC ?

Pourquoi je dois lire des RFC ?

- Une mine d'informations : c'est l'Histoire et l'avenir d'Internet devant nous ;

Pourquoi je dois lire des RFC ?

- Une mine d'informations : c'est l'Histoire et l'avenir d'Internet devant nous ;
- Obligatoire pour implémenter un protocole, l'analyser, etc ;

Pourquoi je dois lire des RFC ?

- Une mine d'informations : c'est l'Histoire et l'avenir d'Internet devant nous ;
- Obligatoire pour implémenter un protocole, l'analyser, etc ;
- De supers livres de chevet.

Pourquoi je dois lire des RFC ?

- Une mine d'informations : c'est l'Histoire et l'avenir d'Internet devant nous ;
- Obligatoire pour implémenter un protocole, l'analyser, etc ;
- De supers livres de chevet.



1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

RFC1149/RFC2549 : *IP over Avian Carriers*¹ (*with Quality of Service*²)

-
1. <https://datatracker.ietf.org/doc/html/rfc1149>
 2. <https://datatracker.ietf.org/doc/html/rfc2549>

RFC1149/RFC2549 : *IP over Avian Carriers*¹ (*with Quality of Service*²)

- Proposée en 1990 et 1999 ;

1. <https://datatracker.ietf.org/doc/html/rfc1149>

2. <https://datatracker.ietf.org/doc/html/rfc2549>

RFC1149/RFC2549 : *IP over Avian Carriers*¹ (*with Quality of Service*²)

- Proposée en 1990 et 1999 ;
- Implémentée seulement en 2001 ;

1. <https://datatracker.ietf.org/doc/html/rfc1149>

2. <https://datatracker.ietf.org/doc/html/rfc2549>

RFC1149/RFC2549 : *IP over Avian Carriers*¹ (*with Quality of Service*²)

- Proposée en 1990 et 1999 ;
- Implémentée seulement en 2001 ;
- Principe : imprimer son paquet IP sur papier et l'enrouler autour de la patte d'un oiseau (ex : pigeon)

1. <https://datatracker.ietf.org/doc/html/rfc1149>

2. <https://datatracker.ietf.org/doc/html/rfc2549>

RFC1149/RFC2549 : *IP over Avian Carriers*¹ (*with Quality of Service*²)

- Proposée en 1990 et 1999 ;
- Implémentée seulement en 2001 ;
- Principe : imprimer son paquet IP sur papier et l'enrouler autour de la patte d'un oiseau (ex : pigeon)



1. <https://datatracker.ietf.org/doc/html/rfc1149>
2. <https://datatracker.ietf.org/doc/html/rfc2549>

RFC1149/RFC2549 : Implémentation³



3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html



3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html



3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html



3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html

RFC1149/RFC2549 : Implémentation³



3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html


```
64 bytes from 10.0.3.1: icmp_seq=0 ttl=255 time=6165731.1 ms
64 bytes from 10.0.3.1: icmp_seq=4 ttl=255 time=3211900.8 ms
64 bytes from 10.0.3.1: icmp_seq=2 ttl=255 time=5124922.8 ms
64 bytes from 10.0.3.1: icmp_seq=1 ttl=255 time=6388671.9 ms
```

```
--- 10.0.3.1 ping statistics ---
```

```
9 packets transmitted, 4 packets received, 55% packet loss
round-trip min/avg/max = 3211900.8/5222806.6/6388671.9 ms
```

3. https://web.archive.org/web/20111004221416/http://www.blug.linux.no/rfc1149/vegard_bilder/index.html

Avantages Inconvénients

Avantages	Inconvénients
------------------	----------------------

Écologique

Avantages	Inconvénients
Écologique MTU configurable	

Avantages

Écologique

MTU configurable

Adaptable à d'autres protocoles

Inconvénients

Avantages

Écologique
MTU configurable
Adaptable à d'autres protocoles

Inconvénients

Perte de paquets (faucon)

Avantages

Écologique
MTU configurable
Adaptable à d'autres protocoles

Inconvénients

Perte de paquets (faucon)
Maladies

RFC1149/RFC2549 : On en pense quoi ?

Avantages

Écologique
MTU configurable
Adaptable à d'autres protocoles

Inconvénients

Perte de paquets (faucon)
Maladies
Pas de multicast

IPoB : IP over Burrito Carriers⁴

4. <https://www.ietf.org/archive/id/draft-lohsen-ip-burrito-00.txt>

- Proposée en 2005 ;

4. <https://www.ietf.org/archive/id/draft-lohsen-ip-burrito-00.txt>

- Proposée en 2005 ;
- Un *draft* ;

4. <https://www.ietf.org/archive/id/draft-lohsen-ip-burrito-00.txt>

IPoB : IP over Burrito Carriers⁴

- Proposée en 2005 ;
- Un *draft* ;
- Principe : Utiliser un burrito comme paquet IP envoyé par un livreur.



4. <https://www.ietf.org/archive/id/draft-lohsen-ip-burrito-00.txt>

IPoB : IP over Burrito Carriers⁵

```
.....
|Version| IHL |Type of Service|          Total Length |
|.....
|          Identification |Flags|          Fragment Offset |
|.....
| Time to Live | Protocol |          Header Checksum |
|.....
|          Source Address |
|.....
|          Destination Address |
|.....
|          Data |
|.....
```

The Internet Header Format [RFC-791]

Figure 1.

```
.....
|Obvious| Onion | Jalapenos | Physical Length (mm) |
|.....
|          Number Written on Foil |Bean Type| Number of Beans |
|.....
| Given Delivery Time | Guacamole |          Receipt |
|.....
|          Lettuce |
|.....
|          Rice |
|.....
|          Beef |
|.....
```

The Burrito Internet Header Format

Figure 2.

5. <https://www.ietf.org/archive/id/draft-lohsen-ip-burrito-00.txt>

Avantages Inconvénients

Avantages**Inconvénients**

Nourriture et communication

Avantages**Inconvénients**

Nourriture et communication

Burrito

Avantages	Inconvénients
Nourriture et communication	
Burrito	
Adaptable à d'autres plats	

Avantages	Inconvénients
Nourriture et communication	16 octets/burrito
Burrito	
Adaptable à d'autres plats	

Avantages	Inconvénients
Nourriture et communication	16 octets/burrito
Burrito	« Uberisation »
Adaptable à d'autres plats	

IPoB : On en pense quoi ?

Avantages	Inconvénients
Nourriture et communication	16 octets/burrito
Burrito	« Uberisation »
Adaptable à d'autres plats	Dépendance sur le menu

1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

6. <https://datatracker.ietf.org/doc/html/rfc1924>

- Proposé en 1996 ;

6. <https://datatracker.ietf.org/doc/html/rfc1924>

- Proposé en 1996 ;
- Pas un protocole mais un encodage ;

6. <https://datatracker.ietf.org/doc/html/rfc1924>

- Proposé en 1996 ;
- Pas un protocole mais un encodage ;
- Principe : convertir l'IP en base 85 pour passer de 39 à 20 octets.

6. <https://datatracker.ietf.org/doc/html/rfc1924>

① 1080:0:0:0:8:800:200C:417A

- ① 1080:0:0:0:8:800:200C:417A
- ② 21932261930451111902915077091070067066

- ① 1080:0:0:0:8:800:200C:417A
- ② 21932261930451111902915077091070067066
- ③ 4-68-70-46-66-12-63-31-61-19-4-37-53-75-0-58-57-65-34-51

- ① 1080:0:0:0:8:800:200C:417A
- ② 21932261930451111902915077091070067066
- ③ 4-68-70-46-66-12-63-31-61-19-4-37-53-75-0-58-57-65-34-51
- ④ 4)+k&C#VzJ4br>0wv%Yp

RFC 1924 : On en pense quoi ?

Avantages**Inconvénients**

Adresse plus compacte

RFC 1924 : On en pense quoi ?

Avantages**Inconvénients**

Adresse plus compacte

Offuscation naturelle

RFC 1924 : On en pense quoi ?

Avantages

Inconvénients

Adresse plus compacte

Offuscation naturelle

Pas d'omission de 0

RFC 1924 : On en pense quoi ?

Avantages

Adresse plus compacte
Offuscation naturelle
Pas d'omission de 0
Taille fixe

Inconvénients

1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

RFC 9564 : Faster Than Light Speed Protocol (FLIP) ⁷

7. <https://datatracker.ietf.org/doc/html/rfc9564e>

RFC 9564 : Faster Than Light Speed Protocol (FLIP) ⁷

- Proposée en 2024 ;

7. <https://datatracker.ietf.org/doc/html/rfc9564e>

RFC 9564 : Faster Than Light Speed Protocol (FLIP) ⁷

- Proposée en 2024 ;
- L'avenir d'Internet ;

7. <https://datatracker.ietf.org/doc/html/rfc9564e>

RFC 9564 : Faster Than Light Speed Protocol (FLIP) ⁷

- Proposée en 2024 ;
- L'avenir d'Internet ;
- Principe : Utiliser des LLMs pour prédire la communication.

7. <https://datatracker.ietf.org/doc/html/rfc9564e>

RFC 9564 : Faster Than Light Speed Protocol (FLIP)⁷

- Proposée en 2024 ;
- L'avenir d'Internet ;
- Principe : Utiliser des LLMs pour prédire la communication.



7. <https://datatracker.ietf.org/doc/html/rfc9564e>

Avantages Inconvénients

Avantages	Inconvénients
------------------	----------------------

Vitesse	
---------	--

RFC 9564 : On en pense quoi ?

Avantages	Inconvénients
------------------	----------------------

Vitesse

Chiffrement

RFC 9564 : On en pense quoi ?

Avantages	Inconvénients
Vitesse Chiffrement	Coût énergétique (à équilibrer avec IPoAC)

1 Introduction

2 RFC 1149/RFC 2549

3 RFC 1924

4 RFC 9564

5 Conclusion

Conclusion

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;

8. [https:](https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments)

[//en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments](https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments)

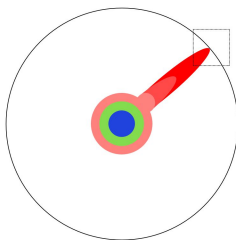
- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;
- Quand on doit se plonger dedans, on se rend compte qu'on est en train de travailler sur quelque chose de vraiment concret et que ça fait avancer les choses.

8. [https:](https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments)

[//en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments](https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments)

Conclusion

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;
- Quand on doit se plonger dedans, on se rend compte qu'on est en train de travailler sur quelque chose de vraiment concret et que ça fait avancer les choses.



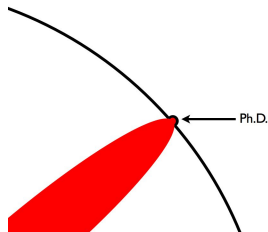
9

8. https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

9. <https://matt.might.net/articles/phd-school-in-pictures/>

Conclusion

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;
- Quand on doit se plonger dedans, on se rend compte qu'on est en train de travailler sur quelque chose de vraiment concret et que ça fait avancer les choses.

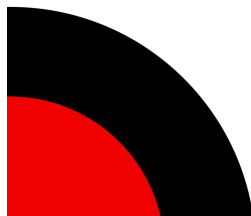


9

8. https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments
9. <https://matt.might.net/articles/phd-school-in-pictures/>

Conclusion

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;
- Quand on doit se plonger dedans, on se rend compte qu'on est en train de travailler sur quelque chose de vraiment concret et que ça fait avancer les choses.



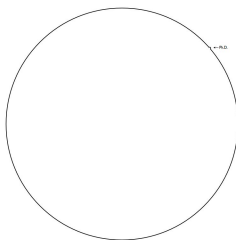
9

8. https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

9. <https://matt.might.net/articles/phd-school-in-pictures/>

Conclusion

- Les RFC sont des documents essentiels dans nos domaines et pour pleins de métiers (développeurs, chercheurs, intégrateurs) ;
- Les futurs standards y sont décrits⁸ ;
- Quand on doit se plonger dedans, on se rend compte qu'on est en train de travailler sur quelque chose de vraiment concret et que ça fait avancer les choses.



9

8. https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

9. <https://matt.might.net/articles/phd-school-in-pictures/>