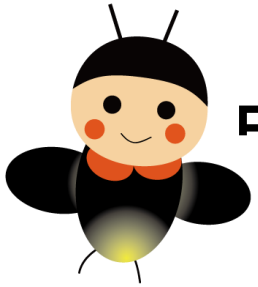


中华数据库
行业协会

2014中华数据库与运维安全大会

官方网址：www.zhdba.com

MySQL Database Replay

王斌（网易）
QQ交流群：192300573

非数据库专家

写一个专业的MySQL Replay工具?

可行

大纲

- 相关研究
- MySQL协议剖析
- Replay原理
- 代码量
- 演示

1、相关研究

Log回放

Oracle Database Replay

数据包回放？

没有

更没有实时Replay

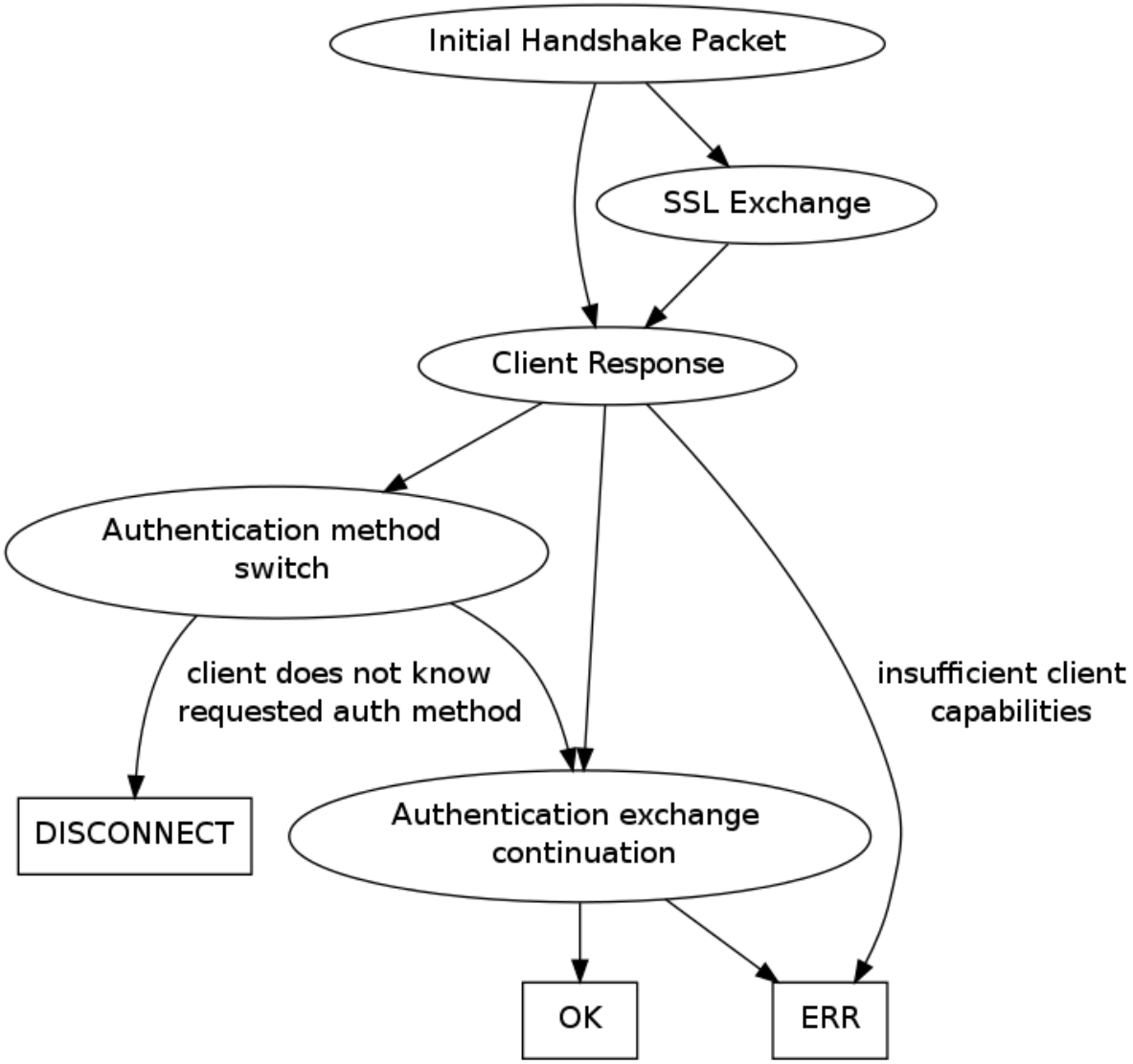
2011.9，TCPCopy发布

不久，一位MySQL专家尝试了TCPCopy

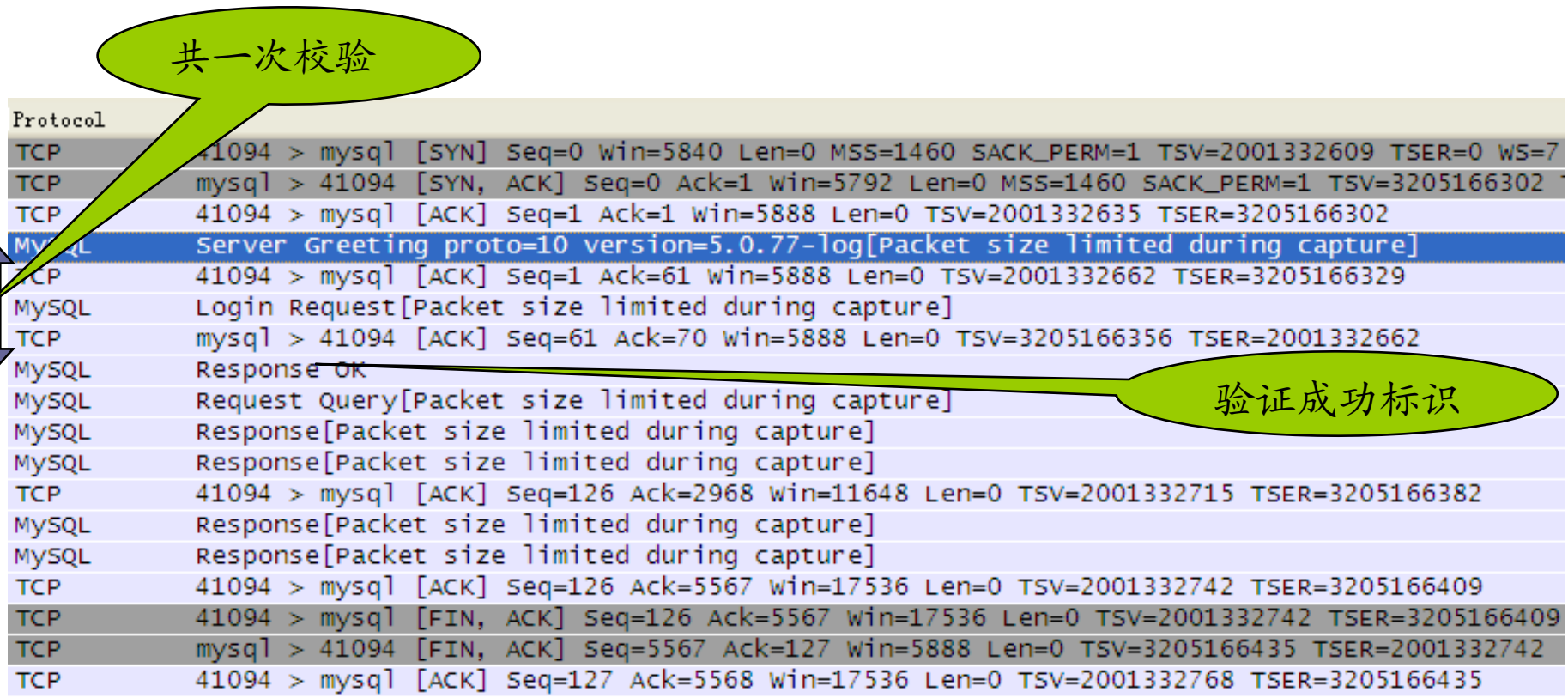
采用skip-grant-table运行了半小时

2、MySQL协议剖析

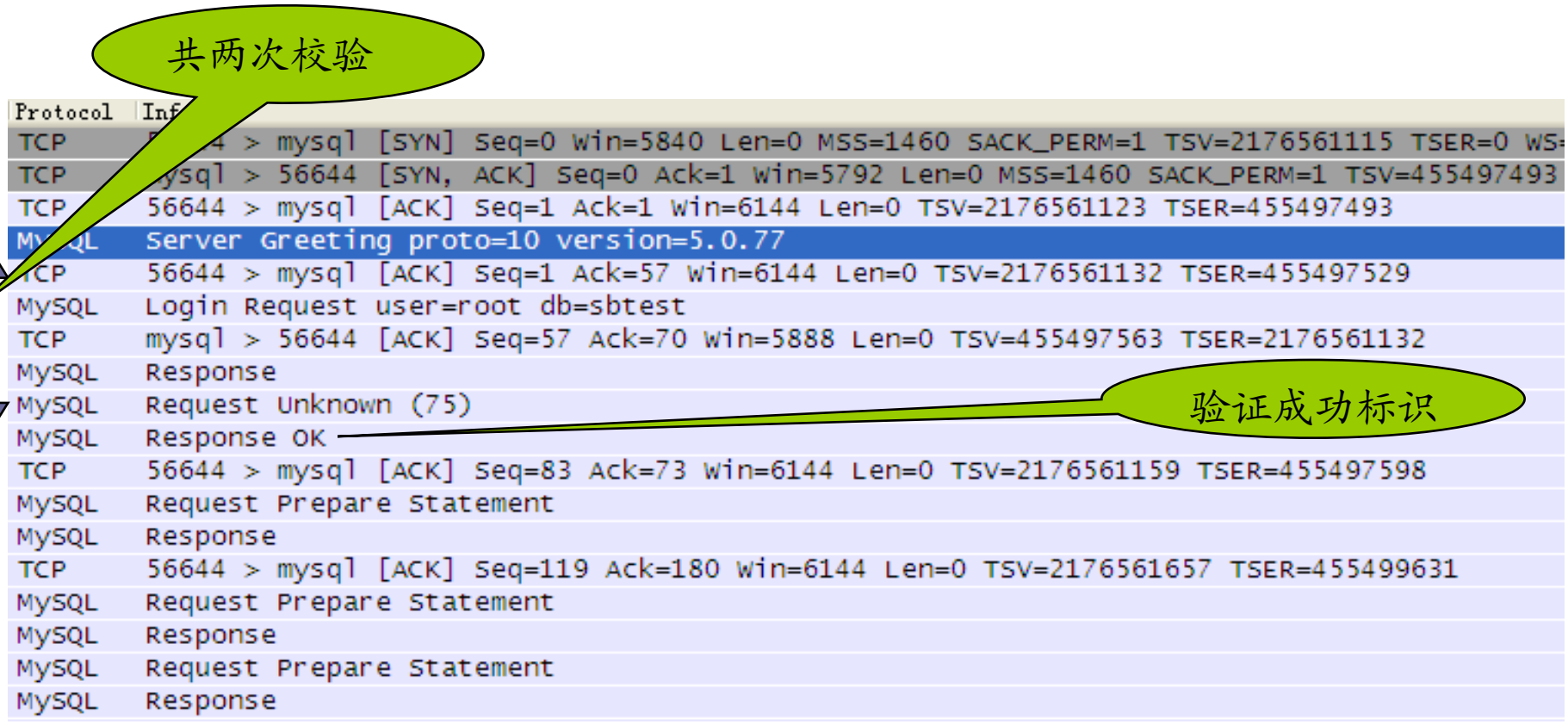
Connection Phase



Connection Phase



Connection Phase



Any more?

请求响应交互模式

3、Replay原理

数据包回放(离线或实时)

MySQL官方文档提供的线索

协议安全设计

Neither **snooping on the wire** nor **mysql.user.Password** are sufficient for a successful connection.

But

When one has both

mysql.user.Password and **the intercepted data on the wire**,

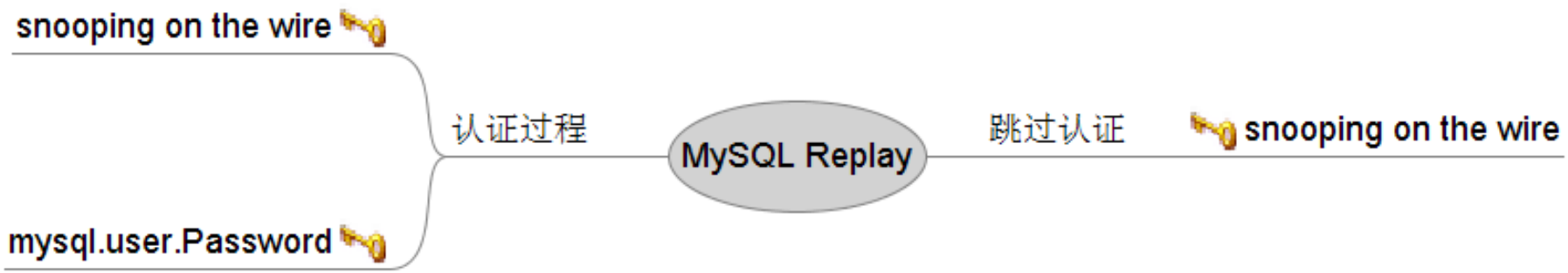
he has enough information to connect.

做一些有益的事情

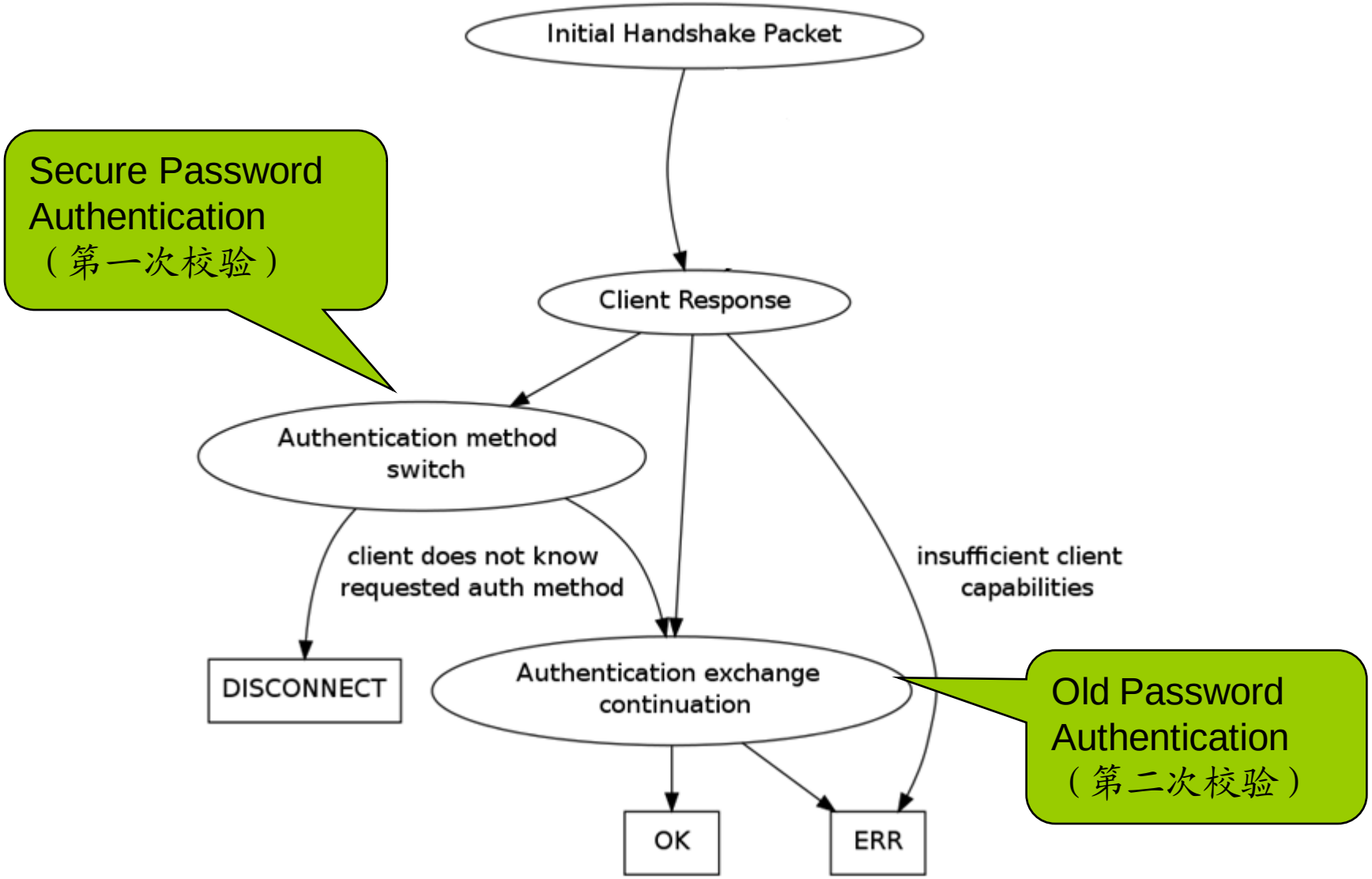
提供Replay服务

还有哪些可挖的信息？

skip-grant-tables


snooping on the wire
mysql.user.Password
认证过程
MySQL Replay
跳过认证
snooping on the wire

攻克方向


Initial Handshake Packet
Secure Password Authentication （第一次校验）
Client Response
Authentication method switch
client does not know requested auth method
insufficient client capabilities
DISCONNECT
Authentication exchange continuation
Old Password Authentication （第二次校验）
OK
ERR

Authentication攻克策略

- 采用skip方式来部署测试系统

  避开认证过程

- 非skip方式

  1）在线系统和测试部署一致，降低攻克难度

  a) mysql.user要一致

  b) 用户权限要一致

  c) 不支持第三方的auth plugins

  2）对数据包做必要修改

  a) 修改secure Password Authentication中的Password字段

  b) 修改old Password Authentication中的scramble_buff字段

如何解决运行半小时问题？

重建connection phase过程

还原prepared statements

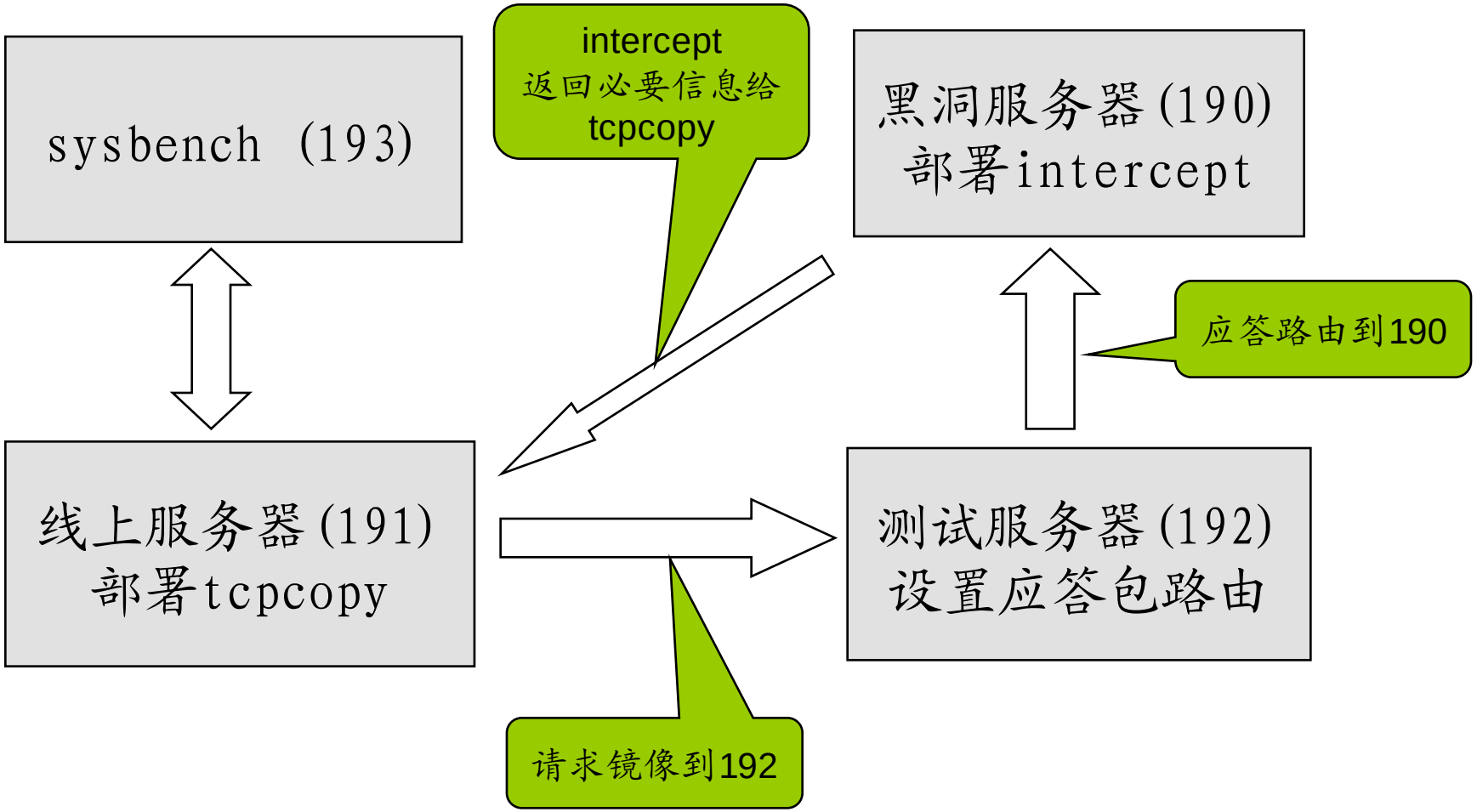
4、代码量

skip方式：300行

认证方式：900行

5、演示

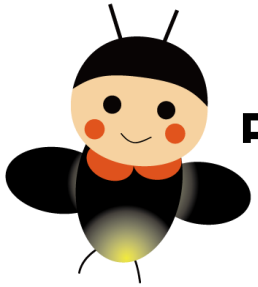
部署图


sysbench (193)
intercept
返回必要信息给
tcpcopy
黑洞服务器(190)
部署intercept
应答路由到190
线上服务器(191)
部署tcpcopy
测试服务器(192)
设置应答包路由
请求镜像到192

MySQL.avi

2014年11月中华架构师大会预告

演讲主题	演讲嘉宾	公司名称	职位/职称
待定	朱超	360	中间件研发负责人
TFS技术架构及运维	张友东	阿里云	TFS研发负责人
待定	黄俊	国药集团	常务副总经理
golang实时消息推送架构实战	毛剑	金山网络	移动游戏技术经理
MyCAT之前世今生	吴治辉	惠普中国	系统架构师
雪球的架构实践	王栋	雪球财经	CTO
待定	刘建平	热璞科技	技术总监



中华数据库
行业协会

- 中华数据库行业协会
- 官方网站：www.zhdba.com
- 官方微信平台：zhdba2014
- 官方微博：中华数据库行业协会ZHDBA
- 技术交流QQ群：91596001