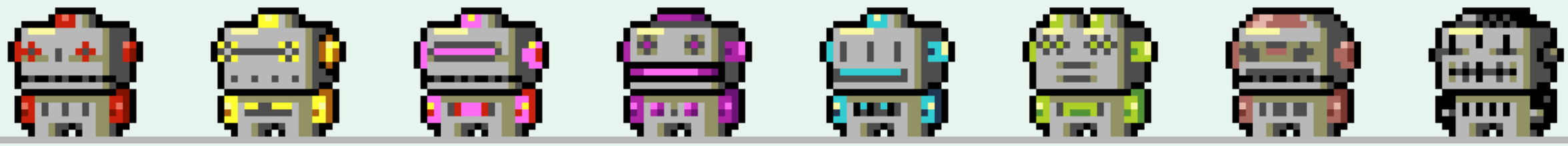
Anti-DDoS Bot

(gobgpd + flowspec編)

JANOG37
Shintaro Kojima / @codeout



https://www.flickr.com/photos/iloveui/7090895435/

小島 慎太郎
コーダンス

codeout

http://about.me/codeout

みなさん、DDoSと戦ってますか？

モチベーション

システムで検知します

↓

ダッシュボード クリックします

↓

… 詳しくは説明できません が

DDoSが止まります

エラーバジェット

ダッシュボード クリックします

DDoSが止まります

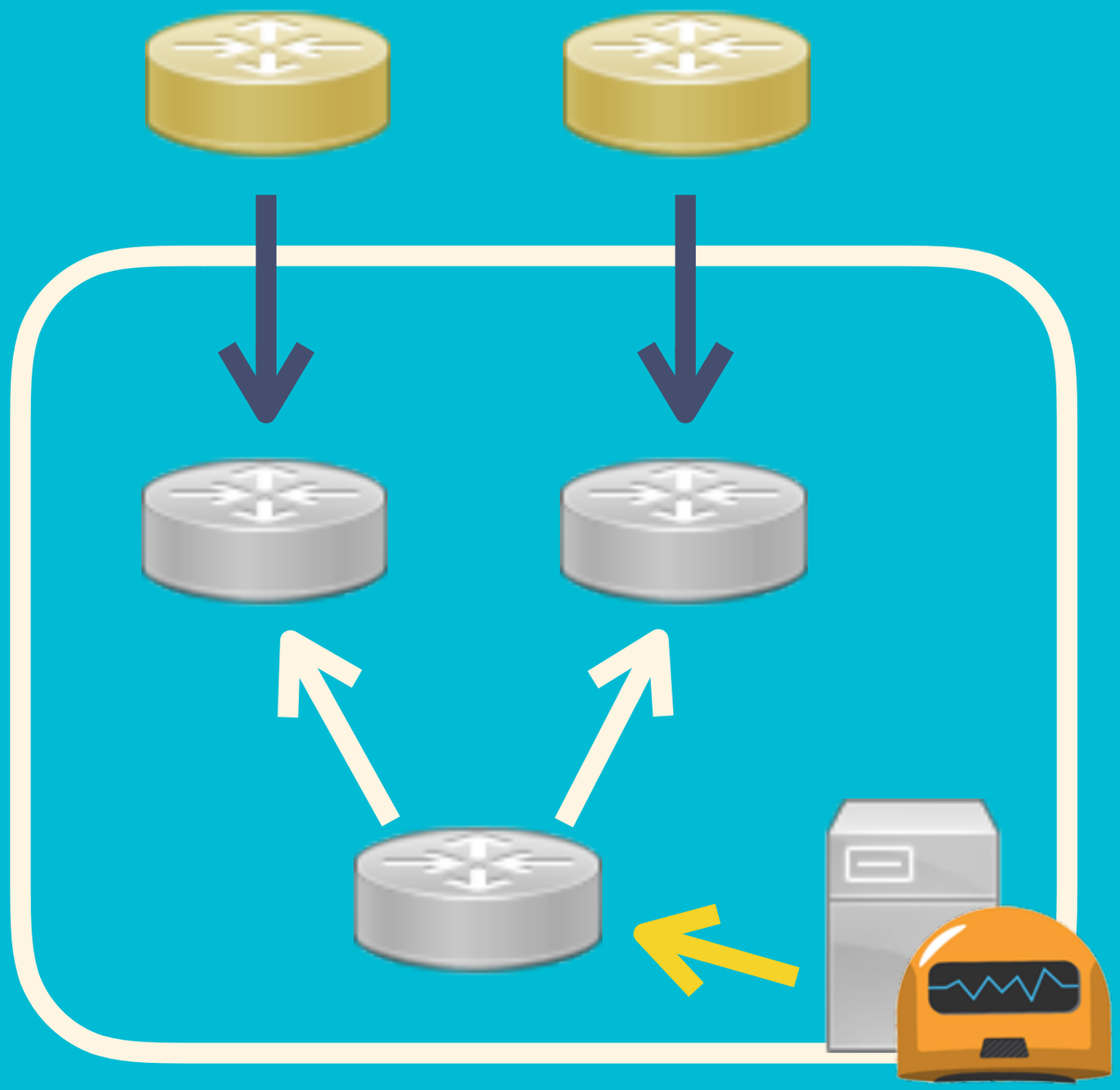
false positive
怖い

パイプが埋まる
ほどじゃない

中身が透ける
くらいシンプル
でいい

でも一瞬で

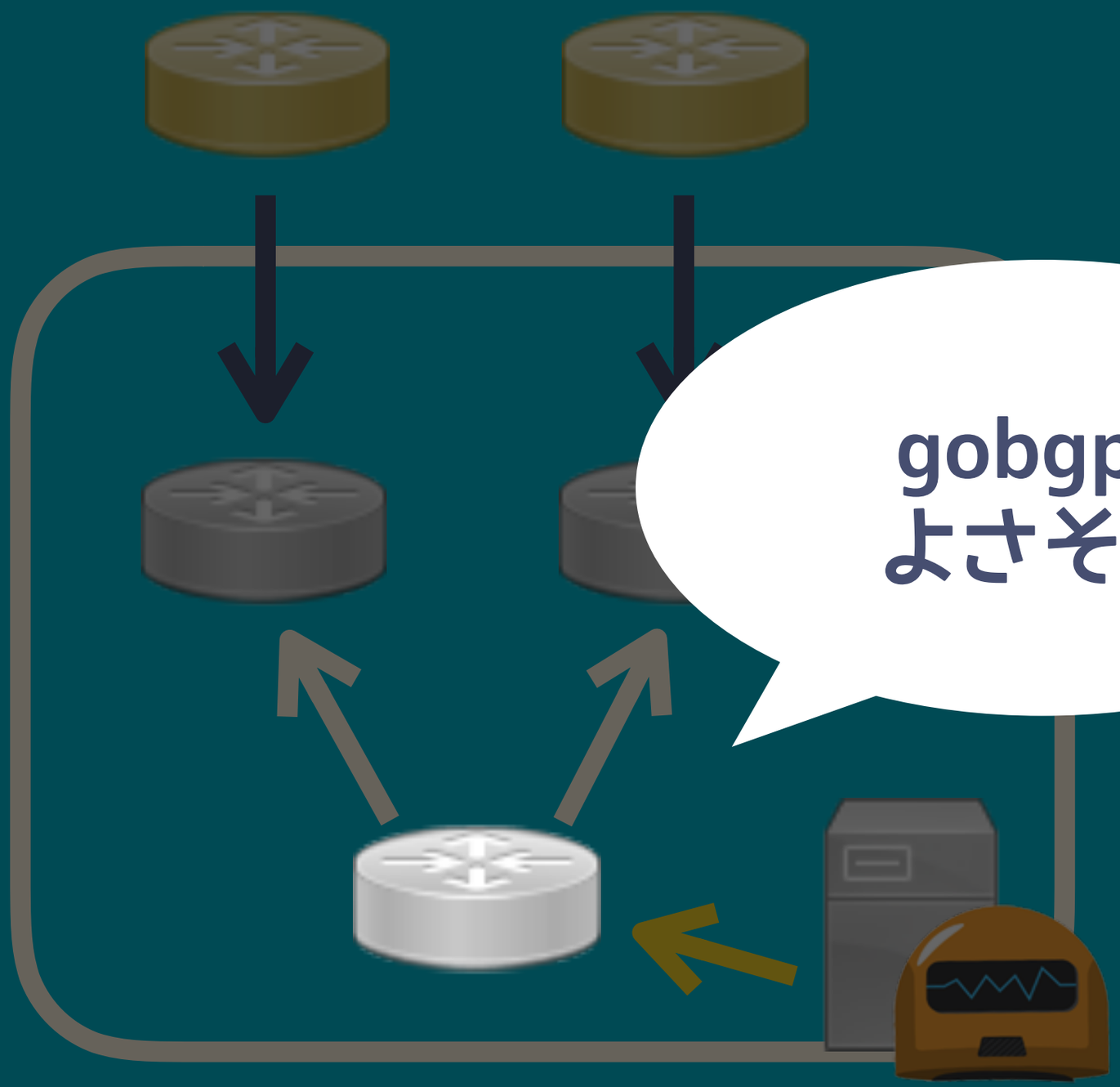
こんなのどうです？



1. チャットで命令
2. flowspec で伝搬
3. DDoS が止まる

flowspec
オリジネートは
壊れてもいいやつで

こんなのどうです？



1. チャットで命令
2. flowspec で伝搬
3. DDoS が止まる

flowspec
オリジネートは
壊れてもいいやつで

osrg/gobgp

https://github.com/osrg/gobgp

- Go で実装されたbgpd
- クライアント / サーバー 間が gRPC
- JANOGにもコミッターが！ 👍🏼

神サポート ⚡

Tamihiro Yuzawa 8/27, 1:10am

困っているというよりはワガママになってしまいますが、MRTから食わせたv4フルを３０秒くらいではきだせるのがあれば、なんでもテストできるだろうなぁと、、

September 1, 2015

Wataru Ishida 9/1, 7:26am

https://github.com/osrg/gobgp/blob/master/docs/sources/route-reflector.md

RRとして動くようになりました！

あとメッセージ数もquaggaと同数に改善されました

Shintaro Kojima 9/1, 10:07am

gRPC

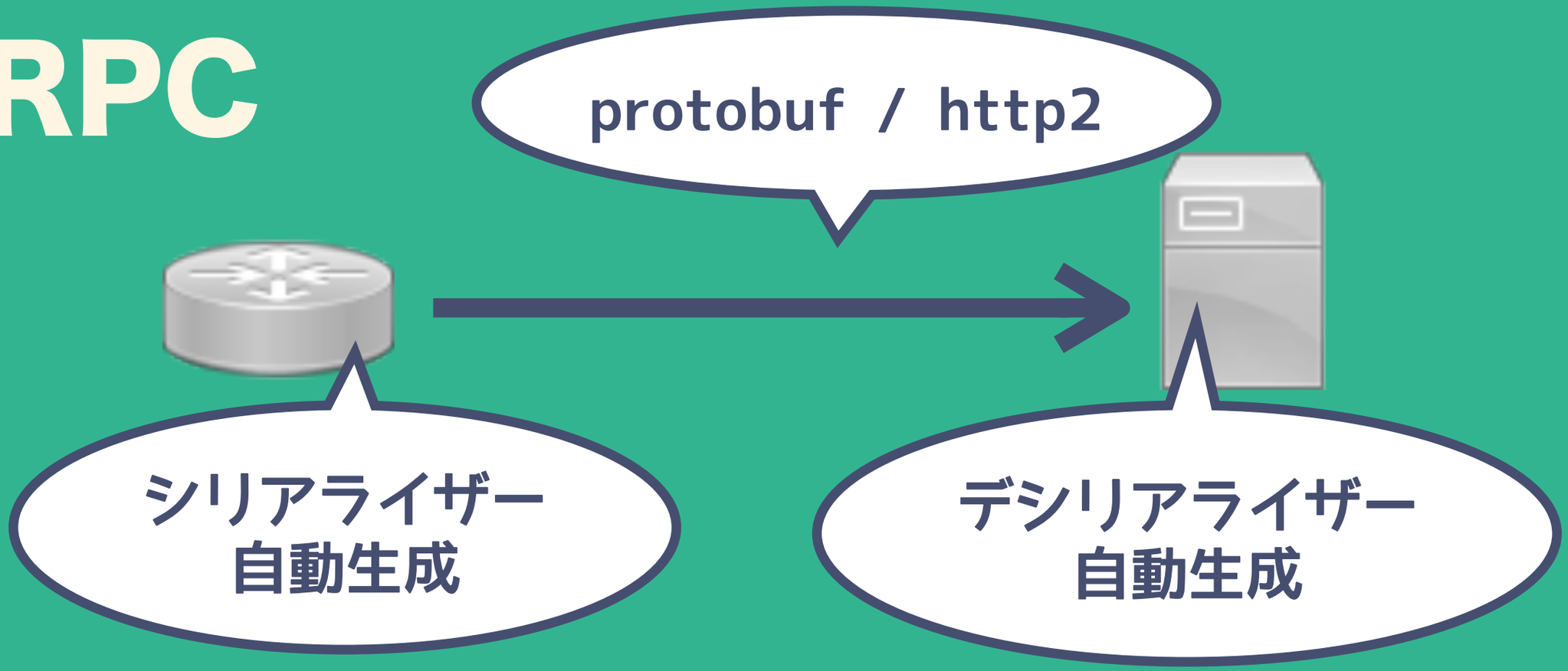
- Google が作ってるRPC フレームワーク
- トランスポート = HTTP2
- シリアライザー = Protocol Buffer
- 解決する問題は NETCONF に似ている

gRPC

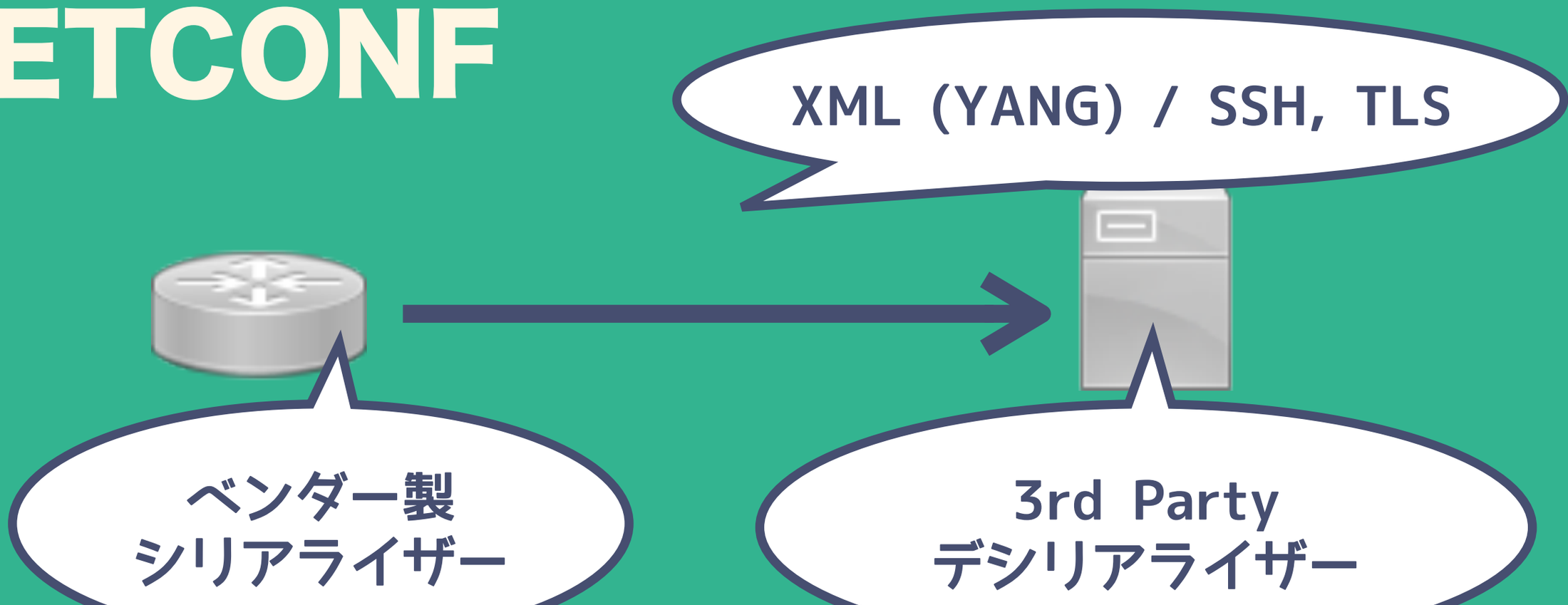
&

NETCONF

gRPC



NETCONF



クライアントの書きやすさ: 大差ない

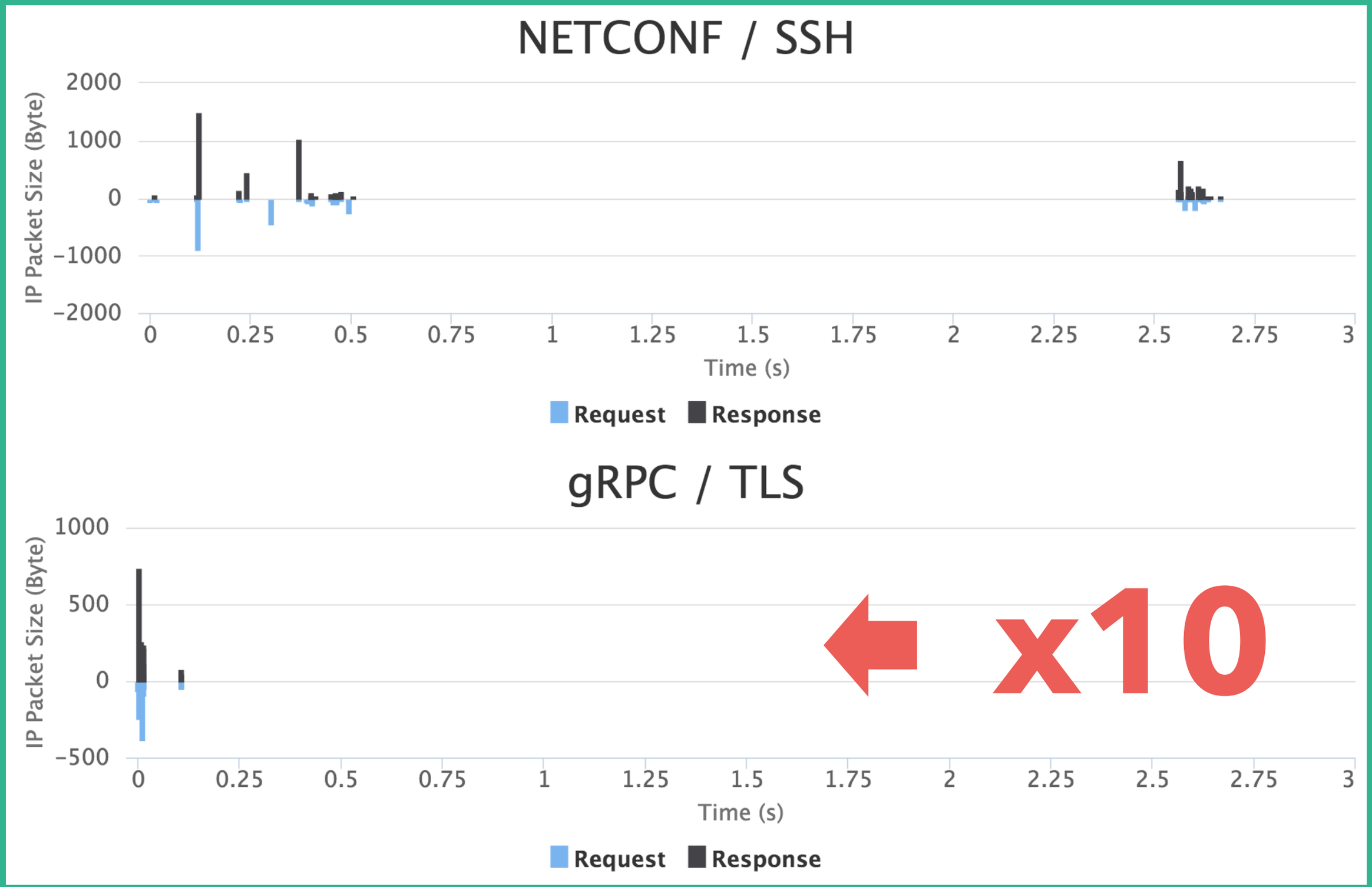
```
1 var grpc = require('grpc');
2 var api = grpc.load('node_modules/gobgp/deps/gobgp/gobgp.proto').gobgpapi;
3 var stub = new api.GobgpApi('localhost:50051', grpc.Credentials.createInsecure());
4
5 var call = stub.getNeighbors({});
6 call.on('data', function(neighbor) {
7   console.log(JSON.stringify(neighbor));
8 });
```

gRPC

```
 1 var netconf = require('netconf');
 2 var router = new netconf.Client({
 3   host: 'localhost',
 4   port: 830,
 5   username: 'codeout',
 6   password: 'password'
 7 });
 8
 9 router.open(function afterOpen(err) {
10   if (!err) {
11     router.rpc('get-bgp-neighbor-information', function (err, reply) {
12       router.close();
13       if (err) {
14         throw (err);
15       }
16       console.log(JSON.stringify(reply));
17     });
18   } else {
19     throw (err);
20   }
21 });
```

NETCONF

Speed !


NETCONF / SSH
IP Packet Size (Byte)
2000
1000
0
−1000
−2000
0
0.25
0.5
0.75
1
1.25
1.5
1.75
2
2.25
2.5
2.75
3
Time (s)
Request
Response
gRPC / TLS
IP Packet Size (Byte)
1000
500
0
−500
0
0.25
0.5
0.75
1
1.25
1.5
1.75
2
2.25
2.5
2.75
3
Time (s)
Request
Response
x10

gRPC を選んだ理由

- クライアントが自動生成できる
- 手間なく基本機能が実装できる
  eg）サーバーと通信せずエラーチェック
- 速い ！

さて、

書いてみよう！

思い描いてたもの

```
1 var Gobgp = require('gobgp');
2 var gobgp = new Gobgp('localhost:50051');
3
4 gobgp.modPath('ipv4-flowspec',
5                'match source 10.0.0.0/24 then rate-limit 10000');
```

現実 😰

```
var Gobgp = require('gobgp');
var gobgp = new Gobgp('localhost:50051');

gobgp.modPath({path: { nlri: <Buffer >,
                       pattrs:
                       [ <Buffer 80 0e 0b 00 01 85 00 00 05 02 18 0a 00 00>,
                         <Buffer 40 01 01 02>,
                         <Buffer c0 10 08 80 06 00 00 46 1c 40 00> ] }});
```

なぜ…

ishidawataru 11月 28 17:28

Hi! originally we had such APIs but we removed since preparing all the BGP structs in .proto file gets tedious. (see osrg/gobgp@a01b549)

But I understand it’s difficult for some languages which don't have good BGP library to play with current gRPC API.

Maybe it will be good to have some portion of basic BGP structs in gRPC API

わかる

さて、

どうしよう？

案1

gRPC (JS)

NodeJS

V8 (C++)

シリアライズは
JS で

案2

gRPC
(C++)

gobgp
(C)

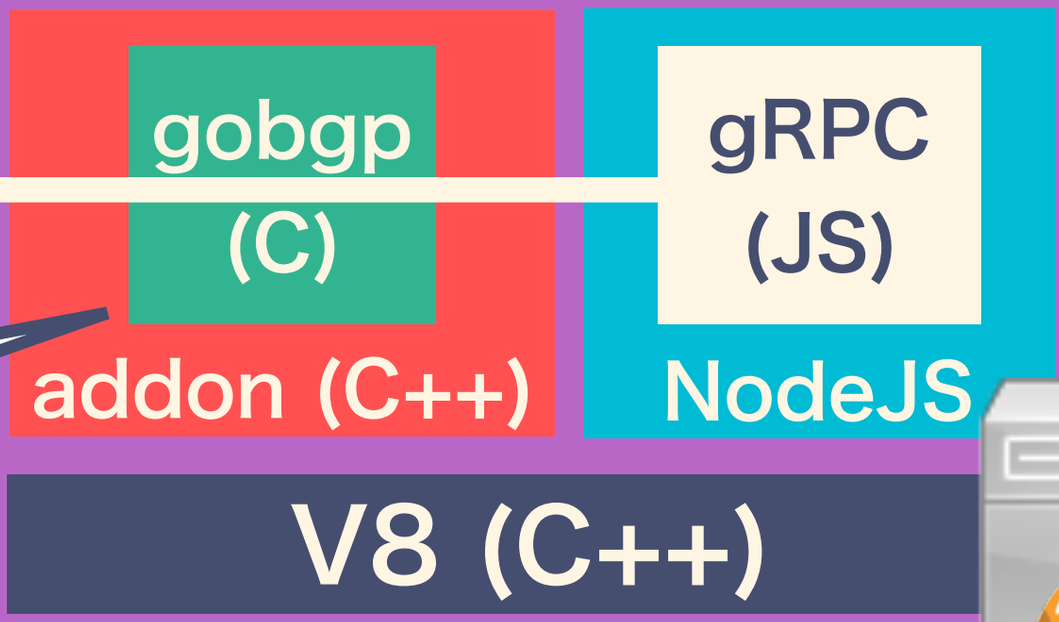
addon (C++)

NodeJS

V8 (C++)

シリアライズは
gobgp の C-Shared Libで

こうか！！！



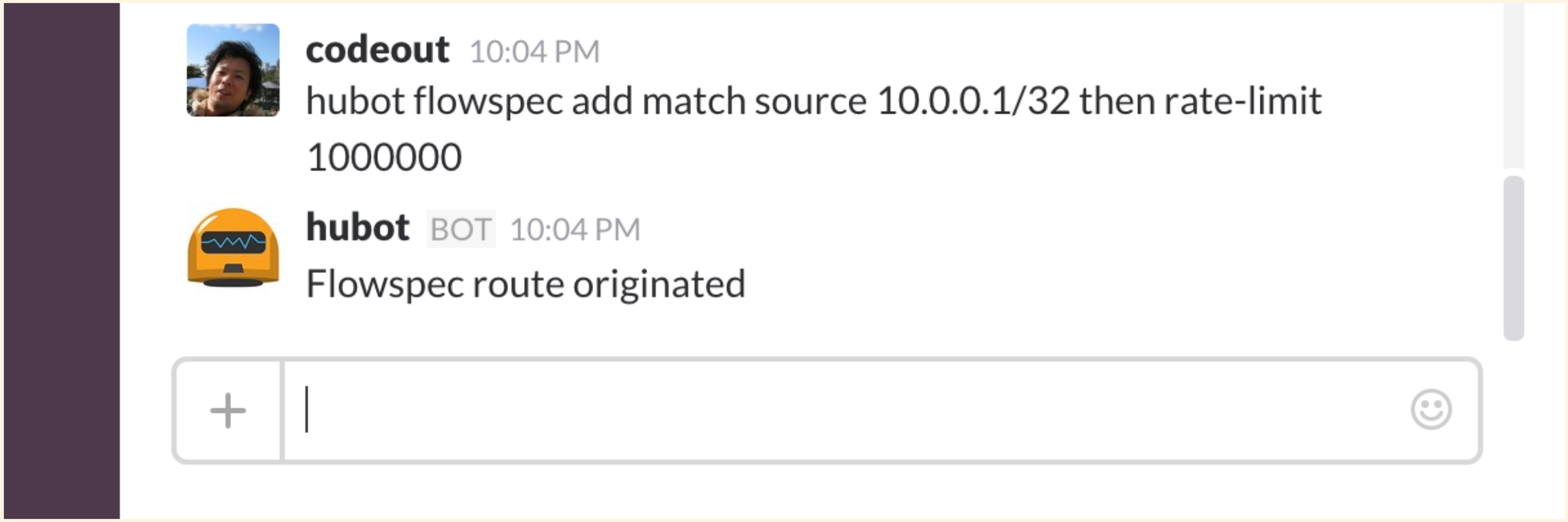
シリアライズだけ
gobgp の C-Shared Libで

codeout/gobgp-node

https://github.com/codeout/gobgp-node

- NodeJS 向けgobgp クライアント
- 今のところ、経路操作のみ実装
- Hubot スクリプト例
  https://gist.github.com/codeout/20bc799560b6efe7b2be

主な機能:
経路の生成、削除、表示



そのほか、

- unicast 経路のルックアップ
- ホストアドレス → プレフィックスに変換して flowspec 経路を生成

できれば…こうしたい

システムで検知します

↓

Hubot に ID を渡します

↓

(ID をもとに情報とってきて

flowspec 経路生成して)

DDoSが止まります

もっと言えば…こうしたい

システムが検知して

DDoS 検知システムに API をおねがいします！

Hubotなどが ID を渡します

(ID をもとに情報とってきて

flowspec 経路生成して)

DDoSが止まります

まとめ

- gobgpd + flowspec で DDoS を止められる
- しかもChatOps で ！

その他

- flowspec はベンダーごとにvalidation 動作が違うので注意
  - draft-ietf-idr-bgp-flowspec-oid-02
- Anti-DDoS Bot (ACL 自動生成編) も動いてる