



Dotouch XPRO 云测网络仿真测试工具 配置指南

V2.0R3

声明

Copyright © 2022 北京触点互动信息技术有限公司及其许可者版权所有，保留一切权利。

未经北京触点互动信息技术有限公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。



Dotouch及图标 触点互动 北京触点互动信息技术有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生变更，恕不另行通知。

目录

第 1 章	前言.....	5
1.1	文档介绍	5
1.2	声明.....	5
1.3	文档约定	5
1.4	技术支持	6
第 2 章	基本概念	7
2.1	关于 XPRO 云测网络仿真测试工具.....	7
2.2	测试场景与拓扑.....	7
2.2.1	串接测试场景.....	7
2.2.2	并接测试场景.....	7
2.2.3	单臂测试场景.....	8
2.3	客户端概念说明.....	8
2.4	服务端概念说明.....	9
第 3 章	配置指南	10
3.1	工程.....	10
3.2	系统配置	13
3.2.1	开放平台	13
3.2.2	用户管理.....	13
3.2.3	外部攻击库	14
3.2.4	L3 回放库管理	15
3.2.5	病毒库管理	15
3.2.6	L7 回放库管理	16
3.2.7	系统信息.....	16
3.3	接入配置	17
3.3.1	PPPoE.....	17
3.3.2	DHCP	20
3.4	网口设置	22
3.5	变量设置	24
3.6	媒体对象	25
3.7	客户端.....	26
3.7.1	客户端子网配置.....	26
3.7.2	客户端网络配置.....	27
3.7.3	客户端负载配置.....	28
3.7.4	客户端动作配置.....	29
3.8	服务端.....	48
3.8.1	服务端子网配置.....	48
3.8.2	服务端网络配置.....	49
3.8.3	服务端 Profiles 配置	49
3.9	关联.....	61
3.9.1	服务端和客户端关联.....	61
3.9.2	添加测试订单.....	62

3.9.3	协议篡改规则配置	62
3.10	测试订单	65
3.11	报表	70
3.11.1	网口报表	70
3.11.2	测试用例报表	71
3.11.3	URL 统计报表	71
3.11.4	应用统计报表	71
3.11.5	RTCP 报表	72
3.11.6	RTP 报表	72
3.11.7	RTP 详细报表	73
3.11.8	RTSP 报表	73
3.11.9	CUSP 报表	73
3.11.10	CUSP 用户接入报表	74
3.11.11	用户接入报表	74
3.12	终端	75
第 4 章	L3 Throughput 配置指南	76
4.1	工程	76
4.2	网口设置	76
4.3	L3 Throughput	76
4.4	运行	78
4.5	订单列表	78
4.6	报表	80
4.7	终端	80
第 5 章	L2 replay 配置指南	81
5.1	工程	81
5.2	网口设置	81
5.3	报文捕获	82
5.4	报文资源管理	82
5.5	回放	83
5.6	运行	83
5.7	测试订单	84
5.8	报表	84
5.8.1	网口报表	84
5.8.2	测试用例报表	85
5.9	终端	85
第 6 章	Attack 配置指南	86
6.1	工程	86
6.2	系统配置	86
6.3	接入配置	86
6.4	网口配置	86
6.5	变量设置	86
6.6	媒体对象	86
6.7	客户端	86

6.7.1	客户端子网配置.....	86
6.7.2	客户端网络配置.....	86
6.7.3	客户端负载配置.....	86
6.7.4	客户端动作配置.....	86
6.8	关联.....	89
6.9	测试订单.....	89
6.10	报表.....	89
6.11	包构建器.....	89
6.12	终端.....	90
第7章	RFC2544 配置指南	90
7.1	工程.....	90
7.2	系统配置.....	90
7.3	接入配置.....	90
7.4	网口配置.....	91
7.5	变量设置.....	91
7.6	媒体对象.....	91
7.7	客户端.....	91
7.7.1	客户端子网配置.....	91
7.7.2	客户端网络配置.....	91
7.7.3	客户端负载配置.....	91
7.7.4	客户端动作配置.....	91
7.8	关联.....	91
7.9	测试订单.....	92
7.10	报表.....	93

第1章 前言

1.1 文档介绍

本手册对北京触点互动信息技术有限公司的 XPRO 云测网络仿真测试工具系列产品的安装及配置方法进行说明。

1.2 声明

本手册面向具备一定技术能力的软件开发工程师/测试工程师使用，使用人员至少具备基本的 Linux 系统操作能力及基础的网络技术知识。

1.3 文档约定

约定	描述
	注意事项.

条目	描述/全称
DUT	Device Under Test 被测设备
DPDK	Data Plane Development Kit 数据平面开发套件
Client	业务层面的客户端，如 HTTP Client, FTP Client
Server	业务层面的服务端，如 Web Server, FTP Server
HTTP	Hyper Text Transfer Protocol 超文本传输协议
FTP	File Transfer Protocol 文件传输协议
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer 基于安全套接层的 HTTP
SSL	Secure Sockets Layer 安全套接层
TLS	Transport Layer Security 传输层安全
DNS	Domain Name System 域名系统
RTSP	Real Time Streaming Protocol 实时流传输协议
MODBUS	串行通信协议
NETCONF	网络配置协议
OPCUA	通信接口协议
L2TP	工业标准的 Internet 隧道协议
HANDLE	工控协议
SMTP	电子邮件传输协议

POP3	Post Office Protocol - Version 3 邮局协议
IPSEC	Internet Protocol Security 安全协议包
SIP	Session Initiation Protocol, 会话初始协议
MQTT	Message Queuing Telemetry Transport 消息队列遥测传输
COAP	Constrained Application Protocol 受限应用协议

1.4 技术支持

Email: support@dotouch.com.cn

第2章 基本概念

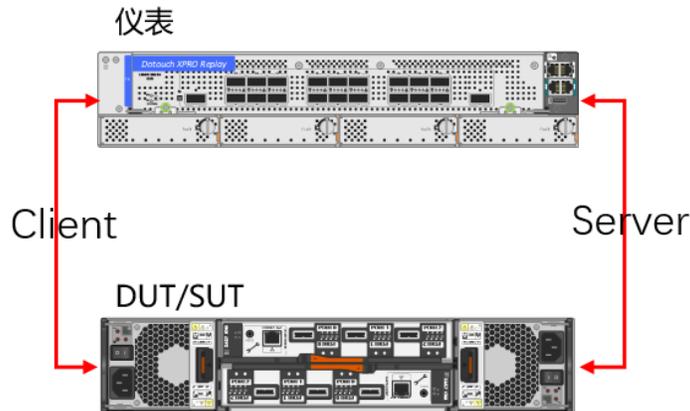
2.1 关于 XPRO 云测网络仿真测试工具

XPRO 云测网络仿真测试工具（是一款面向 4~7 层网络协议仿真的专业测试仪表，用来仿真各类网络协议及应用、网络攻击的流量，同时具备高性能、高可扩展性的特点，目前业内同类型产品为 Spirent 的 Avanzance 与 IXIA 的 BreakPoint System。

2.2 测试场景与拓扑

2.2.1 串接测试场景

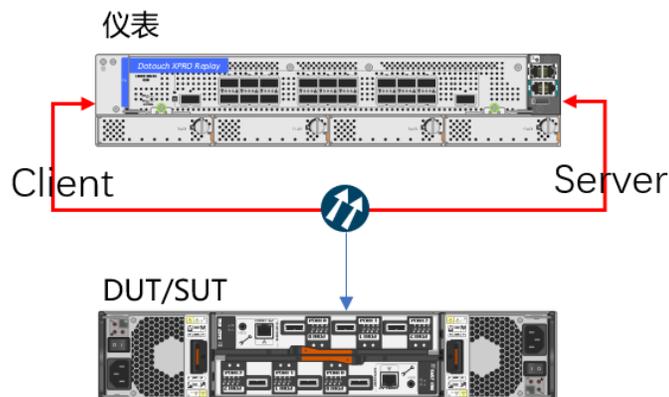
串接测试作为测试过程中最常见的测试场景，一般用来测试如 DUT 的带业务转发性能、行为封堵、流量管理，典型测试对象是网关/网桥模式部署下的防火墙、负载均衡、VPN、上网行为管理、流控管理等类型设备，典型测试拓扑如下：



! 测试时客户端与服务端可位于同一台服务器之上，此时仪表相当于自环状态，也可分布在两台不同的服务器之上，如服务器 A 充当 HTTP 客户端，服务器 B 充当 Web 服务端，这样客户端和服务端可以独占各自服务器硬件的 CPU 资源与内存资源，提升性能。

2.2.2 并接测试场景

并接测试作为测试过程中最常见的测试场景，通过分光器件、交换机/路由器镜像等将仪表产生的流量复制后送至被测设备，一般用来测试如 DUT 的协议识别准确性，典型的测试对象是运营商 DPI 设备，APM/NPM 等无需进行流量转发的设备，也可用来测试并接模式下的行为审计等类型设备。典型测试拓扑如下：

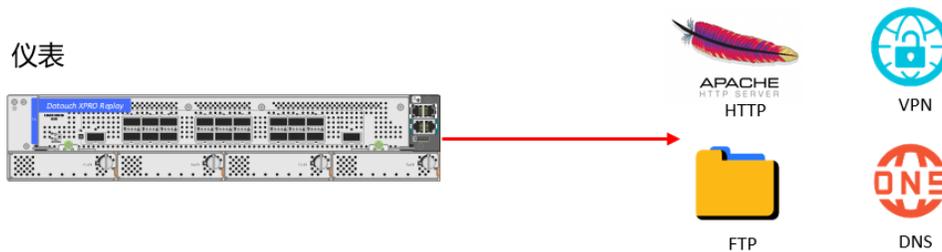




测试时客户端与服务端可位于同一台服务器之上，此时仪表相当于自环状态，也可分布在两台不同的服务器之上，如服务器 A 充当 HTTP 客户端，服务器 B 充当 Web 服务端，这样客户端和服务端可以独占各自服务器硬件的 CPU 资源与内存资源，提升性能。

2.2.3 单臂测试场景

在串接测试与并接测试场景下，都是使用仪表来充当业务的 Client 端与 Server 端，但在单臂测试场景下，仪表一般仅充当 Client 端或者 Server 端，用来测试目标服务的功能与性能，如使用仪表充当 DNS 客户端，向客户自有的 DNS 服务器发起海量的 DNS 请求，测试 DNS 服务器的极限性能，因此单臂测试模式测试对象往往是业务系统，如 DNS 服务、Web 服务等等，典型测试拓扑如下：



单臂模式部署时，仪表既可充当客户端，也可充当服务端。

2.3 客户端概念说明

在仪表仿真业务时，会仿真业务的客户端与服务端，如仿真 HTTP 业务时，会模拟海量 HTTP Get 向 Server 发起请求，因此客户端与服务端是站在业务的角度来定义的。

Client 端作为业务请求的发起方，在测试时，根据所配置 Testcase 仿真所需业务流量，客户端的定义是应用的发起端，如发起 HTTP 请求的 HTTP Client，发起 FTP 请求的 FTP Client，发起域名解析请求的 DNS Client。

在定义客户端时，需要定义客户端发起请求时的源/目 IP 范围，传输层端口（源端口范围/访问的目的端口范围），应用层的请求参数以及业务发起模型。

在配置客户端时有如下关键步骤：

- 定义客户端的子网范围，如仿真 10000 个用户向服务端发起业务请求，这 10000 个用户的源/目 IP 范围就是客户端的子网，在配置时，对应的是“客户端”的“客户端子网”配置项，从协议栈的角度看，子网配置的是客户端发起请求时的 IP 层信息。
- 定义客户端的在发起业务请求的传输层端口信息，如仿真 10000 个用户向服务端发起业务请求，这 10000 个用户在发起业务请求时，传输层所使用的源端口及将要访问的目的端口，在配置时，对应的是“客户端”的“客户端网络”配置项，从协议栈的角度看，客户端网络配置的是客户端发起请求时的传输层信息。
- 定义客户端的在发起业务请求的业务模型，包括定义新建速度，并发规模，新建与并发的优先级，以及流量的爬坡时间，稳定测试时间，下坡时间。
- 定义客户端的在发起业务请求的应用层信息，如仿真 10000 个用户向服务端发起业务请求，此处定义具体发起的业务类型，如发起的是 HTTP 业务还是 FTP 业务抑或是 DNS 业务，用户可自定义应用层的详细参数，如 HTTP 头部字段，Method 类型，POST 内容等等，在配置上对应的是“客户端动作”配置项，从协议栈的角度看，客户端动作配置的是客户端发起请求时的应用层信息。
- 仪表在进行仿真业务时，为了提高配置的灵活性，将 IP 层信息，传输层信息，应用层信息，业务模型解耦，

各个部分独立配置，以使用户通过自由组合生成不同的客户端配置，因此当完成客户端子网、客户端网络、客户端负载、客户端动作配置后，还需完成最后一个步骤，将子网配置、网络配置、负载配置、动作配置进行组合，最终生成一个完整的客户端配置。

2.4 服务端概念说明

Server 端作为请求的响应端，在测试时，按照所配置规则响应客户端请求。

在定义服务端时，需要定义服务端提供服务的 IP 范围，提供服务的端口以及响应客户端请求时应用层参数。

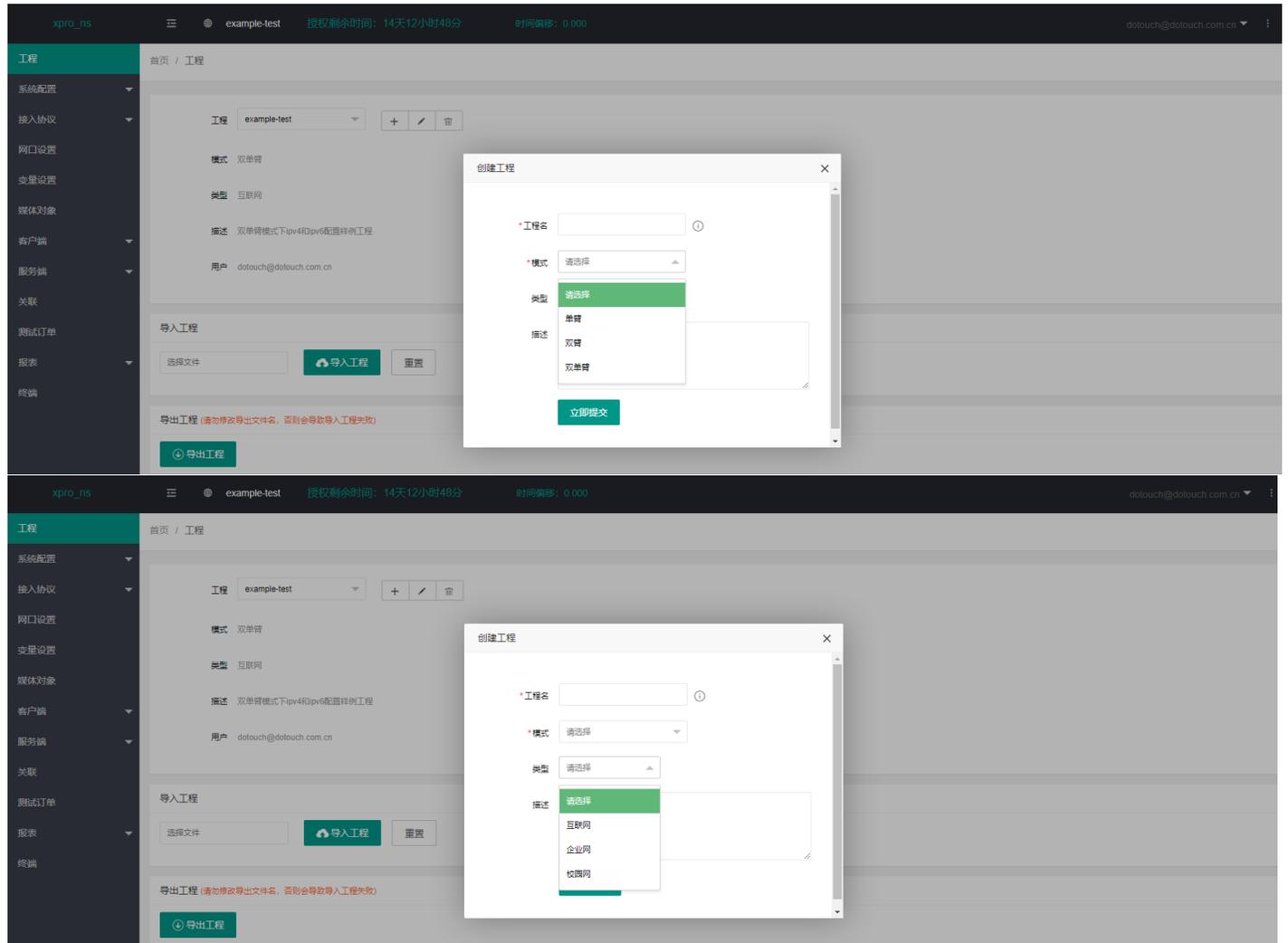
在配置服务端时有如下关键步骤：

- 定义服务端的子网范围，如服务端仿真 1 个或多个 Web Server，Web Server 的 IP 范围就是服务端的子网，在配置时，对应的是“服务端”的“服务端子网”配置项。从协议栈的角度看，子网配置的是服务端的 IP 层信息。
- 定义服务端的传输层端口信息，如服务端仿真 1 个或多个 Web Server，Web Server 提供 web 服务的四层端口范围就是服务端的网络，在配置时，对应的是“服务端”的“服务端网络”配置项，从协议栈的角度看，服务端网络配置的是服务端对外提供服务的四层端口，服务端将在此处所配置的端口上监听业务请求。
- 定义服务端的在响应业务请求时的应用层信息，如服务端响应客户端的 HTTP 请求，用户可自定义服务端响应时的应用层的详细参数，如 HTTP 响应码是 200 OK 还是 404 Not Found 等等，在配置上对应的是“Profiles”配置项，从协议栈的角度看，服务端 Profiles 配置的是服务响应请求时的应用层信息。
- 仪表在进行应用仿真时，为了提高配置的灵活性，将服务端 IP 层信息，传输层信息，应用层信息解耦，各个部分独立配置，以使用户通过自由组合生成不同的服务端配置，因此当完成服务端子网、服务端网络、服务端 Profiles 配置后，还需完成最后一个步骤，将子网配置、网络配置、业务配置进行组合，最终生成一个完整的服务端配置。

第3章 配置指南

3.1 工程

工程作为测试任务最高的组织形式，定义了一个完整的测试任务。



在工程菜单页，管理员可自行添加、删除及编辑测试工程。

点击图标 ，新增工程，根据业务需求选择对应的模式和类型

点击图标 ，编辑指定工程

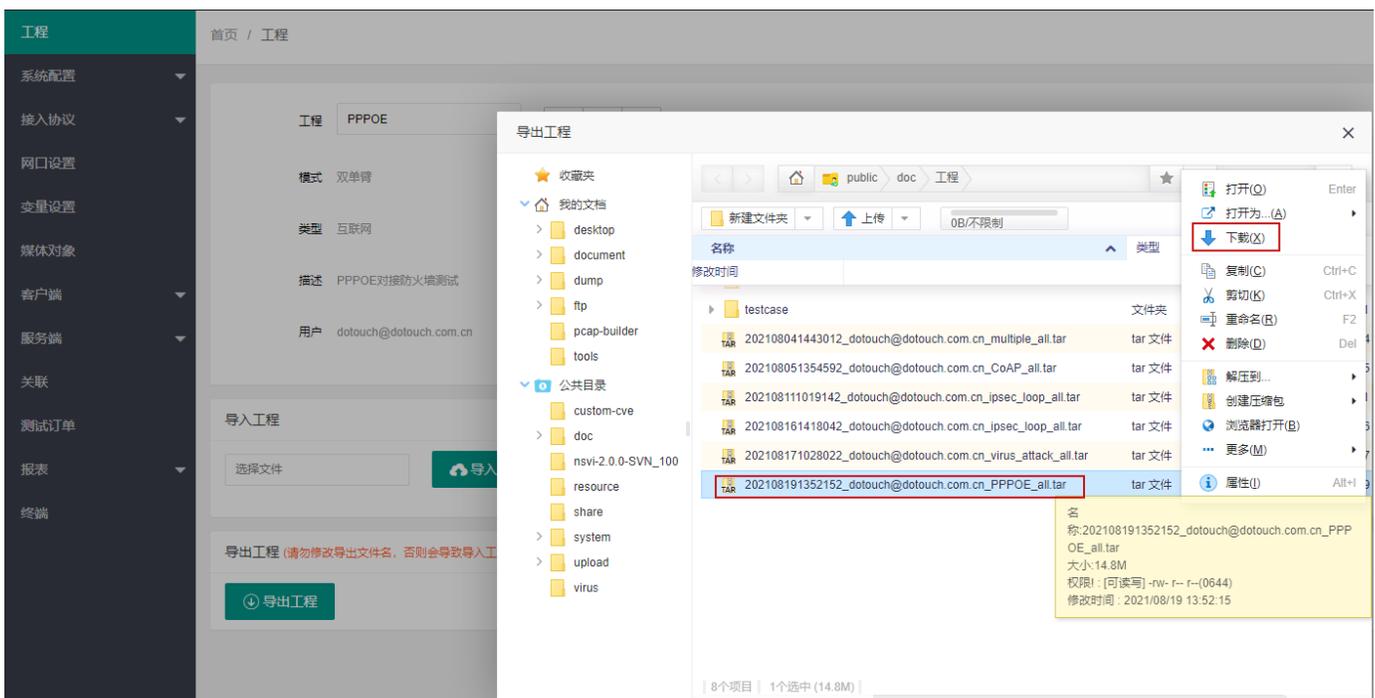
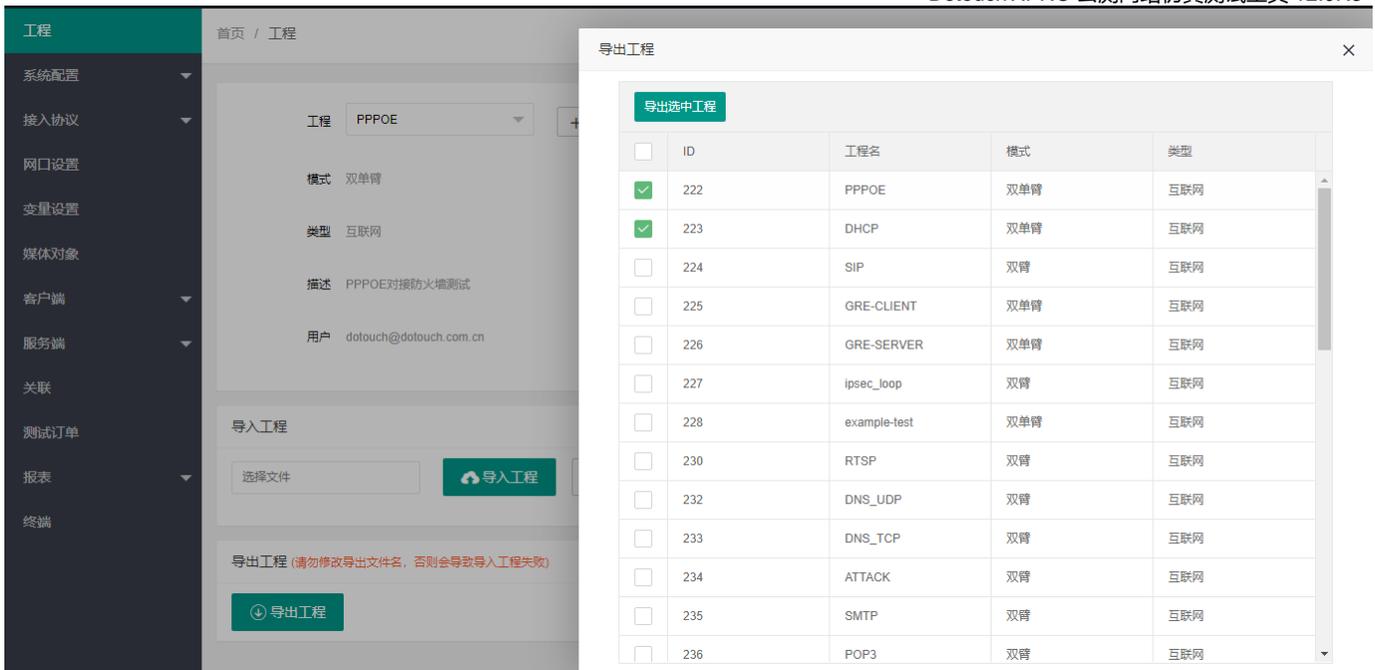
点击图标 ，删除指定工程



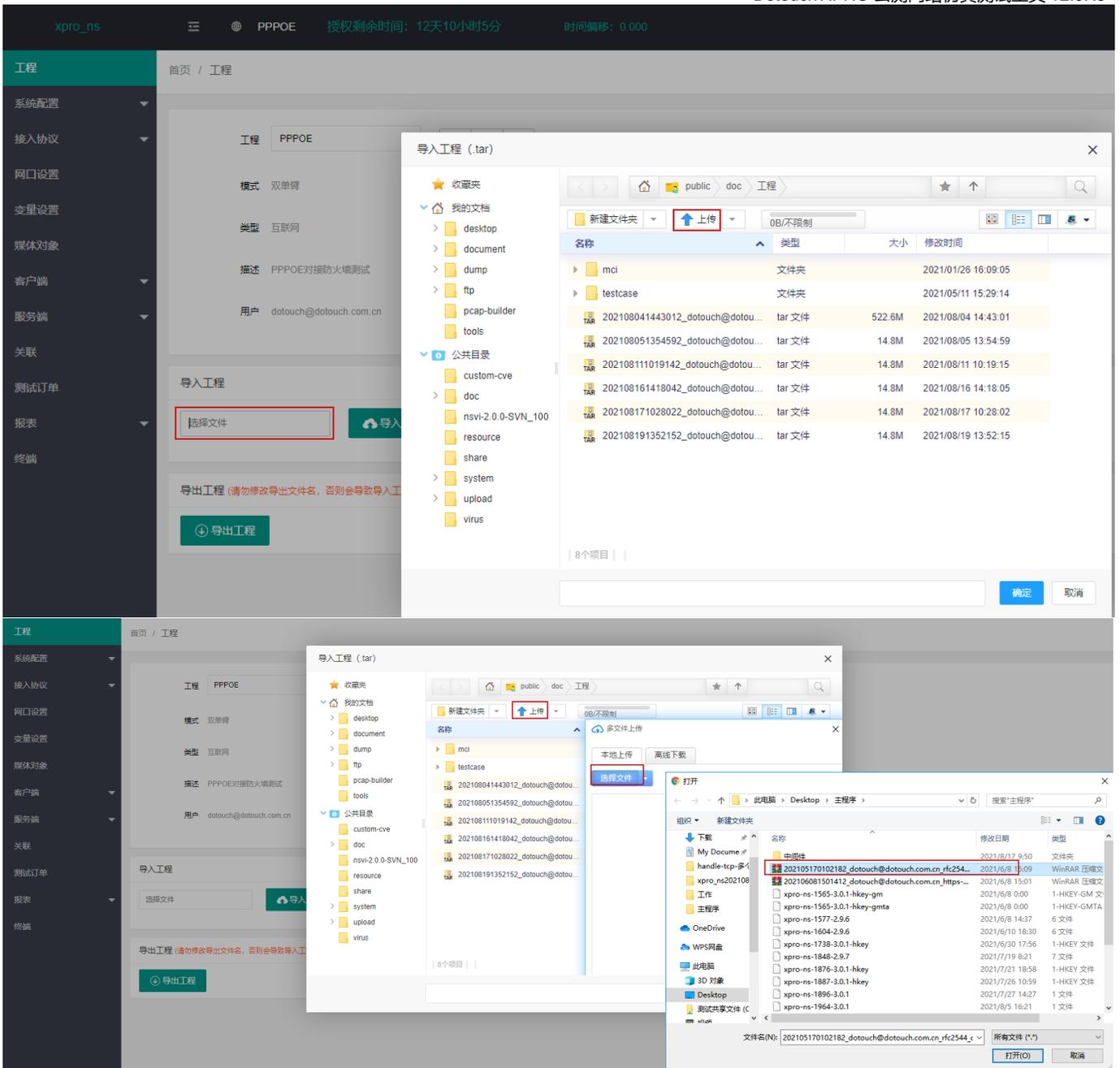
第一次使用时，必须在新建工程后方可配置其他功能模块。

点击图标  可以将指定工程导出。支持同时导出多个工程。

导出的工程在资源管理器里，鼠标右键可以下载到本地。



点击 导入工程下面的“选择文件”输入框，可以选择 已导出的工程，若需要导入的工程不在资源管理器中，可以点击资源管理器中的 上传 按钮，将工程出上传到资源管理器中，再点击  按钮，可以将选择的工程导入。



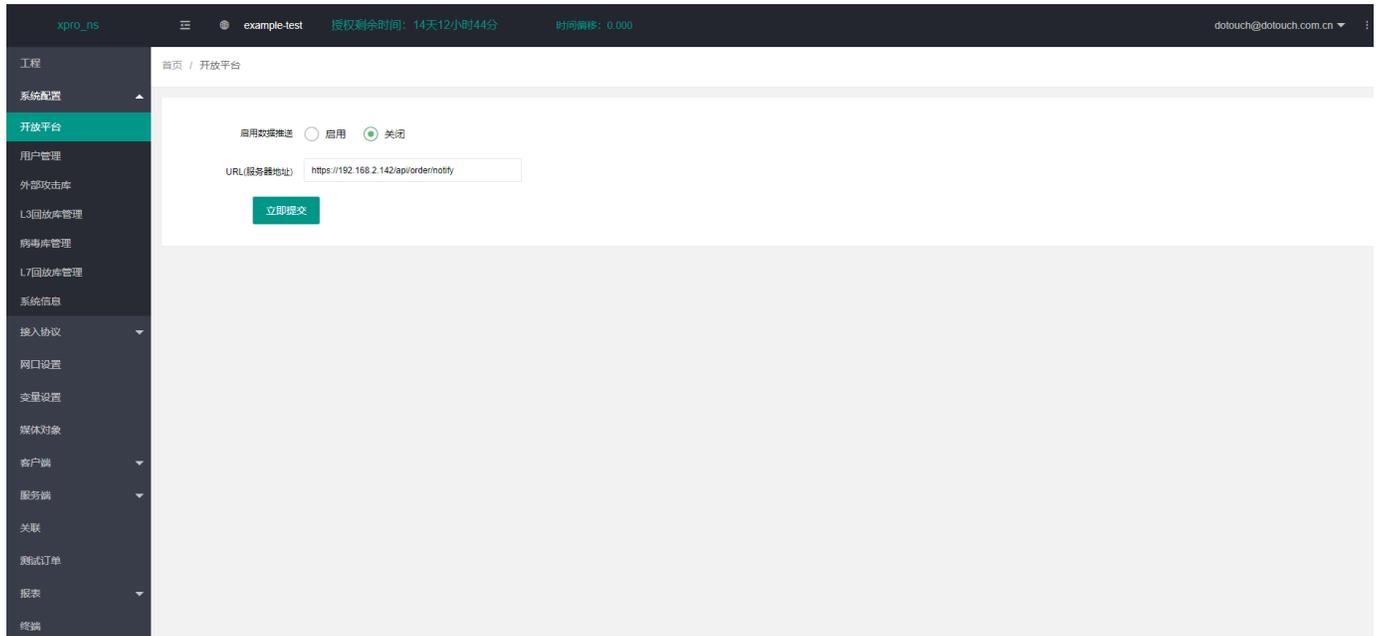
⚠️ 工程导入仅支持相同版本，或是高版本导入低版本导出的工程。低版本导入高版本导出的工程会出现导入失败的情况。

3.2 系统配置

系统配置中的参数对所有的工程都生效

3.2.1 开放平台

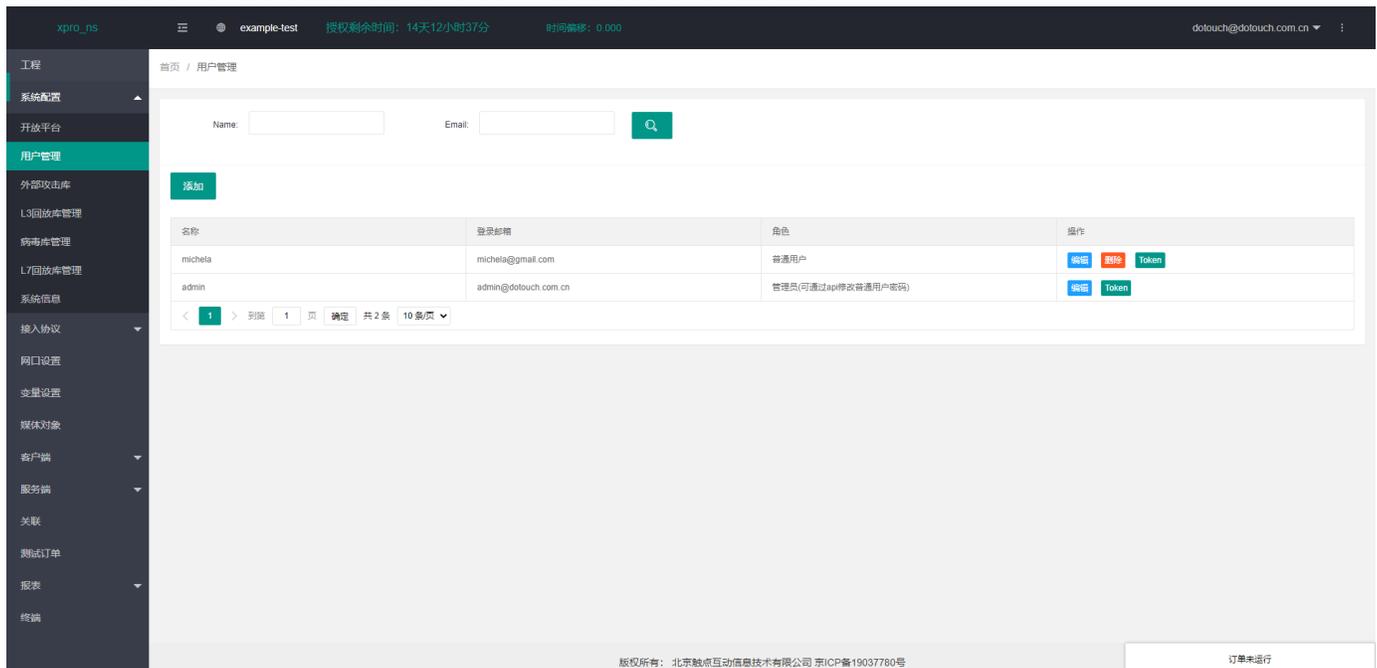
开放平台中可以配置第三方的 url 接口，系统可以在测试时向指定的 url 推送测试输出的数据



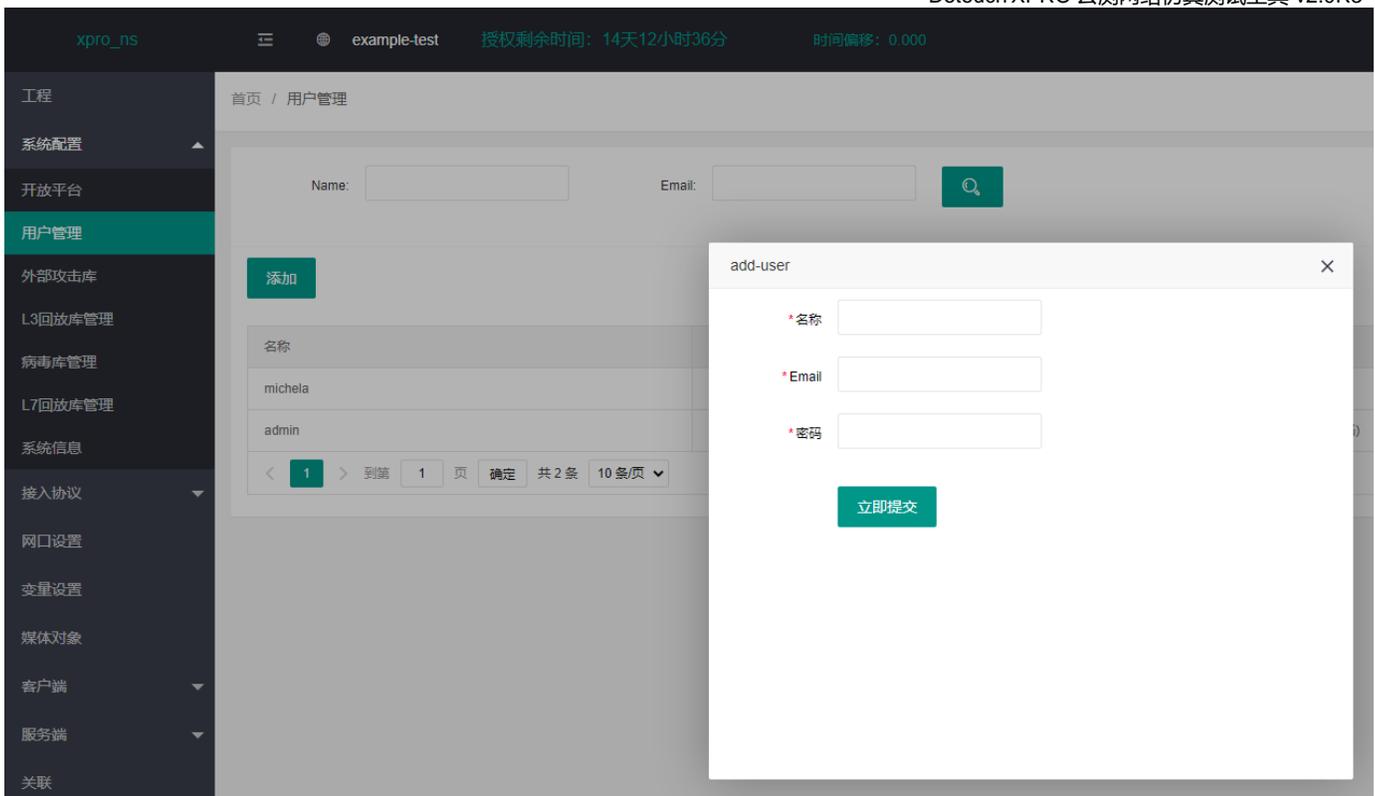
此功能默认为关闭，根据需要进行配置。

3.2.2 用户管理

用户管理页面可以给系统添加新用户，并且对用户账户进行编辑管理。



点击页面上的 **添加** 按钮，打开新增用户的编辑页面



名称：自定义的账户名称

Email：新增的账户登录用的邮箱，无需校验

密码：账户的登录密码

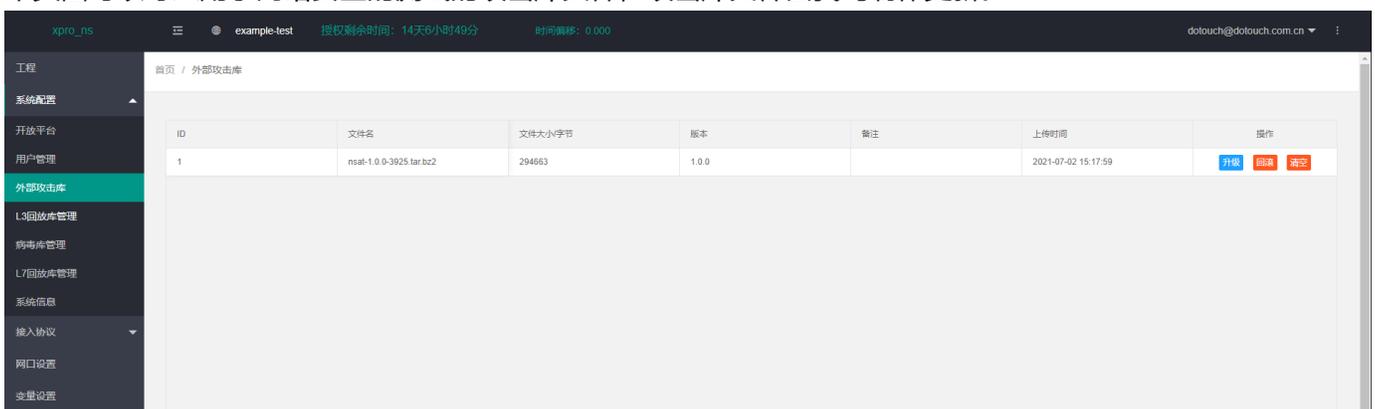
提交保存后就可以使用新的账户登录系统了。页面上同时还可以编辑和删除已有账户。



dotouch@dotouch.com.cn 是默认系统账户，不在“用户管理”页面展示，可在右上角 账号位置 修改密码

3.2.3 外部攻击库

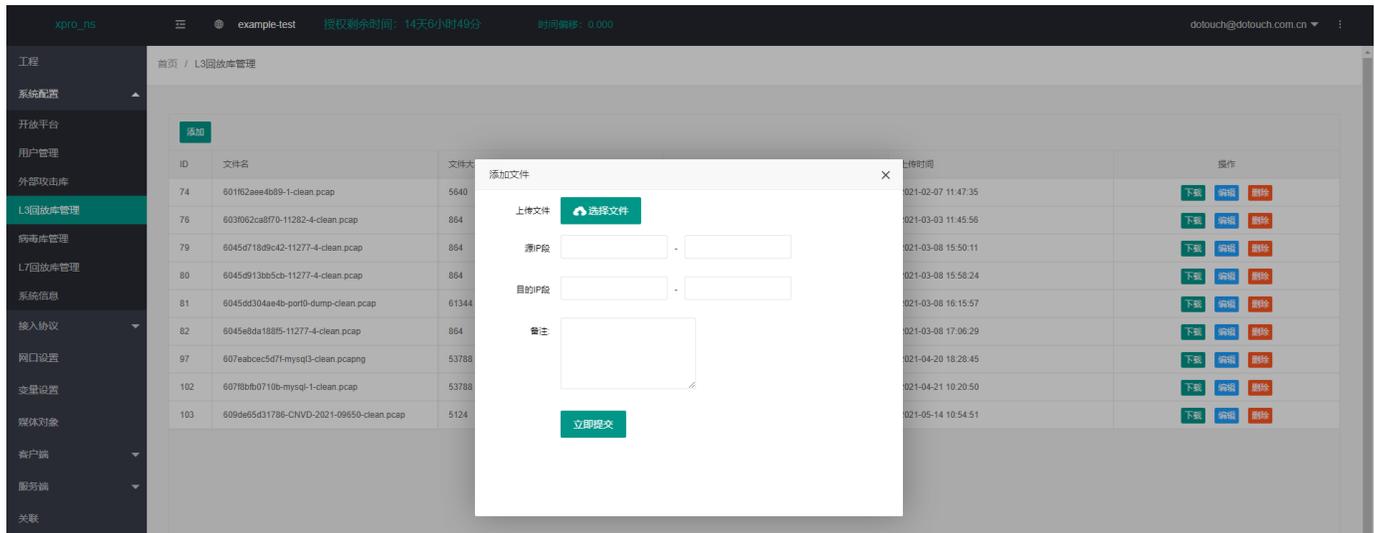
本页面可以导入用于网络安全的测试的攻击库文件，攻击库文件由我司制作更新。



上传后可在 Attack 子系统中模拟网络攻击行为的测试中调用上传的攻击库文件，同时页面还有回滚和清空的功能。

3.2.4 L3 回放库管理

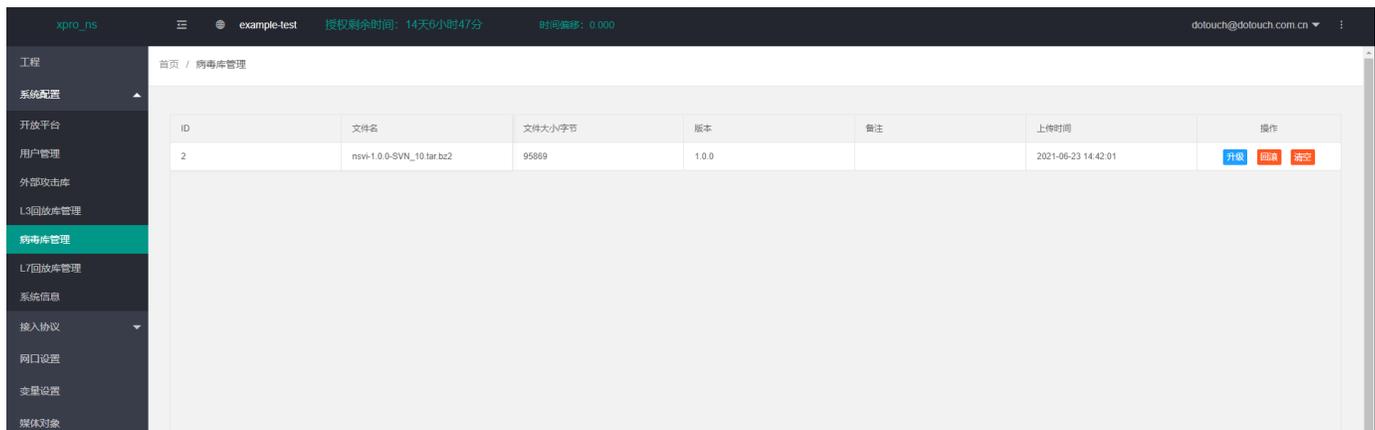
此页面可以导入本地的 pcap 报文，并按照条件过滤，上传到系统中。在 Attack 的子系统中可以选择这里上传的文件，测试时端口按照上传的报文进行回放，实现自定义报文测试。
点击 **添加** 按钮打开添加页面



上传 pcap 文件后，可以输入源 ip 和目的 ip 地址段，然后提交。系统会按照填写的地址段范围过滤上传的 pcap 包中的报文，然后生成新的 pcap 文件并保存。支持上传多个文件，也可以将文件下载到本地，或者编辑、删除已有文件。

3.2.5 病毒库管理

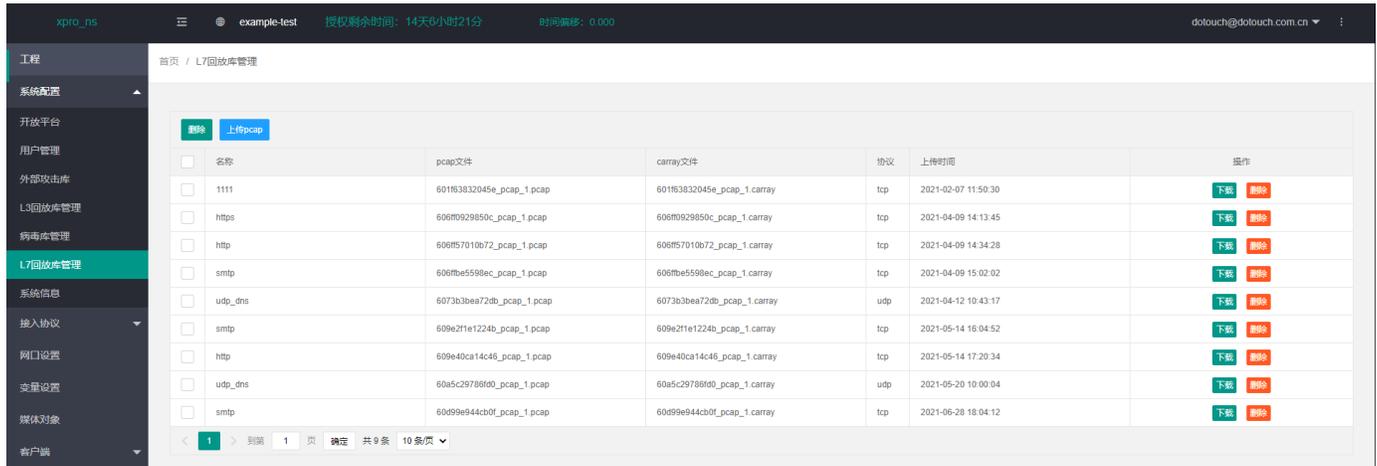
本页面可以导入用于网络安全的测试的病毒库文件，病毒库文件由我司制作更新。



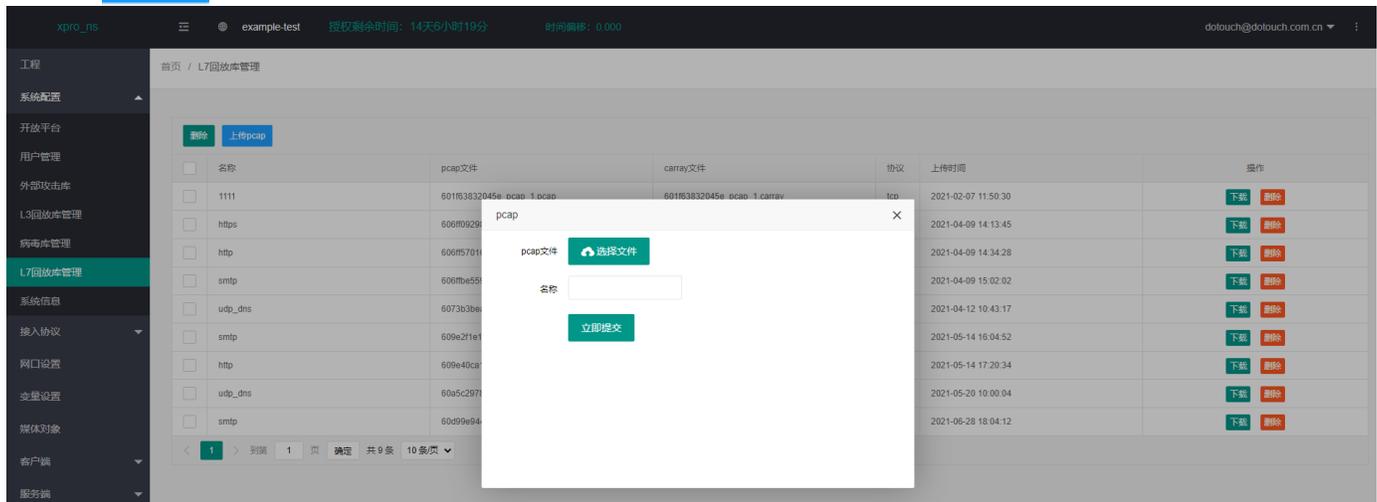
上传后可在 Attack 子系统中模拟网络病毒攻击行为的测试中调用上传的攻击库文件，同时页面还有回滚和清空的功能。

3.2.6 L7 回放库管理

此页面可以导入本地的 pcap 报文，目前只支持单条流的 pcap 文件上传，上传的 pcap 文件在 replay 协议中以回放文件-选择 L7 回放样包进行引用



点击 **上传pcap** 按钮，进入上传 pcap 文件页面，对已经上传的 pcap 文件支持下载到本地或者删除操作。



3.2.7 系统信息

此页面可以查看系统的内存 和 存储空间 的使用情况等信息，还有 测试硬盘写入速率，清理抓包文件 等功能。

点击 **磁盘测速** 按钮，仪表会自动测试硬盘写入速率，测试完成后会在页面展示。

点击 **清理抓包文件** 按钮，会清理 /var/www/KODExplorer/data/User/demo/home/dump/ 目录下所有抓包文件。

系统负载和内存

1分钟: 0.46 总内存: 15886M
5分钟: 0.46 剩余: 4781M
15分钟: 0.26 使用率: 69.90%

磁盘管理

磁盘测速 清理压缩包

文件系统	总大小	已使用	剩余	已使用占比%	挂载点
/dev/mapper/centos-root	26G	21G	5.3G	80%	/
/dev/sda1	1014M	179M	836M	18%	/boot
devtmpfs	4.8G	0	4.8G	0%	/dev
tmpfs	1.6G	0	1.6G	0%	/run/user/0
tmpfs	7.8G	0	7.8G	0%	/sys/fs/cgroup
tmpfs	7.8G	348K	7.8G	1%	/dev/shm
tmpfs	7.8G	34M	7.8G	1%	/run

3.3 接入配置

3.3.1 PPPoE

PPPoE 页面用来添加 PPPoE 请求的客户端配置，配置后可以自动生成一个关联项。IP 协议版本支持 ipv4、ipv6、ipv4&ipv6，用户文件用来配置生成用户端 mac 地址，vlan 等。

首页 / PPPoE

+ 添加

名称	IP协议版本	客户端网卡	文件	心跳时间	延时下线时间	重试次数	用户上线速率	活跃用户数	用户活跃时长	最大连接数	稳定时间	操作
无数据												

点击  添加 按钮，进入到配置界面

PPPoE

*名称	pppoe-ipv4		
IP协议版本	ipv4		
客户端网卡	port0		
*用户文件	ic/home/resource/pppoe-ipv4_file	用户文件模板下载	选择用户文件 生成用户文件
*心跳时间	0	秒	
*延时下线时间	0	秒	
*重试次数	3		
支持认证方式	PAP、CHAP-MD5		

用户上线行为

*用户在线时长	7200000000	us
*最大拨号数	1000	
使用应用负载	<input type="radio"/> OFF	不带承载时不能使用应用负载
上线速率	10	users/sec
活跃用户数	1000	
测试时长	15	秒
拖尾时间	20	秒

名称：填写客户端名称

客户端网卡：选择测试 PPPoE 协议的网卡

用户文件：为了避免每个 PPPoE 请求包的参数都相同，自定义 PPPoE 请求报文的变量。这里支持上传模板和自动生成。

可定义的变量包括：mac、PPPOE 拨号的用户名和密码、外层 vlan 和内层 vlan

心跳时间：PPPoE 心跳间隔

延时下线时间：PPPoE 用户在线时间结束后，延迟下线的的时间

重试次数：PPPoE 拨号失败时重试的测试

支持认证方式：支持 pap 和 CHAP-MD5 两种方式

PPPoE 客户端新建完成后，关联项自动生成，无需手动添加

点击 生成用户文件 可以生成用户文件

信息 ×

* 文件名:

* MAC: ⓘ

MAC变量: {\$mac_var} 范围: - 步长:

* 用户: ⓘ

用户变量: {\$user_var} 范围: - 步长:

* 密码: ⓘ

密码变量: {\$pwd_var} 范围: - 步长:

VLAN1(外层): ⓘ

VLAN1变量: {\$vlan1_var} 范围: - 步长:

VLAN2(内层): ⓘ

VLAN2变量: {\$vlan2_var} 范围: - 步长:

立即提交

配置后自动生成的关联项

xpro_ns example-test 授权剩余时间: 14天5小时47分 时间偏移: 0.000 dotouch@dotouch.com.cn

工程 / PPPoE

+ 添加

名称	IP协议版本	客户端网卡	文件	心跳时间	延时下线时间	重试次数	用户上线速率	活跃用户数	用户活跃时长	最大连接数	稳定时间	操作
pppoe	ipv4	null	/var/www/...	0	0	3	100	1000	720000000	40000000	100	编辑 删除

1 到第 1 页 确定 共 1 条 20 条页

xpro_ns example-test 授权剩余时间: 14天5小时48分 时间偏移: 0.000 dotouch@dotouch.com.cn

工程 / 关联

+ 添加测试订单

客户端关联 服务器关联

名称:

<input type="checkbox"/>	+	名称	关联类型	子网类型	子网	协议类型	动作	网情	开始全局负载	负载	权重
<input type="checkbox"/>	+	pppoe	接入网[pppoe-ipv4]						<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	SIP-UDP	用户型	IPv4	client	标准协议	SIP-UDP	sip	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	SIP-TCP	用户型	IPv4	client	标准协议	SIP-TCP	sip	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	HANDLE-UDP	用户型	IPv4	client	标准协议	HANDLE-UDP	handle	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	pop3	用户型	IPv4	client	标准协议	pop3	pop3	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	smtp	用户型	IPv4	client	标准协议	smtp	smtp	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	ftp	用户型	IPv4	client	标准协议	ftp	ftp	<input type="checkbox"/>	负载	100
<input type="checkbox"/>	+	RAW-TLS_v6	用户型	IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS	<input type="checkbox"/>	负载	100

3.3.2 DHCP

DHCP 页面用来添加 DHCP 请求的客户端配置。IP 协议版本支持 ipv4、ipv6、ipv4&ipv6，用户文件用来配置生成用户端 mac 地址，VLAN 等。

名称	IP协议版本	DHCPv6仿真模式	客户端网卡	文件	延时下线时间	重试次数	用户上线速率	活跃用户数	用户活跃时长	最大连接数	稳定时间	操作
DHCP-ipv...	ipv4&v6	DHCPv6&PD	port0	/var/www/KO...	0	3	1	1000	7200000000	40000000	100	编辑 删除
DHCP-ipv...	ipv4&v6	DHCPv6 PD	port0	/var/www/KO...	0	3	1	1000	7200000000	40000000	100	编辑 删除
DHCP-ipv...	ipv4&v6	DHCPv6	port0	/var/www/KO...	0	3	1	1000	2000000	40000000	10	编辑 删除
DHCP_ipv...	ipv6	DHCPv6&PD	port0	/var/www/KO...	0	3	10	1000	7200000000	40000000	12	编辑 删除
DHCP-ipv...	ipv6	DHCPv6 PD	port0	/var/www/KO...	0	3	1	1000	7200000000	40000000	12	编辑 删除
DHCP-ipv6	ipv6	DHCPv6	port0	/var/www/KO...	0	3	1	1000	2000000	40000000	20	编辑 删除
DHCP-ipv4	ipv4		port0	/var/www/KO...	0	3	1	1000	7200000000	40000000	10	编辑 删除

点击 添加 按钮，进入到配置界面

DHCP

*名称

IP协议版本

客户端网卡

*用户文件

延时下线时间 秒

重试次数

用户上线行为

*用户在线时长 us

*最大拨号数

使用应用负载 ON 不带承载时不能使用应用负载

使用应用负载 OFF 不带承载时不能使用应用负载

上线速率 users/sec

活跃用户数

测试时长 秒

拖尾时间 秒

立即提交

重置

点击 [生成用户文件](#) 可以生成用户文件

信息 ×

* 文件名:

* MAC: ⓘ

MAC变量: {\$mac_var} 范围: - 步长:

VLAN1: ⓘ

VLAN1变量: {\$vlan1_var} 范围: - 步长:

VLAN2: ⓘ

VLAN2变量: {\$vlan2_var} 范围: - 步长:

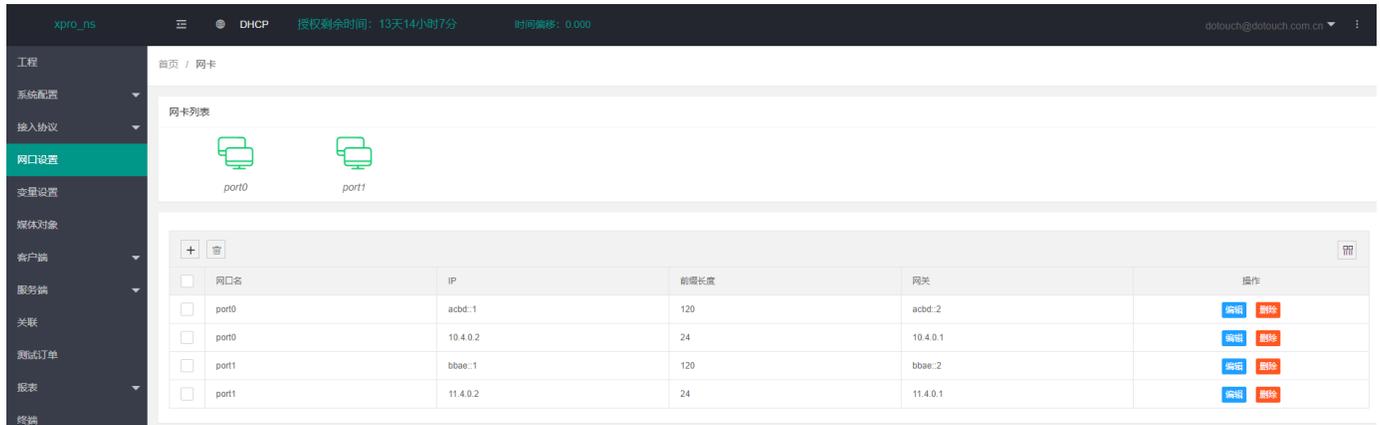
option:

option	value	变量		
		变量名	区间范围	步长

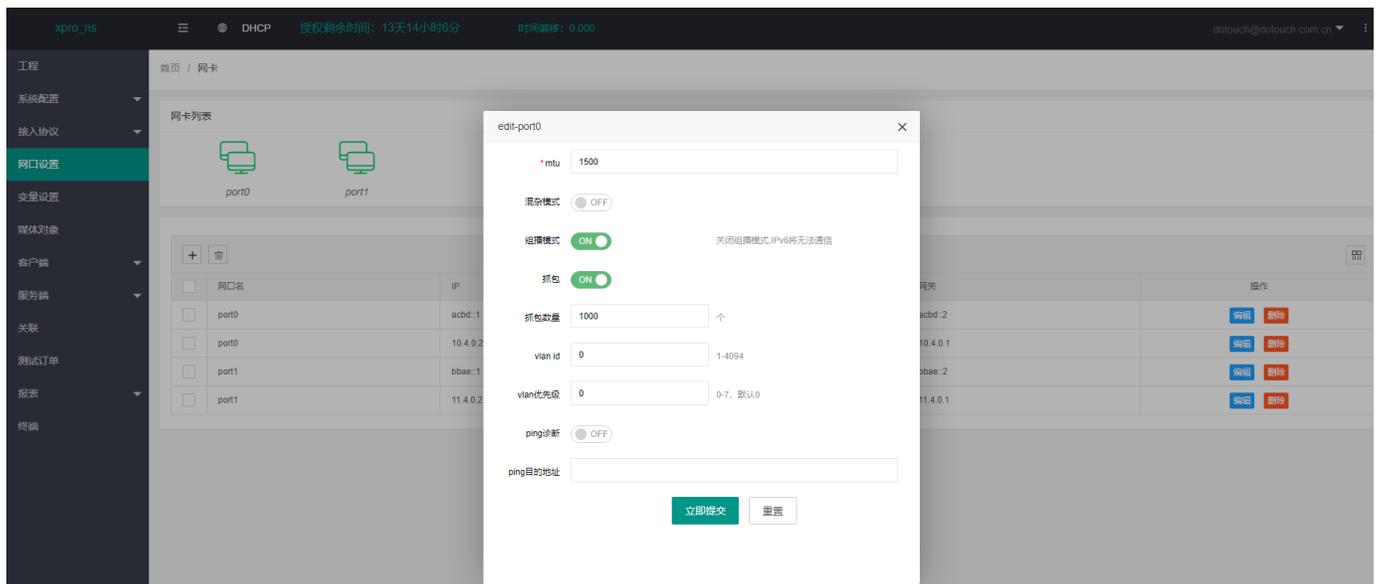
3.4 网口设置

网口设置用来配置设备测试端口的 IP 信息（不含管理口），网卡列表显示的网卡信息由系统自动从设备上读取，无需配置。

将鼠标移动到页面上的网卡  标志处，可以查看网卡信息



点击网卡标志，  可以编辑网卡的配置参数



MTU：配置端口的 mtu 值，默认为 1500

混杂模式：开启或者关闭网口的混杂模式

组播模式：开启或者关闭网口的组播功能，需要注意测试 ipv6 时必须开启此开关

抓包：开启端口抓包的功能，开启后测试运行时端口会自动抓包并保存抓包文件到资源管理器

抓包数量：开启抓包后，配置端口抓包的最大数量

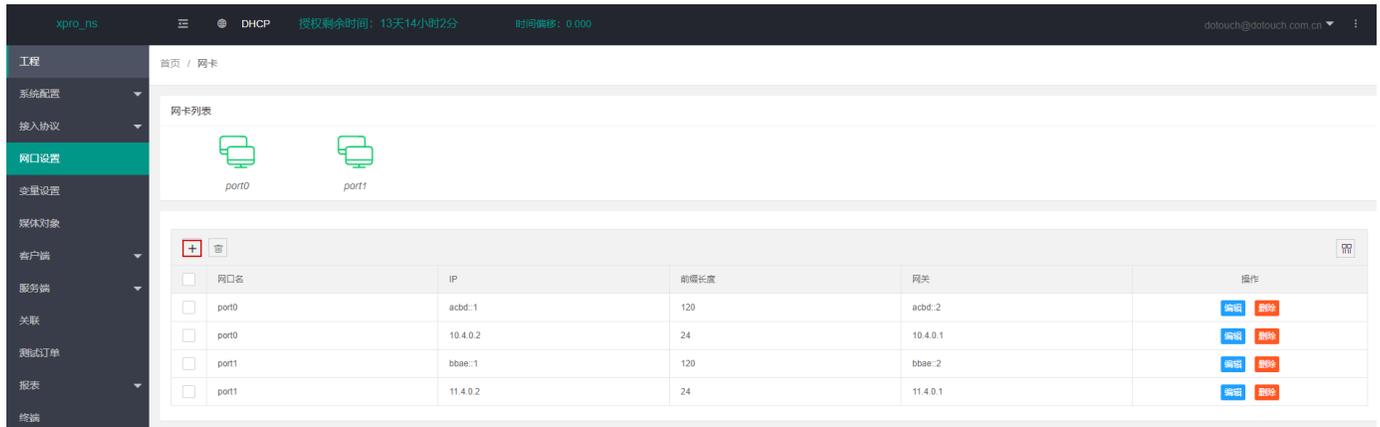
vlan id：配置端口带 vlan id

vlan 优先级：端口带 vlan 时，配置优先级

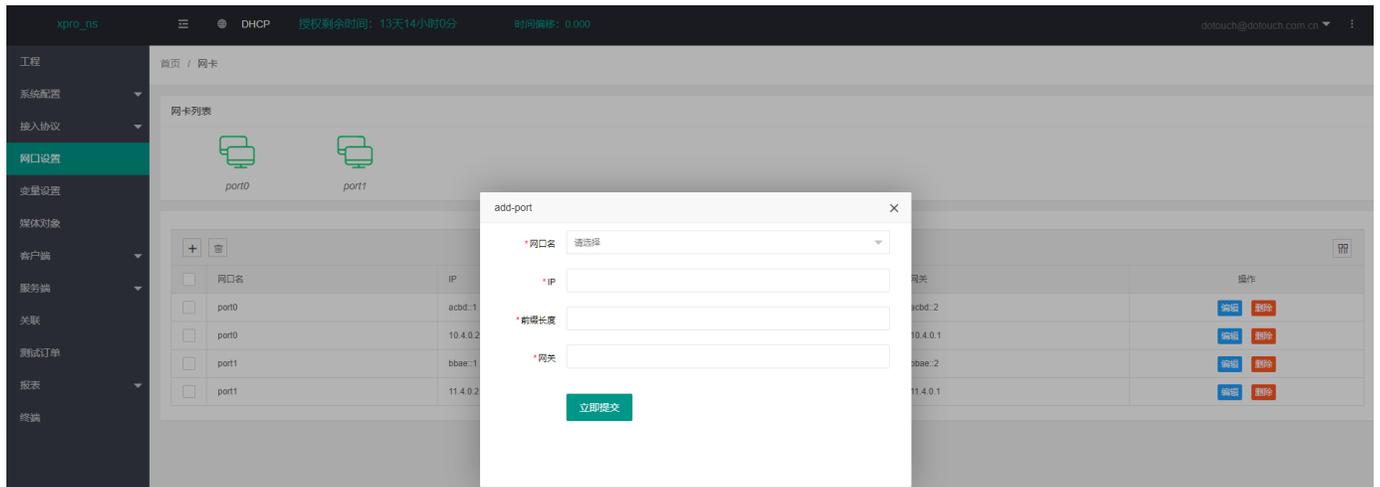
ping 诊断：开启或者关闭网口的 ping 诊断功能

ping 目的地址：开启抓包后，配置 ping 诊断的地址

网口设置页面可以配置网口的 IP 参数



点击 按钮配置打开添加网口 IP 参数的配置页



网口名: 选择所用到的网口

IP 地址: 配置该网口的接口 IP (可按照上图自定义, port0 的 IP 作为 port1 的网关, 反过来 port0 的网关作为 port1 的 ip)

前缀长度: 配置该网口 IP 地址的前缀

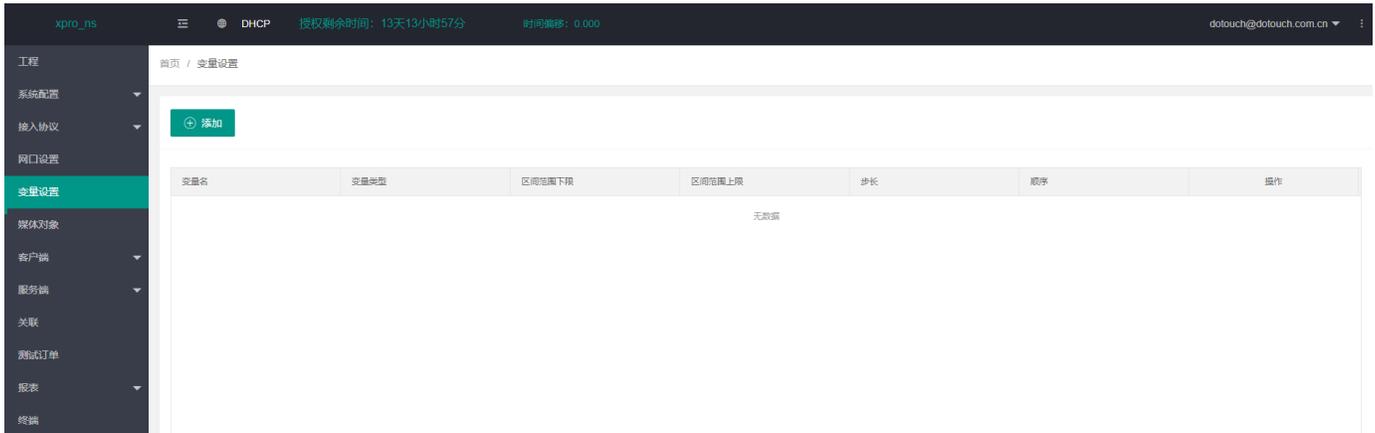
网关: 配置该网口的下一跳 IP 地址

MAC 地址为程序自动获取填入, 无需手动配置

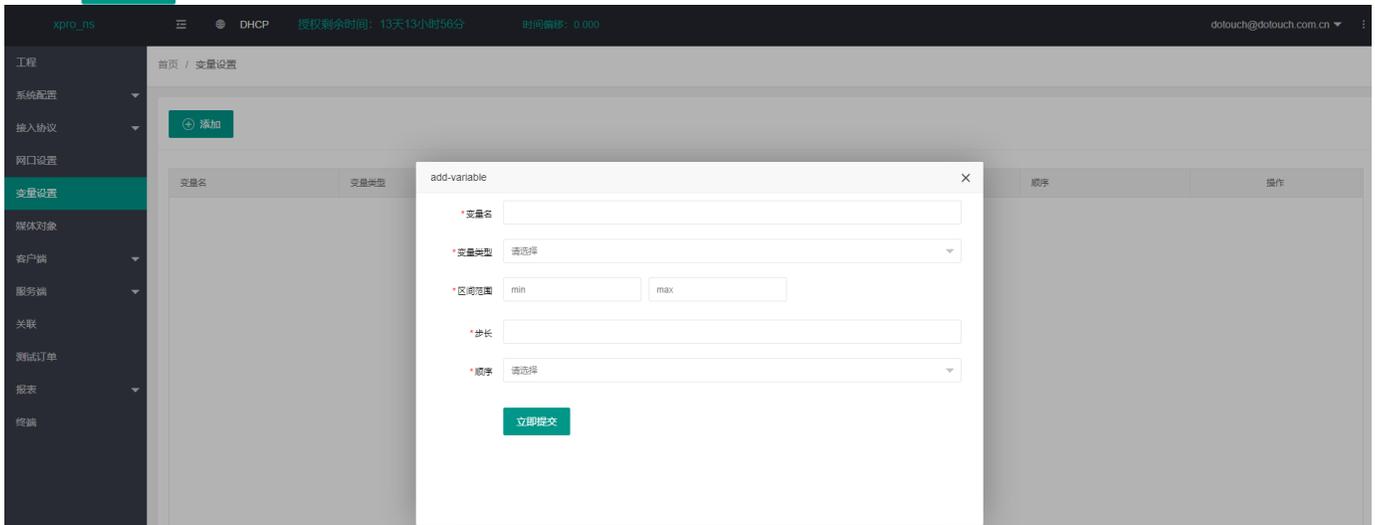
 当前版本不支持通过界面修改管理口 IP, 需自行在 linux 后台修改管理口 IP, 完成管理口 IP 修改后, 请勿使用 service network restart 命令重启网络服务, 请使用 ifdown 和 ifup 命令重启管理网口。如果要打 ipv6 的流量, 需要配上 ipv6 的地址, 同时打开 ipv4 与 ipv6 的流量, 需要在网卡同时配置上 ipv4 与 ipv6 的地址。

3.5 变量设置

该功能模块用来定义变量，用来在仿真 HTTP、https、dns 时调用，按照变量规则生成海量的 HOST 与 URI，避免仿真 HTTP 业务时所仿真的 HTTP 请求的 HOST 与 URI 均相同的情况。



点击 **+** 添加 按钮，进入添加变量页面



变量名：该变量的名称

变量类型：当前仅支持 init 型变量

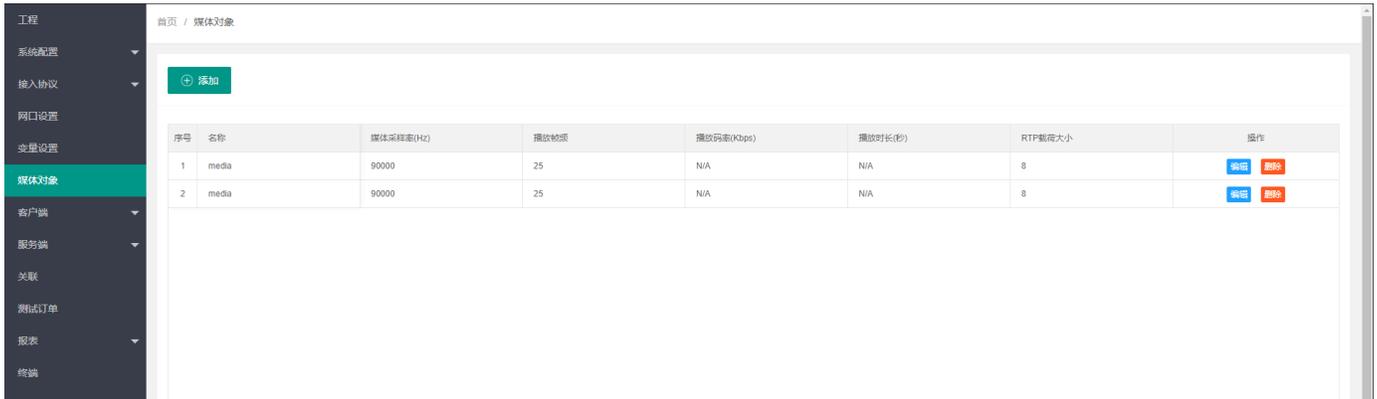
区间范围：变量值的区间范围，如 200~65000

步长：变量的变化规则，如当步长为 1 时，每调用一次变量则加 1 或减 1

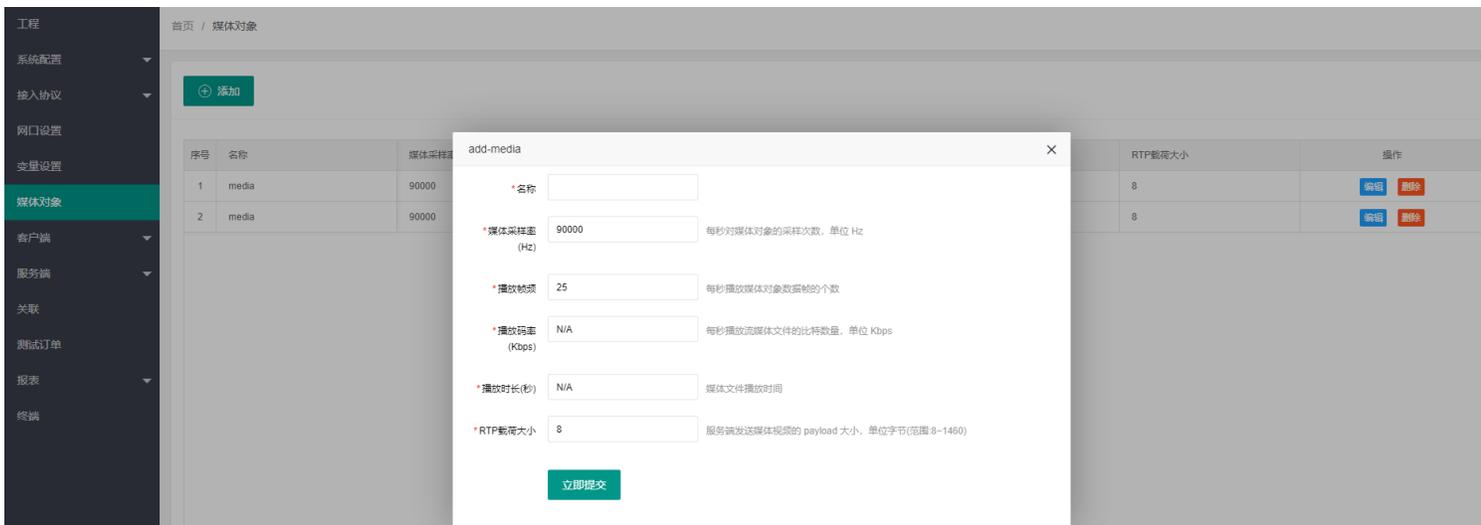
顺序：当前支持递增、递减与随机三种模式，其中当顺序为随机模式时，将不按设定步长变化（目前只支持递增模式）

3.6 媒体对象

媒体对象可以自定义一个虚拟的视频数据流。在 RTSP 协议测试中，服务端可以选择引用这里添加的媒体对象，测试时就可以按照定义的格式向终端发送 RTP 数据流。



点击 [+](#) 添加 按钮，填写视频流的各项参数



名称：自定义媒体流的名称

媒体采样率：视频媒体数据的采样率，表示每秒对媒体对象的采样次数，单位是 Hz

播放帧率：视频数据的帧速率，表示每秒播放媒体对象数据帧的个数

播放码率：视频播放的码率，表示每秒播放流媒体文件的比特数量

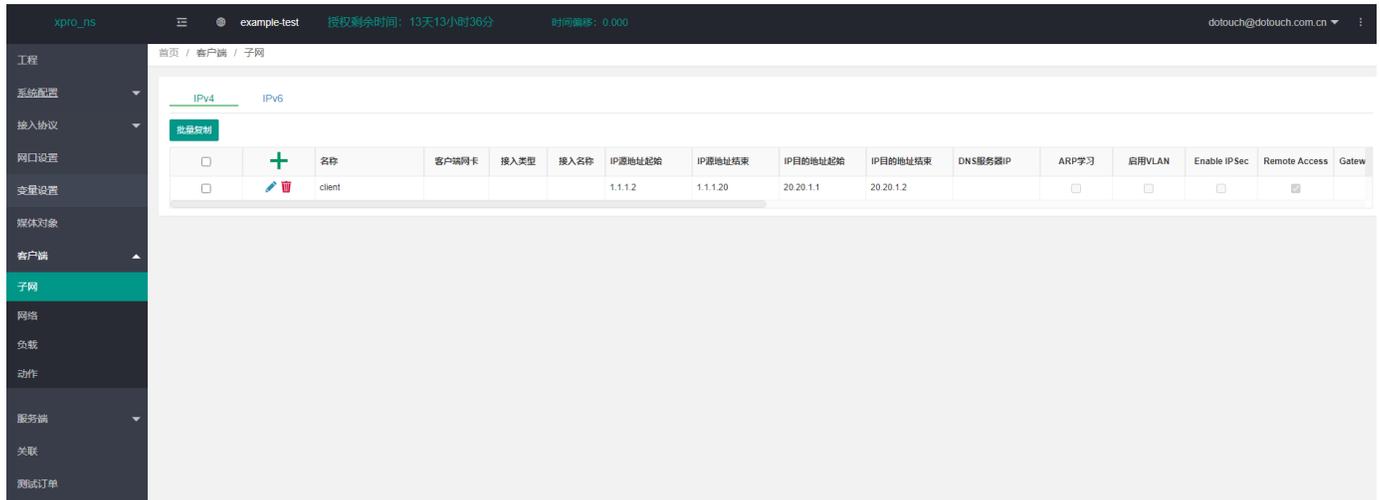
播放时长：表示媒体播放文件的长度，单位是秒

RTP 载荷大小：配置发送的 RTP 报文中所带载荷的大小

3.7 客户端

3.7.1 客户端子网配置

子网配置项用来配置 Client 端发起请求时的源 IP 地址范围，支持 IPv4 与 IPv6，选择 ipv4，添加 ipv4 地址，选择 ipv6，添加 ipv6 的地址。



名称：该 IP 子网的名称

接入类型：该 IP 子网的接入类型，例子中是仿真 http 协议，可不选择

接入名称：该 IP 子网的接入名称，例子中是仿真 http 协议，可不选择

客户端网卡：选择作为客户端的网卡

IP 源地址开始/IP 源地址结束：用来配置该仿真时客户端子网的起始 IP 与结束 IP。

IP 目的地址开始/IP 目的地址结束：用来配置该仿真时服务器子网的起始 IP 与结束 IP

DNS 服务器 IP：当需要解析域名信息时，需指定 DNS 解析服务器的 IP 地址。

ARP 学习：当被测设备工作在二层，如网桥模式、透明模式等，此时仪表客户端与服务端处于同一个网段，在该场景下需开启该功能，此时客户端会直接向服务端 IP 发起 arp 请求后将数据包直接发送给服务端，而不是将数据包交由下一跳网关转发，开启该功能后，设备工作在 L2 模式。



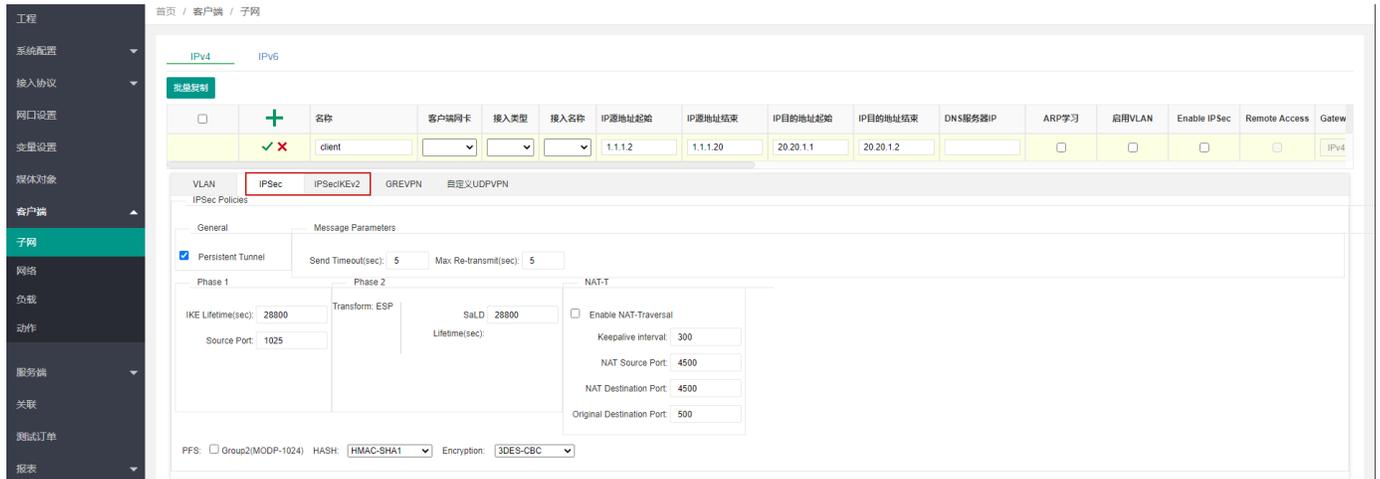
启用 VLAN：当该子网需要启用 VLAN 时需勾选该功能（并配置下方 VLAN 相关信息）

VLAN ID：该子网所在的 VLAN

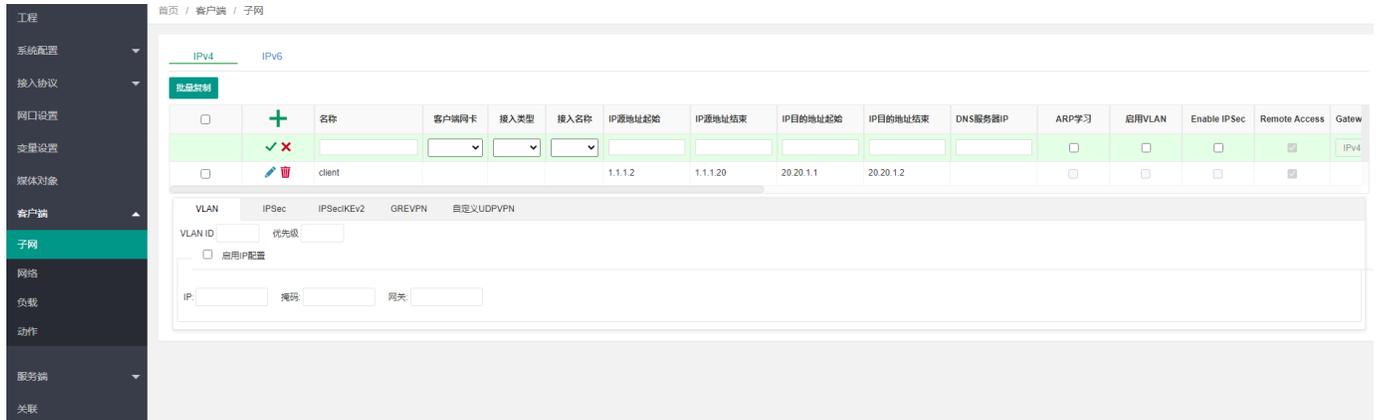
优先级：配置该 VLAN 的 Priority

启用 IP 配置：配置该 Client 子网所在 VLAN 的 VLAN 子网 IP 地址

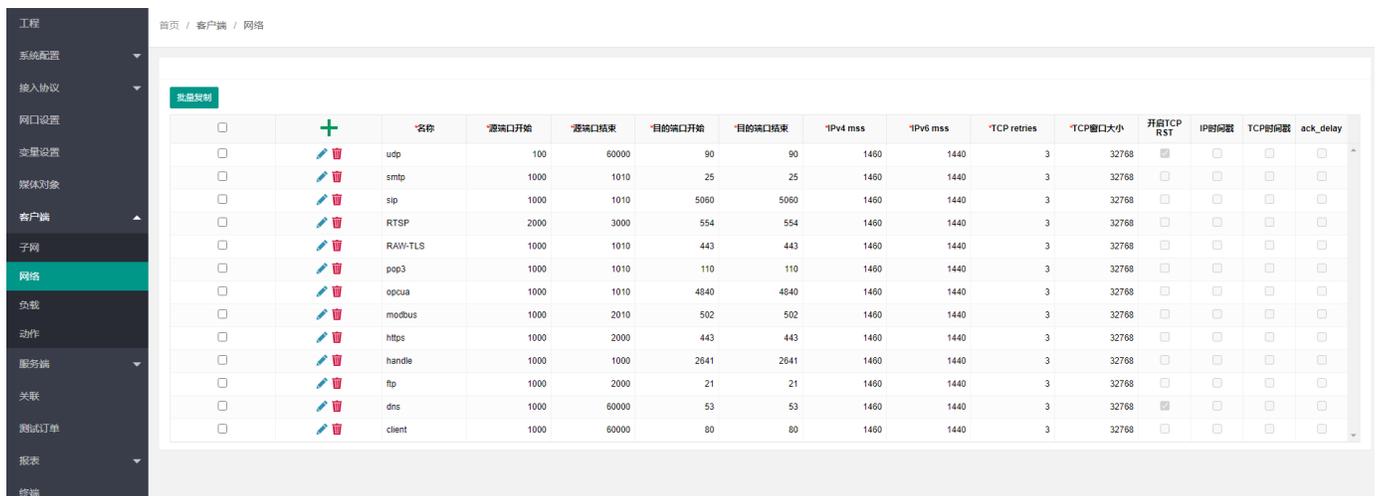
Enable IPsec: 当该子网需要启用 IPsec 是需勾选该功能 (勾选后需要在下方 IPsec 按照需求进行相应配置)



点击 按钮可配置子网, 可添加多个子网, 并可编辑和删除已有子网



3.7.2 客户端网络配置



名称: 该条网络配置的名称

源端口开始: 配置仿真时 Client 端发起请求的四层源端口最小值

源端口结束: 配置仿真时 Client 端发起请求的四层源端口最大值, 最大值为 65535

目的端口开始: 配置仿真时 Client 端发起请求的四层目的端口最小值

目的端口结束: 配置仿真时 Client 端发起请求的四层目的端口最大值, 最大值为 65535

IPv4 mss: IPv4 最大报文段长度

IPv6 mss: IPv6 最大报文段长度

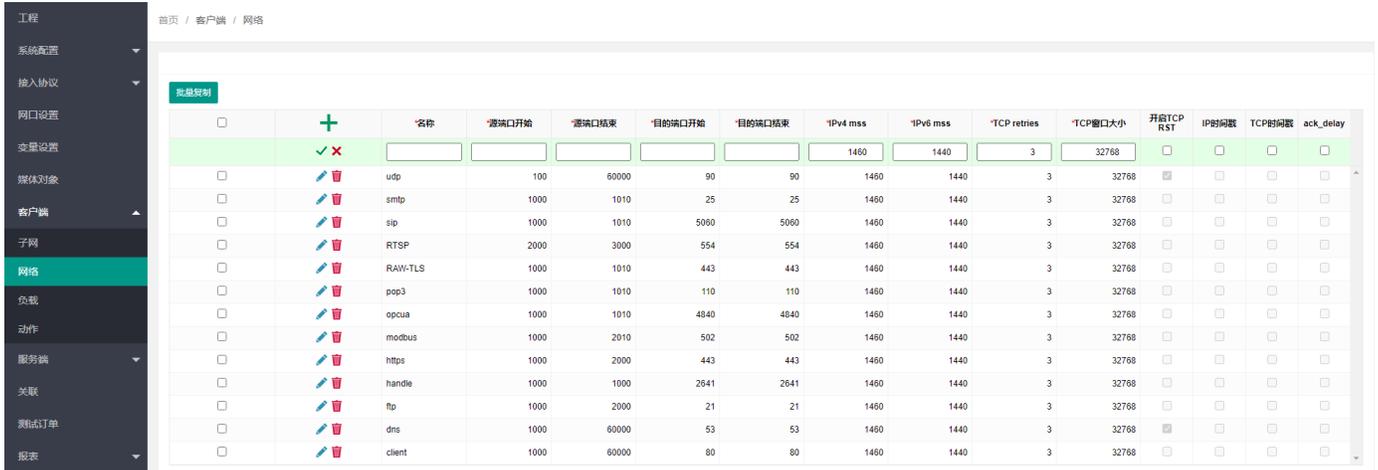
TCP retries: TCP 重传次数

TCP 窗口大小: 可以配置 TCP 默认窗口大小

开启 TCP RST: 用来指定当在测试任务时间到期后，对仍然存活的 TCP 连接采取 TCP RST 的方式关闭连接，当不勾选时默认以 Finish 方式关闭连接

IP 时间戳: 该功能是在 ip option 上打上时间戳来计算链路时延（双单臂需要客户端和服务端同时开启 ip 时间戳才会统计时延）

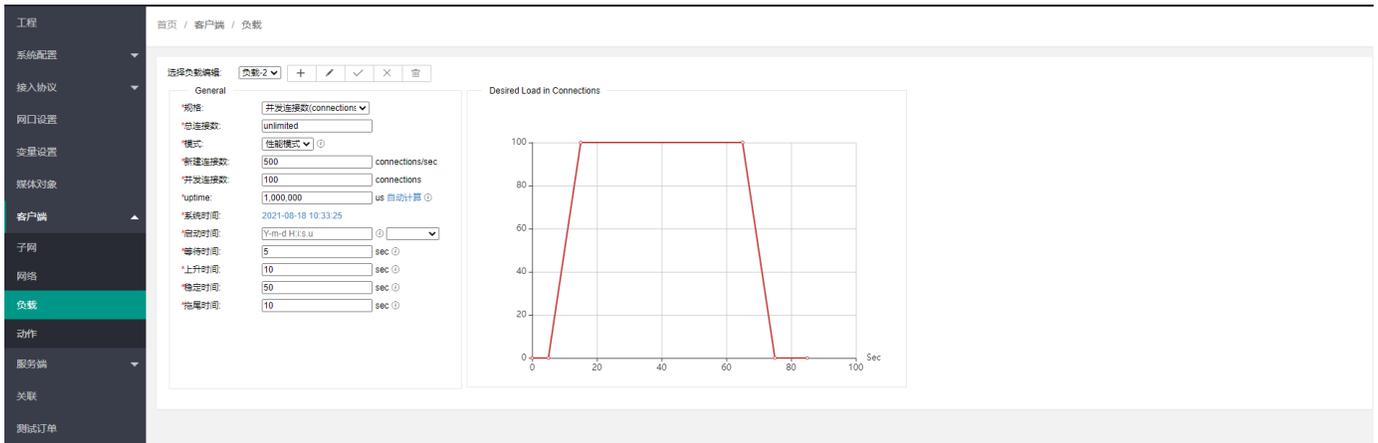
点击  按钮可添加多个网络配置，并可编辑和已有网络配置



名称	源端口开始	源端口结束	目的端口开始	目的端口结束	IPv4 mss	IPv6 mss	TCP retries	TCP窗口大小	开启TCP RST	IP时间戳	TCP时间戳	ack_delay
udp	100	60000	90	90	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
smtp	1000	1010	25	25	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sip	1000	1010	5060	5060	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RTSP	2000	3000	554	554	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RAW-TLS	1000	1010	443	443	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
pop3	1000	1010	110	110	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
opcu	1000	1010	4840	4840	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
modbus	1000	2010	502	502	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
https	1000	2000	443	443	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
handle	1000	1000	2641	2641	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ftp	1000	2000	21	21	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dns	1000	60000	53	53	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
client	1000	60000	80	80	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3.7.3客户端负载配置

负载配置用来配置仿真时的四层业务模型，有 2 种规格：并发连接数、新建连接数。

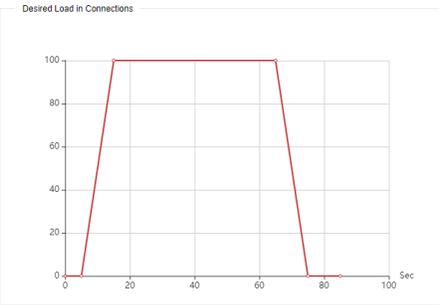


选择负载编辑 负载-2

General

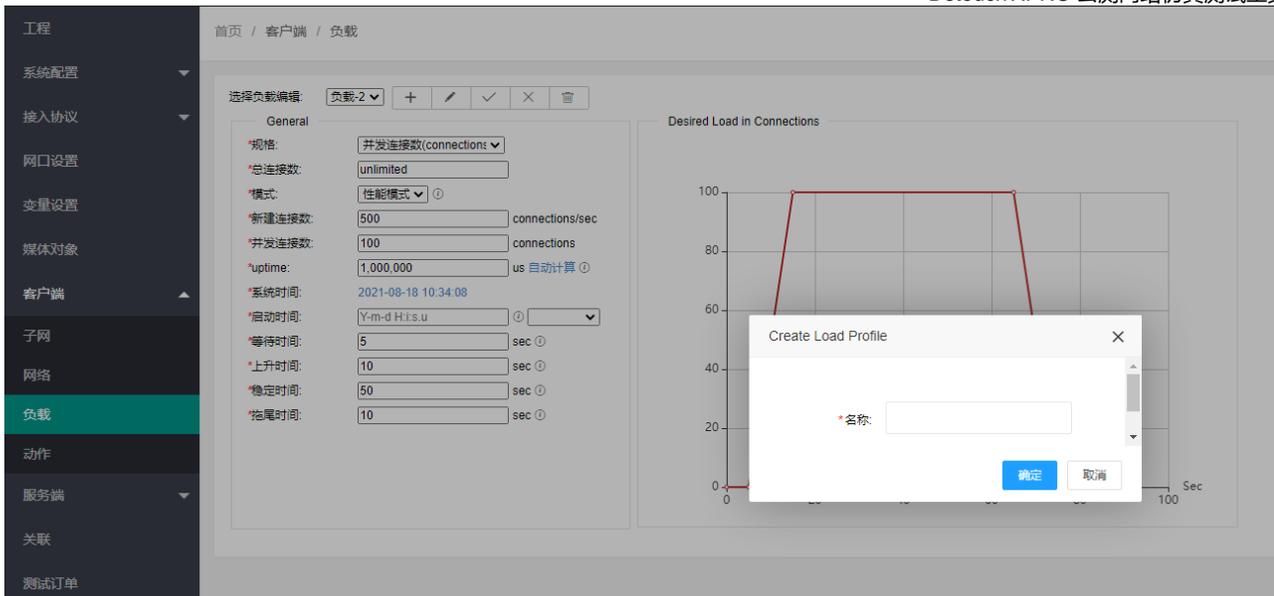
- 名称: 并发连接数(connections)
- 总连接数: unlimited
- 模式: 性能模式
- 新建连接数: 500 connections/sec
- 并发连接数: 100 connections
- uptime: 1,000,000 us 自动计算
- 系统时间: 2021-08-18 10:33:25
- 启动时间: Y-m-d H:i:s
- 等待时间: 5 sec
- 上升时间: 10 sec
- 稳定时间: 50 sec
- 结束时间: 10 sec

Desired Load in Connections



The graph shows the desired load in connections over a 100-second period. The load starts at 0, rises linearly to 100 connections at approximately 10 seconds, remains constant at 100 connections until about 65 seconds, and then falls linearly back to 0 connections by 80 seconds.

点击  按钮可添加多个业务负载模型，并可编辑和删除已有负载模型



名称：配置该负载项的名称

规格：该配置项配置新建连接数、并发连接数的优先级关系，如当选择新建连接数优先时，则在测试时优先满足设定的新建连接数指标。

总连接数：配置总连接数指标值

新建连接数：配置新建连接数指标值

并发数：配置并发数指标值

系统时间：显示当前系统时间

启动时间：配置订单开始运行时间(距离当前时间需要大于 4 分钟)。若运行订单时超过此时间，则此配置不生效。

等待时间：配置测试等待时间

上升时间：配置测试爬坡时间

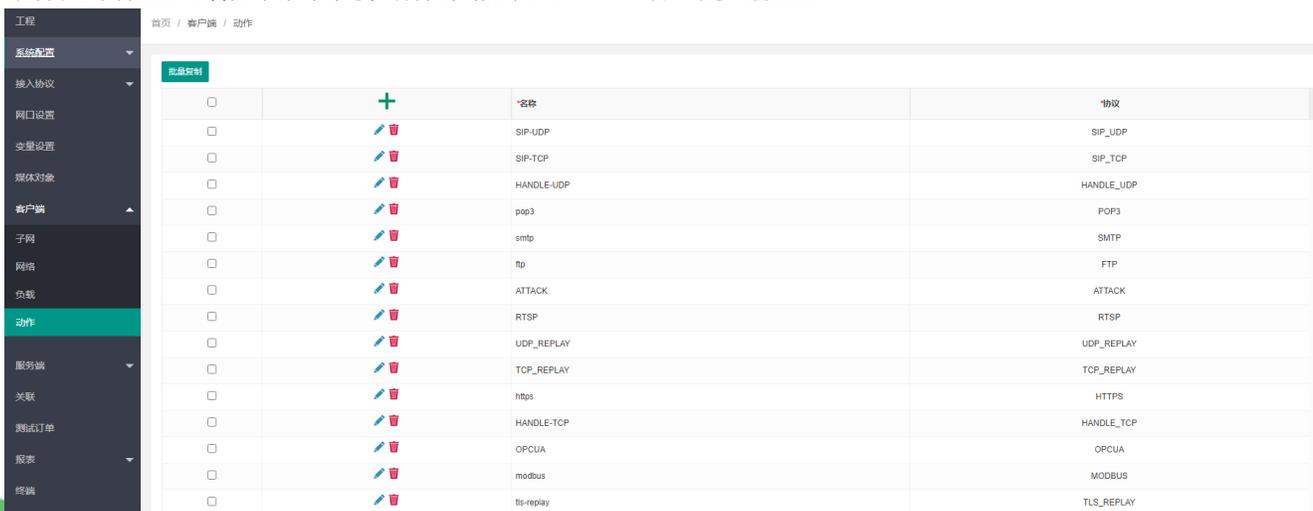
稳定时间：配置测试稳定时间

下降时间：配置测试下坡时间

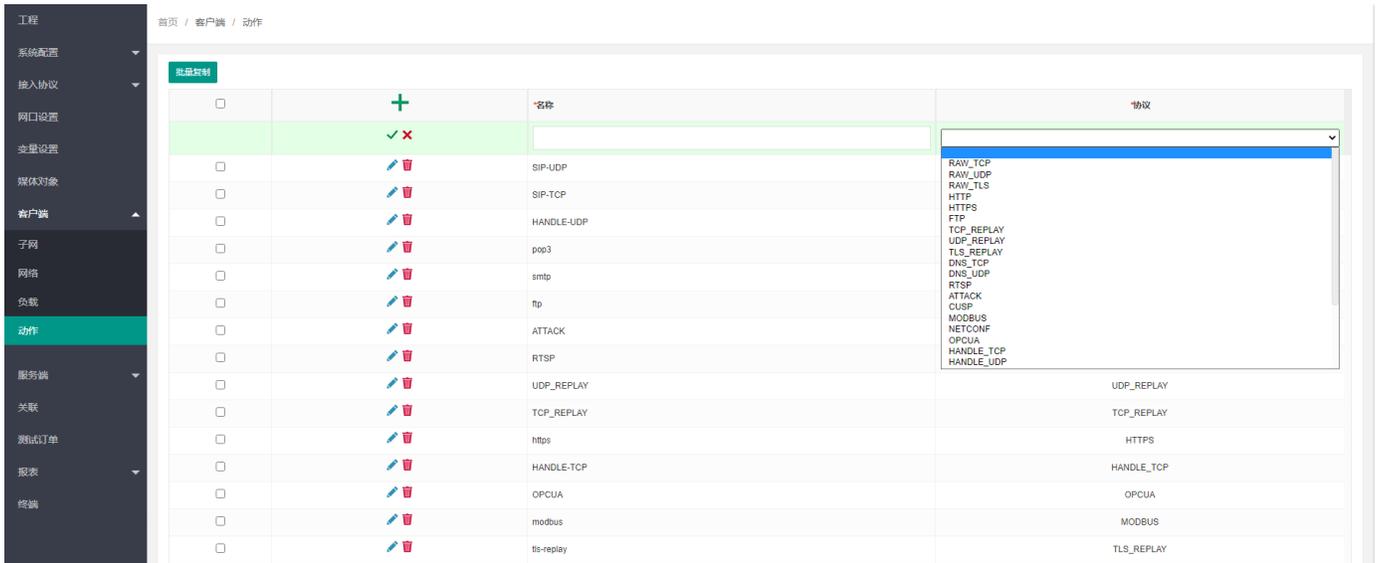
拖尾时间：配置测试拖尾时间

3.7.4 客户端动作配置

动作用来配置网络协议仿真时，所仿真协议的 Client 端一侧的配置。



点击  按钮，通过下拉菜单可以选择所需仿真的协议。可添加多个动作，并可编辑和删除已有动作。



名称	协议
SIP-UDP	RAW_TCP RAW_UDP RAW_TLS HTTP HTTPS FTP TCP_REPLAY UDP_REPLAY TLS_REPLAY DNS_TCP DNS_UDP RTSP ATTACK CUSP MODBUS NETCONF OPCUA HANDLE_TCP HANDLE_UDP
SIP-TCP	
HANDLE-UDP	
pop3	
smtp	
ftp	
ATTACK	
RTSP	
UDP_REPLAY	UDP_REPLAY
TCP_REPLAY	TCP_REPLAY
https	HTTPS
HANDLE-TCP	HANDLE_TCP
OPCUA	OPCUA
modbus	MODBUS
tls-replay	TLS_REPLAY

选择具体协议后，可编辑协议相关的参数，本版本支持如下类型的协议仿真及带 4 层状态的 7 层应用回放功能：

RAW_TCP：一种简单的基于 TCP 承载的非标准应用，可自定义 client/server 端发送内容的大小

RAW_UDP：一种简单的基于 UDP 承载的非标准应用，可自定义 client/server 端发送内容的大小

RAW_TLS：一种简单的基于 TLS 承载的非标准应用，可自定义 client/server 端发送内容的大小

HTTP：仿真标准的 HTTP 业务，支持 get/head/post method，支持自定义 header 字段及内容字段，

HTTPS：仿真 HTTPS 业务，系统自动完成 SSL 协商、KEY 交换及加密通道的建立

FTP：模拟标准的 FTP 协议，支持同时模拟 Client 端与 Server 端，支持主/被动模式

TCP REPLAY：回放基于 TCP 承载的标准应用（如 HTTP）及非标准应用（如微信/QQ）

UDP REPLAY：回放基于 UDP 承载的标准应用及非标准应用

TLS REPLAY：回放基于 TLS 承载的标准应用及非标准应用

DNS TCP：仿真基于 TCP 承载的域名解析服务

DNS UDP：仿真基于 UDP 承载的域名解析服务

RTSP：仿真视频质量测试

ATTACK：仿真基于 CVE 漏洞的网络攻击

CUSP：仿真 CUSP 协议

MODBUS：仿真 MODBUS 协议

NETCONF：仿真 netconf 协议

OPCUA：仿真 opcua 通信接口协议

HANDLE_TCP：仿真基于 TCP 承载 HANDLE 工控协议

HANDLE_UDP：仿真基于 UDP 承载 HANDLE 工控协议

L2TP：仿真隧道协议

SMTP：仿真电子邮件传输协议

PO3P：仿真邮局 POP3 协议

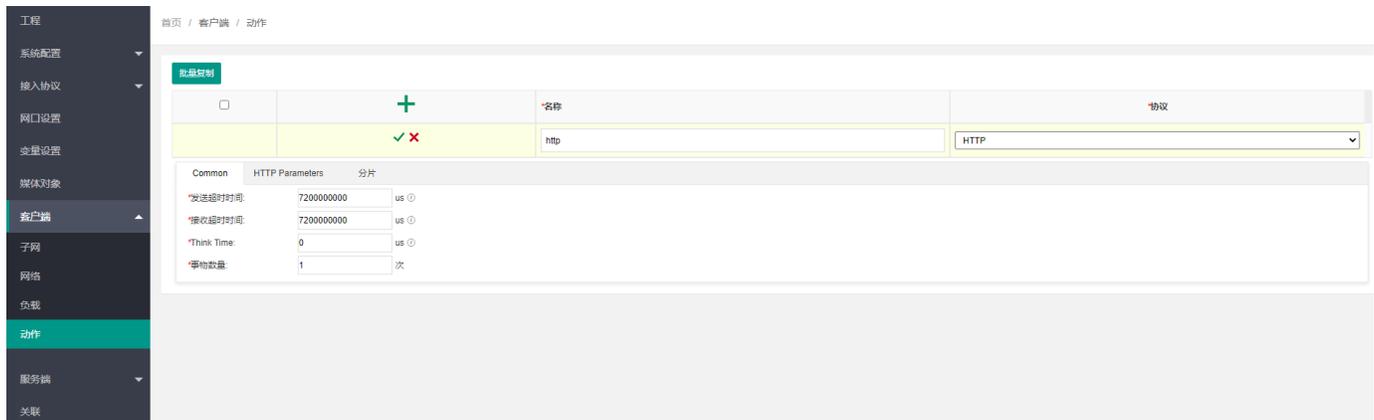
SIP_TCP：仿真基于 TCP 承载 SIP 协议

SIP_UDP：仿真基于 UDP 承载 SIP 协议

MQTT_TCP：仿真基于 TCP 承载 MQTT 协议

COAP_UDP：仿真基于 UDP 承载 COAP 协议

a) 通用配置



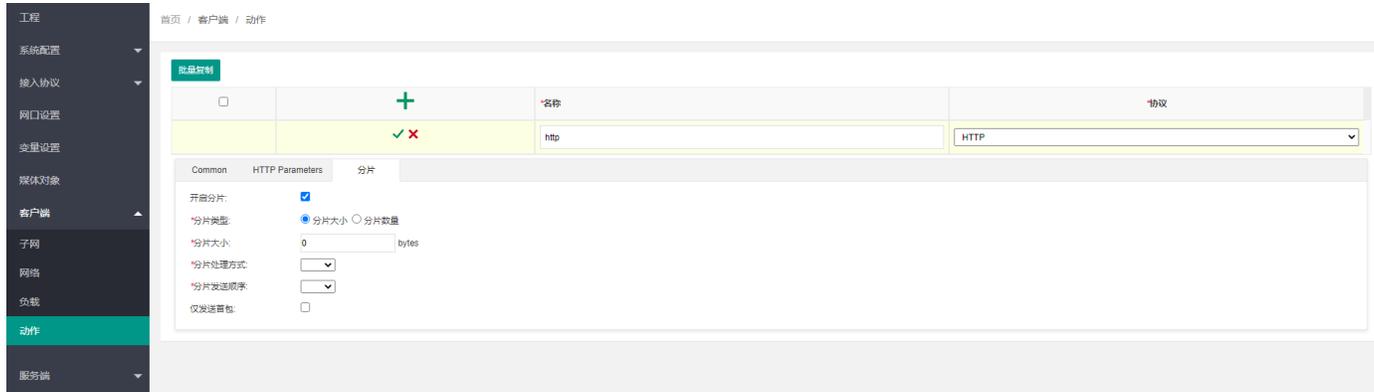
名称：配置该动作的名称

发送超时时间：单位 us，如在该时间范围内未将需要发送的内容发送出去，则认为发送失败

接收超时时间：单位 us，这个接收超时时间是指客户端如在该时间范围内未收到服务端返回的全部内容，则认为接收失败

Think Time：当客户端请求事务数量超过 1 个时，业务延迟时间表示客户端发起的两个事务之间的时间间隔，如 HTTP 事务数量为 2，则表示客户端会发送两次 HTTP 请求，两次 HTTP 请求之间的时间间隔为此处设置的业务延迟时间。

事务数量：配置客户端发起的事务数量，当事务数量为 2 时，表示在一个 TCP 连接中，客户端会发起 2 次相同的业务请求，如仿真 HTTP，Method 为 GET，此时表示客户端会在一个 TCP 连接中发起 2 次 HTTP GET 请求。



开启分片：当打开该功能开关时，客户端将依据设置的规则对 IP 报文进行分片

分片类型：当前支持分片大小与分片数量两种分片方式，当分片类型为“分片大小”时，客户端将按照设置的值对 IP 报文进行分片操作，如设置的分片大小为 100 字节，实际报文大小为 1200 字节，则该 IP 报文将会被分为 12 个 IP 分片。当分片类型为“分片数量”时，客户端将按照设置的数量对原始 IP 报文进行分片，如设置的“分片数量”为 5，实际 IP 报文大小为 1000 字节，则该 IP 报文会被分为 5 个等长的 IP 分片。

分片大小：当“分片类型”设置为分片大小时。该处配置有效，用来配置每个 IP 分片的长度

分片处理方式：当前仅支持自动分片，该处配置默认即可

分片发送顺序：当前支持正序发送分片与倒序发送分片两种方式，正序发送是指按照分片包的顺序先后发送，即按照第一个分片、第二个分片、第 N 个分片的顺序发送，倒序发送则是先发送第 N 个分片，再发送第 N-1 个分片，直至最后发送第一个分片。

开启 SSL/TLS: 开启 SSL/TLS 加密开关，支持 SSL/TLS 加密的协议才会展示（默认勾选）

类型: 选择加密类型

版本: 选择加密协议版本

加密套件 1~5: 选择加密套件，至少选择一个

握手超时时间: 单位 ms，如在该时间范围内握手完成，则认为握手失败

客户端验证: 客户端身份验证开关

客户端证书: 选择客户端证书

客户端私钥: 选择客户端私钥

服务端 Ca 证书: 选择服务端 CA 证书

服务端证书验证模式: 目前支持三种模式，not_verify、allow_untrust、allow_trust 等

b) RAW TCP/UDP/TLS 配置方法

是否测量时延: 勾选表示进行时延测量功能

每秒采集包数: 采样包数时延，会按照配置的数值进行每秒抽样包数进行时延计算，并在结果中进行统计

请求大小: 设置客户端 RAW TCP/UDP/TLS 的请求报文大小（对于 TCP/UDP 而言为 TCP/UDP 的 payload 部分，对于 TLS 而言为 TLS 所承载的内容大小）。

响应大小: 用来客户端对比校验服务端响应客户端请求的内容长度与应该接收的内容长度是否一致，客户端会根据此处配置的大小来校验服务端的响应是否正确。

客户端与服务端仅对双方发送内容的长度进行校验，不对内容是否一致进行校验。



客户端与服务端的请求大小与响应大小必须一致，即客户端的请求大小与服务端的请求大小一致，客户端的响应大小与服务端的响应大小一致。

c) HTTP/HTTPS 配置方法

HTTP/HTTPS 协议仿真时主要区别为当仿真 HTTPS 时，系统会自动完成 SSL 的协商及加密通道的建立过程，具体配置方法完全一致。

The screenshot shows the 'HTTP Parameters' configuration window. It has four tabs: 'Common', 'HTTP Parameters', '分片', and 'TLS'. The 'HTTP Parameters' tab is selected. Under the 'General' section, there are several fields: '关联服务器' with a checkbox, '*Host' with the value 'www.test.com', '*URI' with the value '/index.html', '*Method' with a dropdown menu set to 'GET', and '*响应码' with the value '200'. Below the 'General' section, there are two large text areas labeled 'header字段' and '提交内容'.

关联服务器：绑定服务端 IP 和域名，确保每次访问的服务端 IP 和域名是对应的。

Method：设置 HTTP 的方法类型，当前支持 GET/HEAD/POST

Host：设置 HTTP host 头，如 a.b.com

URI：设置统一资源标识符,即请求的资源路径

变量设置：在构造 HOST 与 URI 时，为了避免仿真的海量 HTTP 业务请求的 host 与 uri 出现一样的情况，可在 HOST 与 URI 中引入变量，仪表将按照设定的变量与步长变化规则对 HOST 与 URI 自动变化，变量的设置在仪表的“变量设置”菜单栏中配置，配置方法见本配置手册第 3.5 章节

提交内容大小：当 method 为 POST 时，该配置项有效，用来当未配置“**提交内容**”配置项时，POST 动作所需提交内容的大小，系统会依据该大小，自动构造内容

Header 字段：用来定义 HTTP 的头部信息，可按照头部标准字段构造头部，或完全自定义头部字段

提交内容：当 Method 为 POST 时该配置项有效，用来配置 POST 动作向服务端提交的内容，当配置该项时，method 必须为 post，且当该项配置时，“**提交内容大小**”配置项不生效

自定义校验 Header：用来自定义客户端自校验 header，服务端会比对客户端请求的 header 校验值与服务端所配置的 header 校验值，如两者不一致，则认为请求非法。

 同一个 HOST 或 URI 中可同时引入多个变量。

d) FTP 配置方法

ftp 协议客户端配置框如下

Common	FTP Parameters	分片	TLS
*Method:	ftp_method_get ▼		
*模式:	ftp_mode_port ▼		
用户名:	anonymous		
密码:	123456		
*URI:	/test.html		
*数据传输端口范围:	40001	-	65000
*上传下载类型:	文件大小 ▼		
文件大小:	1000		bytes
突发大小:	15000		bytes
突发间隔:	2		ms

Method: 设置客户端 FTP 行为, 当前版本支持 GET 与 PUT

模式: 设置客户端 FTP 的工作模式, 当前支持主动模式(port)与被动模式(pasv)

ftp_mode_port: v4 主动模式

ftp_mode_pasv: v4 被动模式

ftp_mode_eprt: v6 主动模式

ftp_mode_epsv: v6 被动模式

ftp_mode_lprt: 服务器指定要连接的长地址和端口

ftp_mode_lpsv: 进入长被动模式

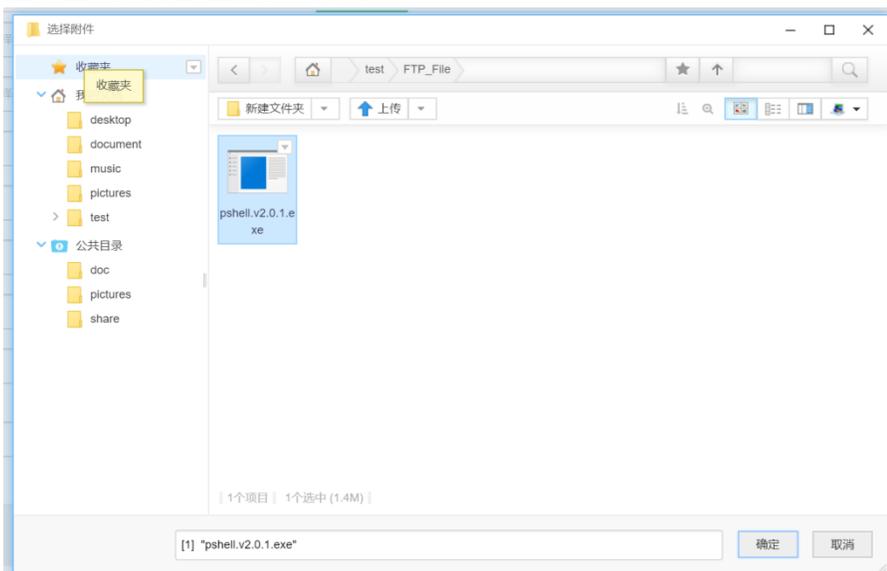
用户名: 设置客户端登陆 FTP 服务器的账号, 账号需要和服务端配置保持一致

密码: 设置客户端登陆 FTP 服务器的密码, 密码需要和服务端保持一致

URI: 在客户端行为为上传时, 此 URI 可任意填写, 服务端并无实际的路径, 当客户端行为为下载时, 此 URI 必须与服务端配置的目标文件 URI 一致 (目前只支持一级目录)

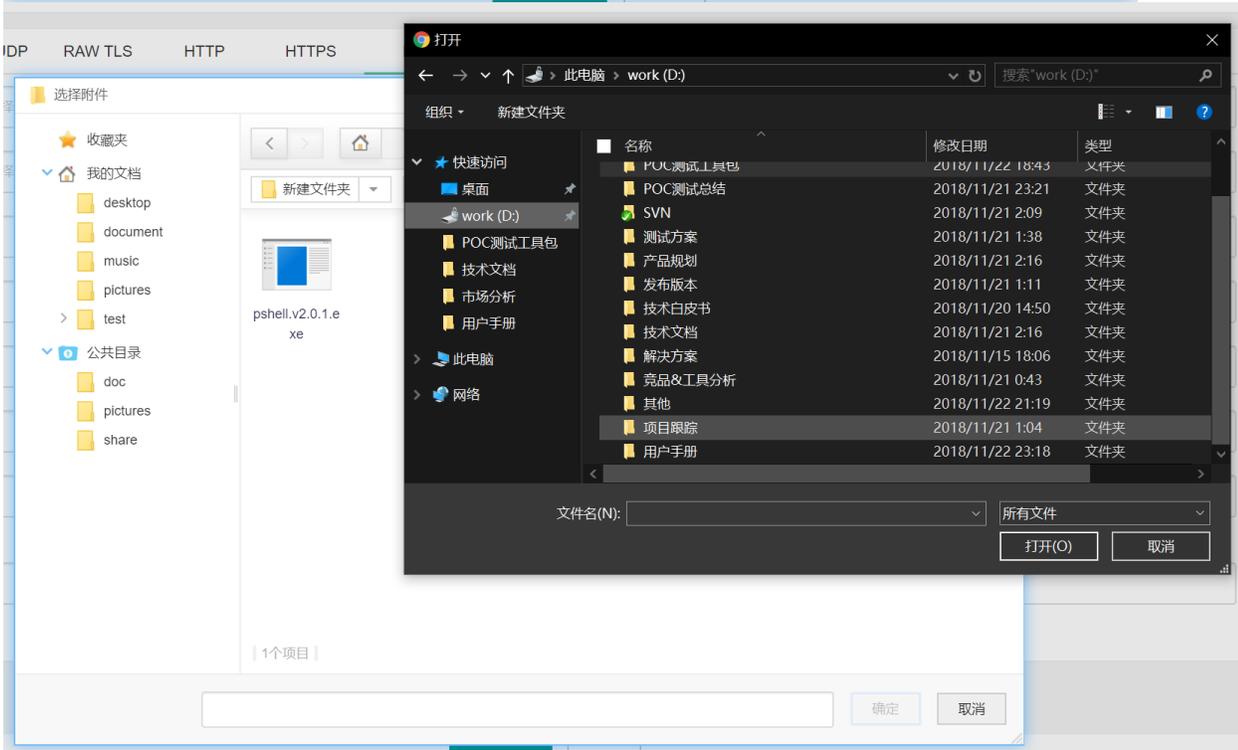
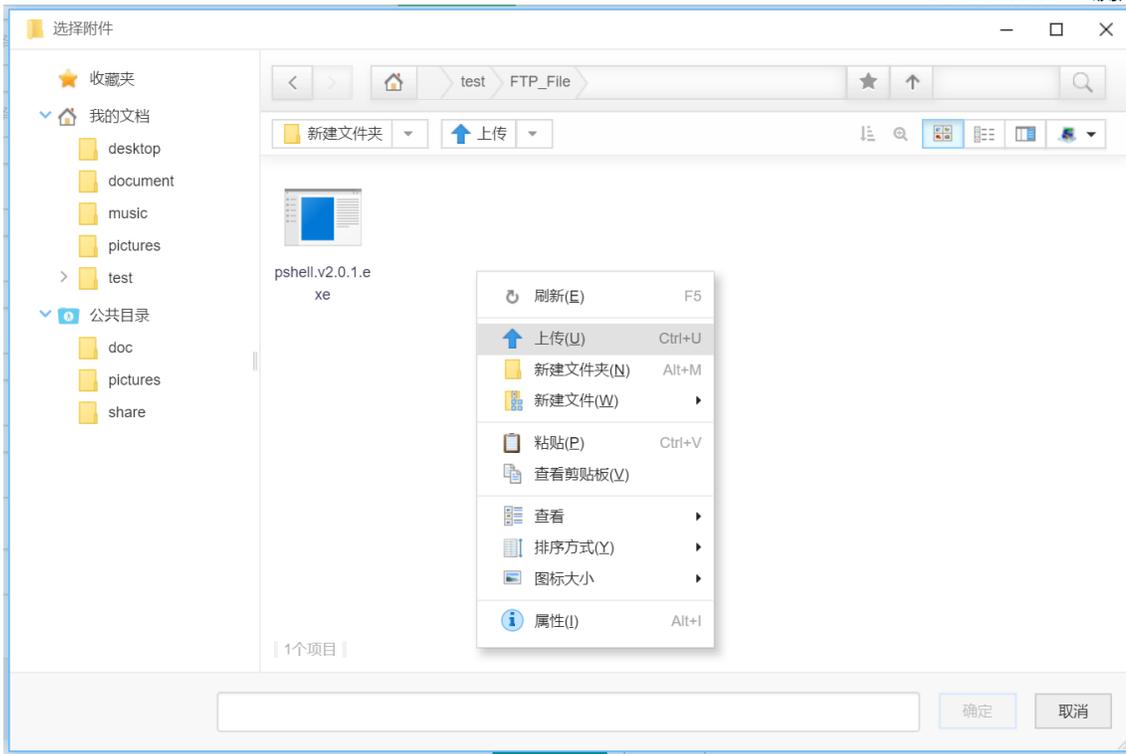
数据传输端口范围: 用来配置 FTP 数据连接时所使用的端口的范围

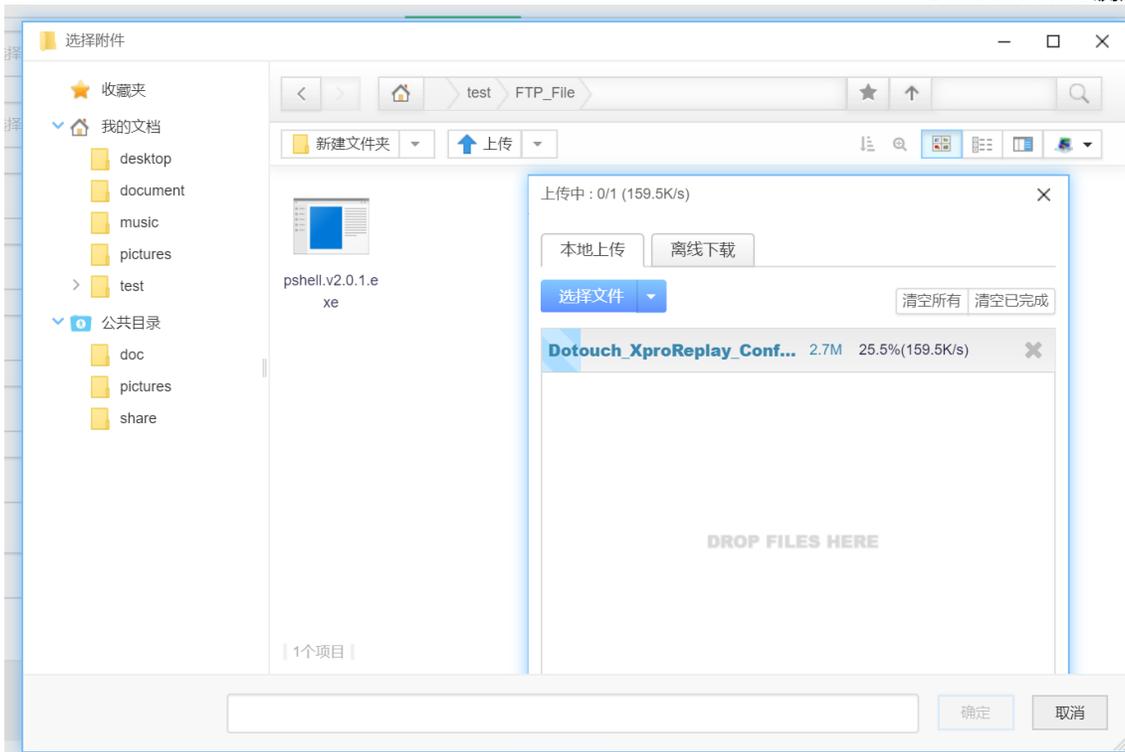
上传下载类型: 支持文件大小和文件路径, 选择为文件大小时, 直接输入大小数值即可; 选择为文件路径时, 可直接选择资源管理器中任意文件



用户可自行向文件库中上传文件, 供配置时调用。

STEP: 右键单击, 选择“上传”, 可从本地向文件库中上传指定的文件





e) TCP/UDP/TLS REPLAY 配置方法

Common	TCP_REPLAY Parameters	分片
*回放文件:	<input type="text" value="选择资源管理器文件"/>	
*回放样包:	<input type="text"/> 选择文件	
开启HOST替换:	<input type="checkbox"/>	
HOST替换:	<input type="text"/>	

TCP/UDP/TLS 回放功能分别用来回放基于 TCP/UDP/TLS 的标准应用或非标准应用，仿真模块会自动构建 4 层的状态信息，实现带 4 层状态的回放，**当前支持单个数据包中仅有 1 条流的回放，不支持单个数据包中含有多条流。**

回放文件：目前支持选择 资源管理文件(carray 文件) 和 L7 回放样包(pcap/cap 文件)。

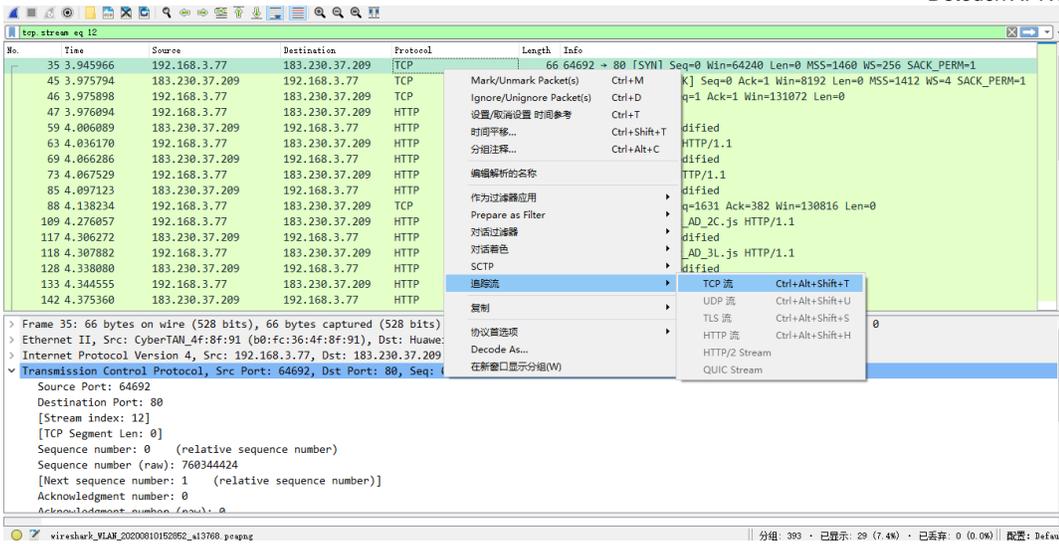
回放样包：当回放文件是选择资源管理器文件时，回放时要求数据包格式为 C Arrays，因此对于常规的 PCAP/CAP 包，因此需借助 wireshark 将其转换成 C Arrays 格式，具体方法如下：

开启 HOST 替换：是否替换回放文件中的 host

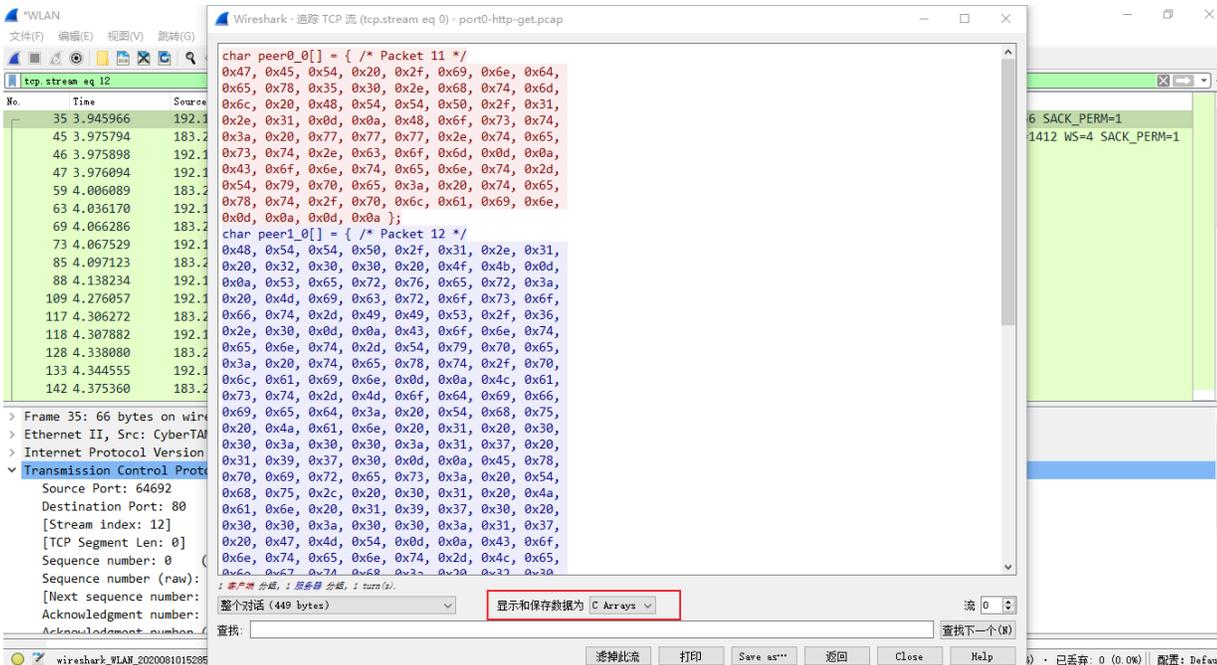
HOST 替换：要替换的 HOST

PCAP/CAP 转 C Arrays 格式方法

STEP 1:用 wireshark 打开数据包，右键点击需要所需回放应用所在流的任意一个数据包，选择“追踪”



STEP 2:选择“显示和保存数据为“C Arrays”，保存即可。



回放时选择保存后的数据包文件即可。



当回放某个指定的应用时，此时客户端与服务端需配置同一个数据包文件。

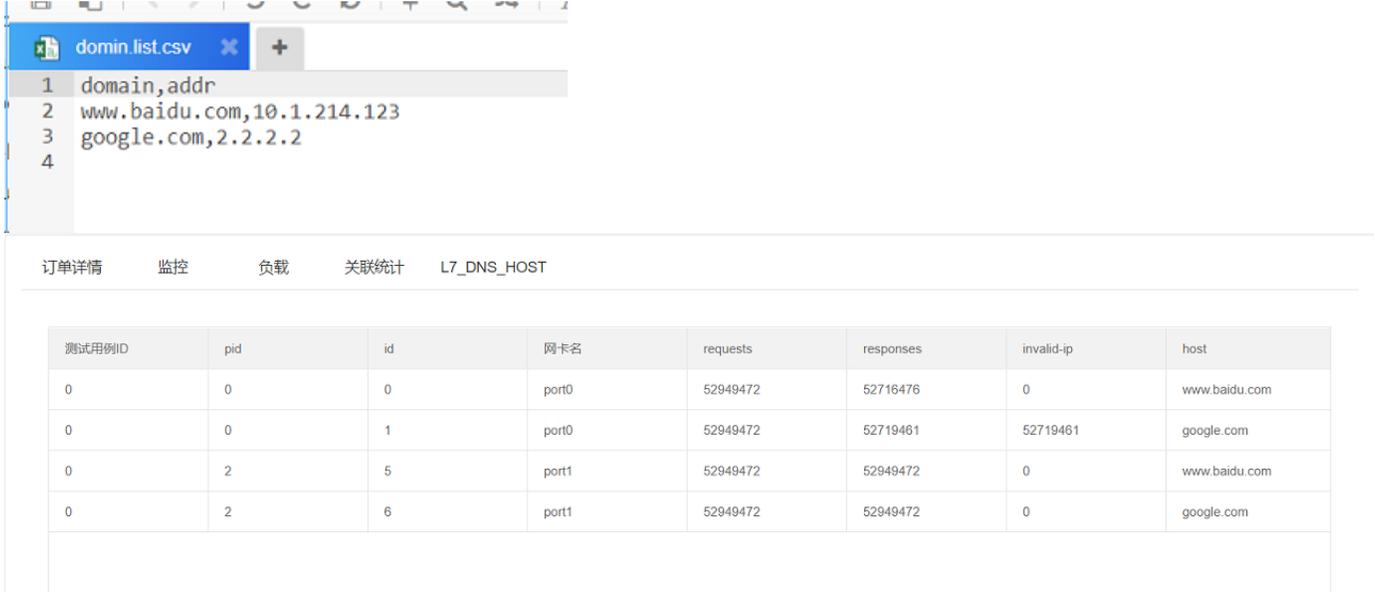
f) DNS_TCP/DNS_UDP 配置方法

DNS_TCP/DNS_UDP 用来模拟客户端 DNS 请求行为，两者的区别为 4 层承载协议是 TCP 或 UDP。



Domain: 用来配置 DNS 解析请求的目标域名，目前 domain 类型支持单个域名、批量生成和上传文件三种。批量生成引用的时变量设置中配置的规则，上传文件时选择资源管理器中的 domain 文件（格式为 csv，文件列头为

domain,addr), 客户端会对请求的域名对应 IP 进行校验, 如有不一致, 则会统计在 invalid-ip 中, 如下图所示



The screenshot shows a CSV file with the following content:

```

1 domain,addr
2 www.baidu.com,10.1.214.123
3 google.com,2.2.2.2
4

```

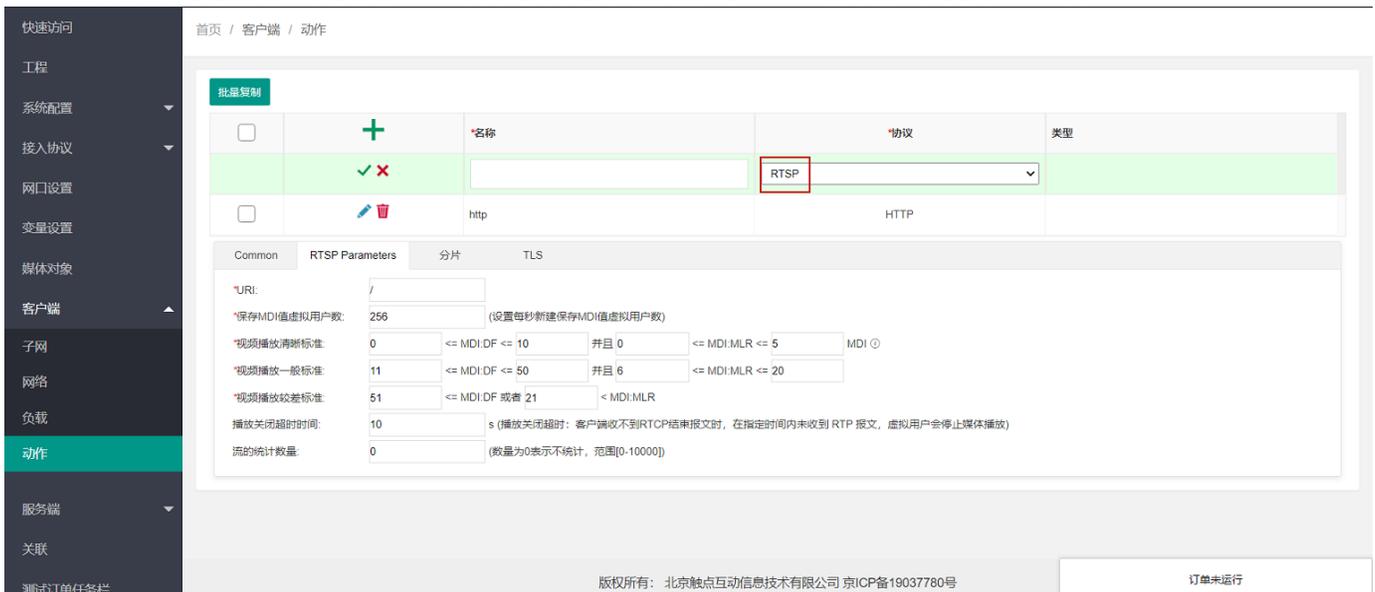
Below the CSV is a table with the following columns: 测试用例ID, pid, id, 网卡名, requests, responses, invalid-ip, host.

测试用例ID	pid	id	网卡名	requests	responses	invalid-ip	host
0	0	0	port0	52949472	52716476	0	www.baidu.com
0	0	1	port0	52949472	52719461	52719461	google.com
0	2	5	port1	52949472	52949472	0	www.baidu.com
0	2	6	port1	52949472	52949472	0	google.com

DNS 类型: 有 A 或者 AAAA 两种, A 表示 IPv4 模式的 DNS, AAAA 表示 IPv6 模式的 DNS。

g) RTSP 配置方法

RTSP 协议用来模拟客户端使用 RTSP 协议播放视频的行为, RTSP 协议默认使用 554 端口



The screenshot shows the RTSP configuration interface. The main configuration area includes:

- URI:** /
- 保存MDI值虚拟用户数:** 256 (设置每秒新建保存MDI值虚拟用户数)
- 视频播放清晰标准:** 0 <= MDI.DF <= 10 并且 0 <= MDI.MLR <= 5 MDI
- 视频播放一般标准:** 11 <= MDI.DF <= 50 并且 6 <= MDI.MLR <= 20
- 视频播放较差标准:** 51 <= MDI.DF 或者 21 < MDI.MLR
- 播放关闭超时时间:** 10 s (播放关闭超时: 客户端收不到RTSP结束报文时, 在规定时间内未收到 RTP 报文, 虚拟用户会停止媒体播放)
- 流的统计数量:** 0 (数量为0表示不统计, 范围[0-10000])

The interface also shows a table with columns for Name, Protocol, and Type, with RTSP selected in the Protocol dropdown.

URI: 设置统一资源标识符,即请求的资源路径

保存 MDI 值虚拟用户数: 报表中输出 MDI 值的虚拟用户数量, 这个值必须小于虚拟用户数的总量。

MDI 为 媒体流丢失率和延迟的组合评价指标

MDI(Media Delivery Index)媒体传输质量指标是由思科公司和 IneoQuest 共同提出的, 对视频流在 IP 网络传输质量进行评估的测量指标。作为 IP 视频流传输质量测试的行业标准, MDI 测量指标广泛地应用于 IPTV 和 IP 有线数字电视网络质量评估和监测。

对 IP 视频流的传输质量用 RFC 4445 MDI 标识为: DF: MLR。

MDI 包括了两个参数:

- Delay Factor (延迟因素, 简称 DF): 该数值表明被测试视频流的延迟和抖动状况。DF 的单位是毫秒

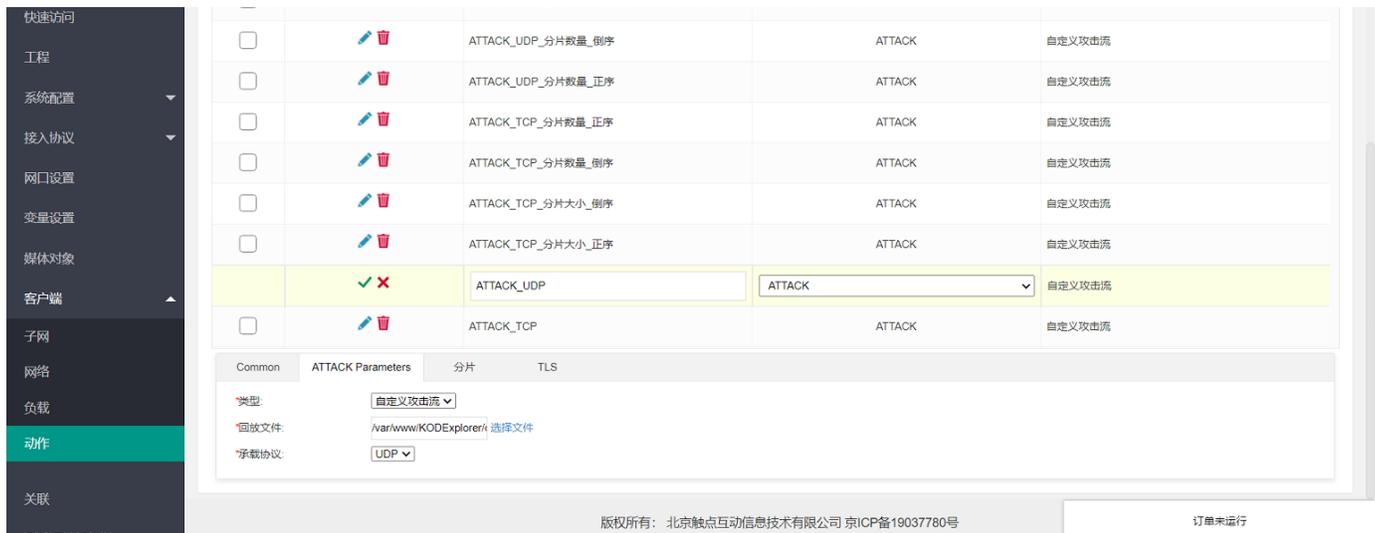
(ms)。DF 将视频流抖动的变化换算为对视频传输和解码设备缓冲的需求。被测视频流抖动越大，DF 值越大。当网络设备和解码器的缓冲区容纳的视频内容时间不小于被测视频流 DF 读数时，将不会出现视频播放质量的下降。因为网络节点需要分配不小于 DF 值的缓冲用于平滑视频流抖动，所以 DF 的最大值为视频内容通过该网络节点的最小延迟。

- Media Loss Rate (媒体丢包速率, 简称 MLR) : MLR 的单位是每秒的媒体封包丢失数量。该数值表明被测试视频流的传输丢包速率。由于视频信息的封包丢失将直接影响视频播放质量, 理想的 IP 视频流传输要求 MLR 数值为零。因为具体的视频播放设备对丢包可以通过视频解码中进行补偿或者丢包重传, 在实际测试中 MLR 的阈值可以相应调整。

流的统计数量: RTP 报表中输出统计数据, 配置统计流的数量就是输出统计流的数量。

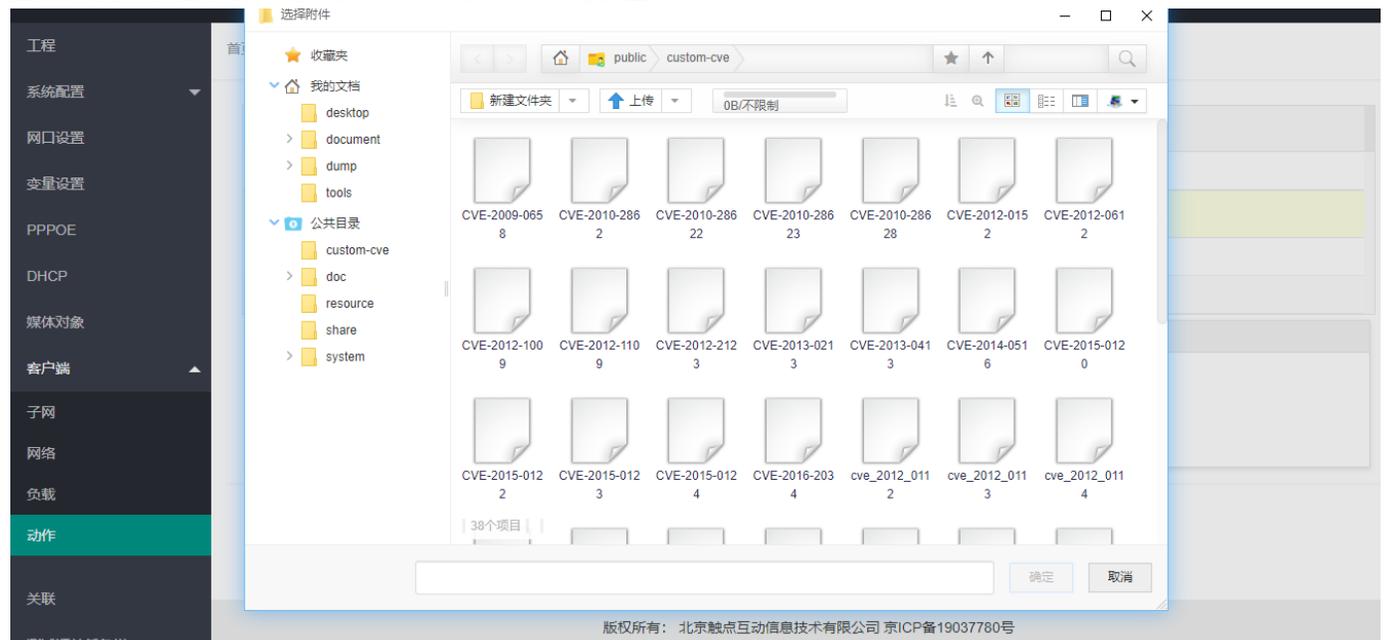
h) attack 配置方法

attack 模拟网络攻击行为, 客户端模拟发送攻击报文, 配置页面如下



类型: 目前仅支持自定义攻击流

回放文件: 回放文件选择系统自带的 CVE 漏洞攻击文件



承载协议: 根据需要, 可选 tcp 或者 udp 协议

i) CUSP 配置方法

模拟 CUSP 协议的 up 进行测试

名称	协议	类型
	CUSP	
L3-replay	L3_REPLAY	
attack1	ATTACK	自定义攻击流
udp	RAW_UDP	
tcp	RAW_TCP	

Common CUSP Parameters 分片 TLS

*CUSP心跳间隔时间: 30 s

*槽位数:

*子槽位数:

*单个槽位虚拟端口数量:

*虚拟口类型:

*VXLAN ID范围: - (仅支持GPE格式)

*VXLAN目的IP:

*拨号类型:

版权所有：北京触点互动信息技术有限公司 京ICP备19037780号

CUSP 心跳间隔时间：协议心跳间隔的时间

槽位数：仿真 UP 的槽位数量

子槽位数：仿真 UP 的子槽位数量

每个槽位虚拟端口数：仿真 UP 的单槽位虚拟口数量设置

虚拟口类型：仿真接口的类型，目前已支持 GE、10GE、40GE、100GE、Eth-Trunk、Tunnel、VE 这 7 种类型

Common CUSP Parameters 分片 TLS

*CUSP心跳间隔时间: 30 s

*槽位数:

*子槽位数:

*单个槽位虚拟端口数量:

*虚拟口类型:

*VXLAN ID范围: - (仅支持GPE格式)

*VXLAN目的IP:

*拨号类型:

VXLAN ID 范围：测试数据 vxlan 的范围

VXLAN 目的 IP：指定 vxlan 的目的 ip 地址

拨号类型：拨号类型可以选择不拨号，也可以选择拨号方式。目前已经支持 PPPoEv4、PPPoE v6、PPPoEv4&v6 兼容模式以及 DHCPv4 模式

Common	CUSP Parameters	分片	TLS
*CUSP心跳间隔时间:	30	s	
*槽位数量:	32		
*子槽位数量:	2		
*单个槽位虚拟端口数量:	4		
*虚拟口类型:	10GE		
*VXLAN ID范围:	200 - 65500	(仅支持GPE格式)	
*VXLAN目的IP:	192.168.2.10		
*拨号类型:	DHCPv4		
*虚拟口拨号次数:	不拨号 PPPOEv4 PPPOEv6 PPPOEv4&v6 DHCPv4		
*虚拟口拨号速率:			
*虚拟口拨号在线时长:	600	s	
*每个虚拟口拨号用户数:	400		
DHCP用户参数			
*重试次数:	3		
*vlan1:			

j) attack play 配置方法 (该功能已经迁移到 L3_REPLAY 子系统中)

attackplay 使用外部攻击库导入攻击文件模拟网络攻击行为

工程

系统配置

网口设置

变量设置

PPPOE

DHCP

媒体对象

客户端

子网

网络

负载

动作

关联

	*名称	*协议	类型
+			
🗑️	L3-replay	L3_REPLAY	
✔️ ✖️	attack1	ATTACK_PLAY	自定义攻击流
🗑️	udp	RAW_UDP	
🗑️	tcp	RAW_TCP	

ATTACK_PLAY Parameters

*启用ip轮换:

*类型: 播放时长

*播放时长(s):

*播放速率(倍数): 10000

播放间隔(ms):

一级目录: 威胁对抗能力验证

二级目录: CVE漏洞利用

*攻击文件列表 (已选文件可拖拽调整文件顺序) 清空文件列表 选择文件

配置页包含如下参数:

启用 IP 轮换: 每一次攻击文件发送时使用的 ip 地址在子网配置的网段中轮换

类型: 播放类型, 包括按时间和按次数播放两种, 按时间播放时设置时间后, 在设置的时间里所选的攻击文件顺序轮播, 时间结束时结束测试; 按次数播放时, 设置播放次数后, 所选文件轮流播放该次数后结束测试。

播放速率: 测试时的发包速率对比源文件的播放速率, 如 2 就是代表以 2 倍的速度发包

播放间隔: 两次播放之间的间隔时间

一级目录/二级目录: 所选攻击文件文件的目录, 由导入的攻击库文件决定

攻击文件列表: 已选中播放的攻击文件列表, 可以配置 1 个也可以配置多个

k) MODBUS 配置方法

modbus 是应用于电子控制器上的一种通用语言，系统仿真 modbus client 与服务端进行通信。

Common
MODBUS Parameters
分片

*工作模式: TCP模式 - client

*启用广播模式: 启用广播模式ID号为0, 未启用ID为1~247

*modbusid: 1 至 1

req/resp:

*req/resp: 添加 清空列表

控制端负载数据	终端负载数据	
0100030013	0103CD6B05	删除
0100030014	0103CD6B05	删除
0100030015	0103CD6B05	删除
0100030016	0103CD6B05	删除
0100030017	0103CD6B05	删除
0100030018	0103CD6B05	删除

工作模式: modbus 支持串口模式和 tcp/ip 模式传输，此开关用于配置是否开启串行链路。开启串行链路则支持 ASCII 模式

modbusid: 配置 modbusclient 的设备 id

req/rsp: 配置控制器和终端的负载数据，可以配置 1 条，也可以配置多条

l) NETCONF 配置方法

仿真 netconf 终端，与 netconf 服务端进行通讯

NETCONF Parameters
分片
SSH

ESN ID:

前缀: 1019001 后缀开始: 1000 后缀结束: 1499 生成效果: 101900101000 ~ 101900101499

*自定义变量: 增加变量 (最大值 - 最小值) % 步长 == 0, 最大值和最小值的差值必须为步长的整数倍, 变量名不能重复, 随机类型无需步长

变量名	最小值	最大值	类型	步长	操作
test	1	10	递增	1	删除
var	1	5	递减	2	删除
rand	1	10	随机		删除

*自定义url: 添加 清空列表 统计名需要保证唯一

url	响应数据	启用统计	请求统计名	响应统计名	操作
urn:huawei:params:xml:ns:yang:huawei-device	<?xml version="1.0" encoding="UTF-8"?>	<input checked="" type="checkbox"/>	huawei-device-req-0	huawei-device-rsq-0	删除
urn:ietf:params:xml:ns:yang:ietf-interfaces	<?xml version="1.0" encoding="UTF-8"?>	<input checked="" type="checkbox"/>	ietf-interfaces-req-1	ietf-interfaces-rsq-1	删除
urn:huawei:params:xml:ns:yang:huawei-license	<?xml version="1.0" encoding="UTF-8"?>	<input checked="" type="checkbox"/>	huawei-license-req-2	huawei-license-rsq-2	删除
urn:huawei:params:xml:ns:yang:huawei-hrp	<?xml version="1.0" encoding="UTF-8"?>	<input checked="" type="checkbox"/>	huawei-hrp-req-3	huawei-hrp-rsq-3	删除
urn:ietf:params:xml:ns:yang:ietf-system	<?xml version="1.0" encoding="UTF-8"?>	<input checked="" type="checkbox"/>	ietf-system-req-4	ietf-system-rsq-4	删除

NETCONF Parameters	分片	SSH
*username:	<input type="text" value="root"/>	
*password:	<input type="text" value="huawei@123"/>	
*hostkey:	<input type="text" value="/var/www/KODEExplorer/c"/> 选择文件	
*客户端公钥:	<input type="text" value="/var/www/KODEExplorer/c"/> 选择文件	
authkey-type:	<input type="text" value="v"/>	

ESN ID：定义 ESN ID 范围，分为前缀和后缀开始和后缀结束

自定义变量：自定义变量的范围，支持单个或以上

自定义 url：自定义 url 请求格式，支持单个或以上

SSH：配置 ssh 相应的认证信息

m) OPCUA 配置方法

快速访问

工程

系统配置

接入协议

网口设置

变量设置

媒体对象

客户端

子网

网络

负载

动作

服务端

关联

首页 / 客户端 / 动作

批量复制

<input type="checkbox"/>	<input type="checkbox"/>	*名称	*协议	类型
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		OPCUA	
<input type="checkbox"/>	<input type="checkbox"/>	https	HTTPS	
<input type="checkbox"/>	<input type="checkbox"/>	test	RAW_TCP	
<input type="checkbox"/>	<input type="checkbox"/>	http	HTTP	

Common OPCUA Parameters 分片

key/value:

*key/value: [添加](#) [清空列表](#)

key	value
test	12345d 删除

版权所有：北京触点互动信息技术有限公司 京ICP备19037780号

订单未运行

Key 值可以填写中文、英文、数字、符号等混合

Value 值只能填写数字

n) HANDLE (TCP/UDP) 配置方法

Common HANDLE Parameters 分片 TLS Handle认证

*命令: [添加](#) [清空列表](#)

命令: Query 名称: test [删除](#)

[添加index](#) [添加type](#) [添加value](#)

index: 1 [删除](#)

type: HS_SITE [删除](#)

type: HS_NA_DELEGATE [删除](#)

value: HS_ADMIN [删除](#)

```
{
  "Index": 1,
  "TimeStamp": 56789434,
  "TTLType": 1,
  "TTL": 34523454,
  "Permission": 15,
  "Type": "HS_ADMIN",
  "Data": {
    "AdminPermission": 15,
    "AdminRef": {
      "RefHandleName": "1234/2345",
      "RefIndex": 1
    }
  }
}
```

Common	HANDLE Parameters	分片	TLS	Handle认证
客户端认证:				
认证 (Authoritative) :				
*认证方式:	秘钥字符串			
*秘钥字符串:	123456			
*HASH算法:	SHA1			
凭证 (Certify) :				
需要凭证:	<input type="checkbox"/>			
DSA密钥文件:	/var/www/KODEExplorer/t	选择文件		
RSA密钥文件:	/var/www/KODEExplorer/t	选择文件		
HASH算法:	SHA1			
会话秘钥字符串:	123654			
摘要 (Digest) :				
需要摘要:	<input type="checkbox"/>			

命令: 添加查询命令和对应的名称

Index: 对应查询命令的索引

type: 对应查询命令的类型, 可支持单个或以上

Value: 对应查询值, 可支持单个或以上

Handle 认证: 客户端与服务端认证信息配置, 保持一致即可

DSA 密钥文件: /var/www/KODEExplorer/data/Group/public/home/doc/handle_cert/dsakey.pem

RSA 密钥文件: /var/www/KODEExplorer/data/Group/public/home/doc/handle_cert/rsapubkey.pem

o) L2TP 配置方法

L2TP 可与华为防火墙对接进行测试, 仪表支持模拟 L2TP client 和 server

Common	L2TP Parameters	分片	TLS
*隧道名称前缀:	dotouch	不超过50个字节	
隧道密码认证:	<input type="checkbox"/>		
*隧道密码:			
*确认隧道密码:			
保活时间:	60	s	
*隧道数量:		1-64000 ⓘ	
*会话数量:		1-64000 ⓘ	
*重试次数:		0-255	
PPP用户接入:	<input checked="" type="checkbox"/>		
*用户名密码:	<input type="text"/> <input type="button" value="+"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>		
会话心跳时间:	0	s	

隧道名称前缀: 配置隧道名称前缀, 仪表作为客户端值对前缀校验

隧道密码认证：是否开启隧道密码认证

隧道密码：client 和 server 协商 L2TP 隧道的密码，2 侧需要保持一致

保活时间：隧道保活时间，超过该时间还未建立隧道，则关闭隧道，默认 60S

隧道数量：单个隧道名需要建立的隧道数量

会话数量：单个隧道需要建立的会话数量

重试次数：隧道建立失败重试的次数

PPP 用户接入：接入类型

用户名密码：用户认证需要的用户名和密码

会话心跳时间：会话是否存活检测发送心跳报文时间

p) SMTP 配置方法

开启服务端认证：是否认证开关，需和服务端保持一致。开启后报文中会出现 SMTP 认证报文

SMTP 服务器：配置 SMTP 服务器信息

SMTP 用户名/密码：SMTP 邮件用户名和密码

SMTP 申明：申明类型，支持 ehlo 和 helo

邮件类型：支持手动编辑和导入 eml

发件人：邮件发件人

收件人/抄送/密送：邮件收件人/抄送/密送，支持单个和以上（多个以英文逗号隔开）

主题：邮件主题：

附件：邮件需要发送的附件，支持 txt/word/excel

正文：邮件发送的正文，支持中英文/数字/字母/特殊符号/图片

q) MQTT_TCP 配置方法

认证方式：选择客户端认证方式（目前支持不认证、用户名密码认证、客户端 ID 认证三种认证方式）

角色：仿真 MQTT 协议中的角色（目前仅支持发布者）

命令：添加对应的指令信息，支持添加和删除，支持参数的命令可以配置参数。

r) POP3 配置方法

账号密码：POP3 邮箱账号密码

命令：添加对应的指令信息，支持添加和删除

s) SIP(TCP/UDP)配置方法

快速访问
工程
系统配置
接入协议
网口设置
变量设置
媒体对象
客户端
子网
网络
负载
动作
关联

SIP_TCP-功能_标准WAV文件 SIP_TCP

SIP_TCP-分片大小-正序 SIP_TCP

Pages: 1 2 Next Last 1 of 2

Common SIP_TCP Parameters 分片

主叫UA Number前缀: 130
* 主叫UA Number起始值: 100000000
* 主叫UA Number步长: 10
被叫UA Number前缀: 189
* 被叫UA Number起始值: 200000000
* 被叫UA Number步长: 10
* 语音文件: 自定义音频
* 编码格式: G.711A
* 采样率: 8000 Hz
* 比特率: 64 kbps
* RTP 流的发包间隔: 40 ms

版权所有: 北京触点互动信息技术有限公司 京ICP备19037780号 订单未运行

主叫 UA Number 前缀:主叫 UA Number 的前缀，仅支持数字，英文字母，下划线

主叫 UA Number 起始值:主叫 UA Number 的起始值，仅支持数字

主叫 UA Number 步长:主叫 UA Number 的步长，在起始值基础上递增

被叫 UA Number 前缀:被叫 UA Number 的前缀，仅支持数字，英文字母，下划线

被叫 UA Number 起始值:被叫 UA Number 的起始值，仅支持数字

被叫 UA Number 步长:被叫 UA Number 的步长，在起始值基础上递增

语音文件:仿真的语音文件，支持 选择标准的 wav 文件 、自定义音频。

编码格式:自定义音频中的配置项，支持 G.711A,G.711U

采样率:自定义音频中的配置项，单位 Hz

比特率:自定义音频中的配置项，单位 Kbps

RTP 流发包间隔:单位 ms，RTP 流发包间隔需要大于或等于 10ms

t) COAP_UDP 配置方法

Common COAP_UDP Parameters 分片

客户端:

请求: 添加 清空列表

删除

method: GET
type: CON(必须回复)
options: coap://
payload:

删除

method: POST
type: CON(必须回复)
options: coap://
payload:

删除

method: PUT
type: CON(必须回复)
options: coap://
payload:

删除

method: DELETE
type: CON(必须回复)
options: coap://
payload:

请求：添加对应的请求，也可以删除，请求选项和载荷可配置。

u) GRE 配置方法

GRE 认证信息在子网中进行配置

启用 GREVPN：是否启用 GREVPN

GRE 本端地址：GRE 隧道的本端地址

GRE 对端地址：GRE 隧道的对端地址

GRE 隧道校验：是否开启隧道校验

GRE 关键字校验：GRE 隧道采用的关键字校验信息

3.8 服务端

3.8.1 服务端子网配置

服务端子网配置项用来配置服务端回应 client 时的源 IP 地址范围，支持 IPv4 与 IPv6 。

点击 **+** 按钮可添加多个服务端子网，并可编辑和删除已有服务端子网。

名称：该 IP 子网的名称

服务端网卡：选择作为服务端的网卡

IP 目的地址开始/IP 目的地址结束：用来配置该仿真时服务端子网的起始 IP 与结束 IP。

ARP 学习：当被测设备工作在二层，如网桥模式、透明模式等，此时仪表服务端与客户端处于同一个网段时，在该场景下需开启该功能，此时服务端会直接向客户端 IP 发起 arp 请求后将数据包直接发送给客户端，而不是将数据包交由下一跳网关转发，开启该功能后，设备工作在 L2 模式。

启用 VLAN：当该子网需要启用 VLAN 时需勾选该功能（并配置下方 VLAN 相关信息）

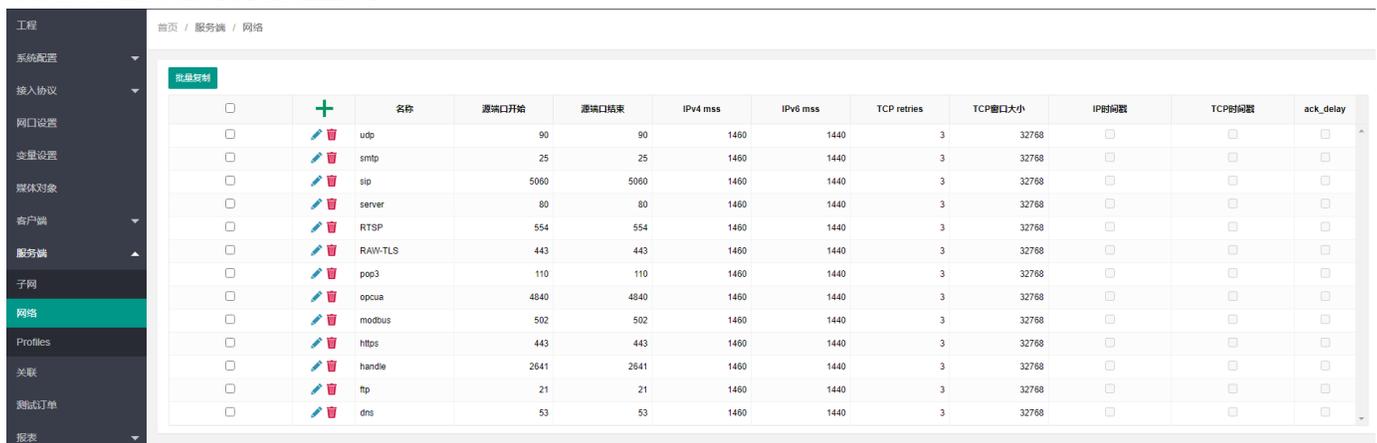
VLAN ID：该子网所在的 VLAN

优先级：配置该 VLAN 的 Priority

启用 IP 配置：配置该 Server 子网所在 VLAN 的 VLAN 子网 IP 地址

3.8.2 服务端网络配置

服务端网络配置配置服务端使用的端口范围和报文长度等参数。点击页面的  按钮新增网络配置，也可以编辑和删除已有网络配置项。



<input type="checkbox"/>		名称	源端口开始	源端口结束	IPv4 mss	IPv6 mss	TCP retries	TCP窗口大小	IP时间戳	TCP时间戳	ack_delay
<input type="checkbox"/>		udp	90	90	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		smtp	25	25	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		sip	5060	5060	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		server	80	80	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		RTSP	554	554	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		RAW-TLS	443	443	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		pop3	110	110	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		opcua	4840	4840	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		modbus	502	502	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		https	443	443	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		handle	2641	2641	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		ftp	21	21	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		dns	53	53	1460	1440	3	32768	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

名称：该条网络配置的名称

源端口开始：配置仿真时 Server 端的四层源端口最小值

源端口结束：配置仿真时 Server 端的四层源端口最大值，最大值为 65535

IPv4 mss：IPv4 最大报文段长度

IPv6 mss：IPv6 最大报文段长度

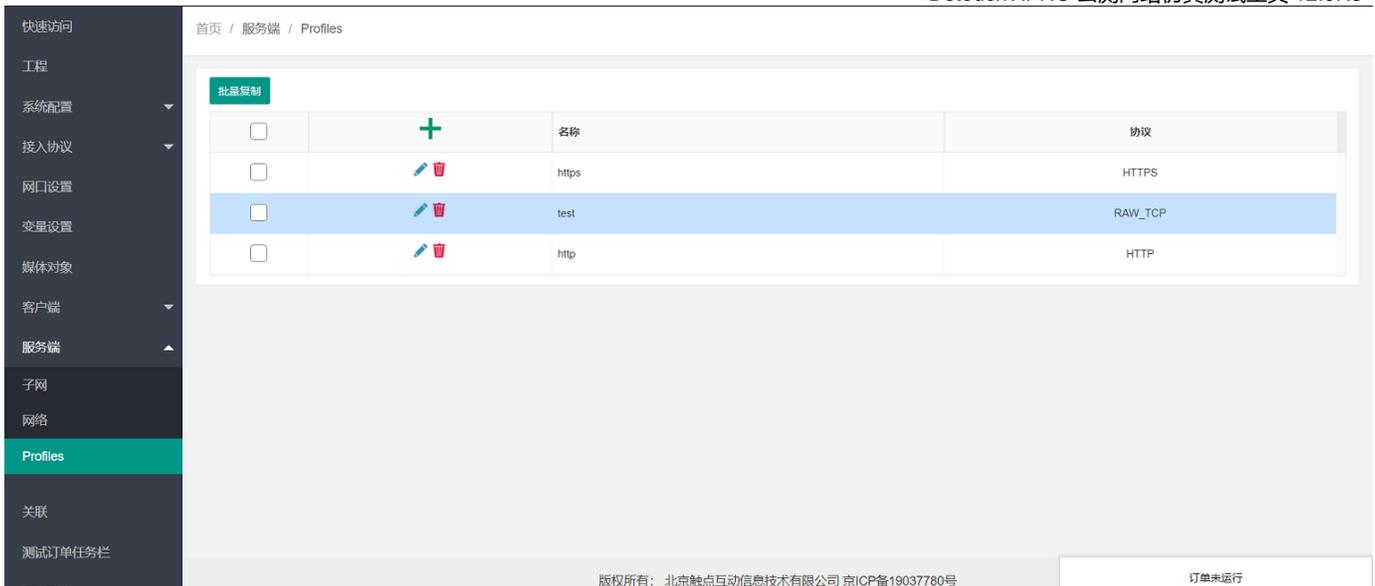
TCP retries：TCP 重传次数

TCP 窗口大小：配置滑动窗口大小

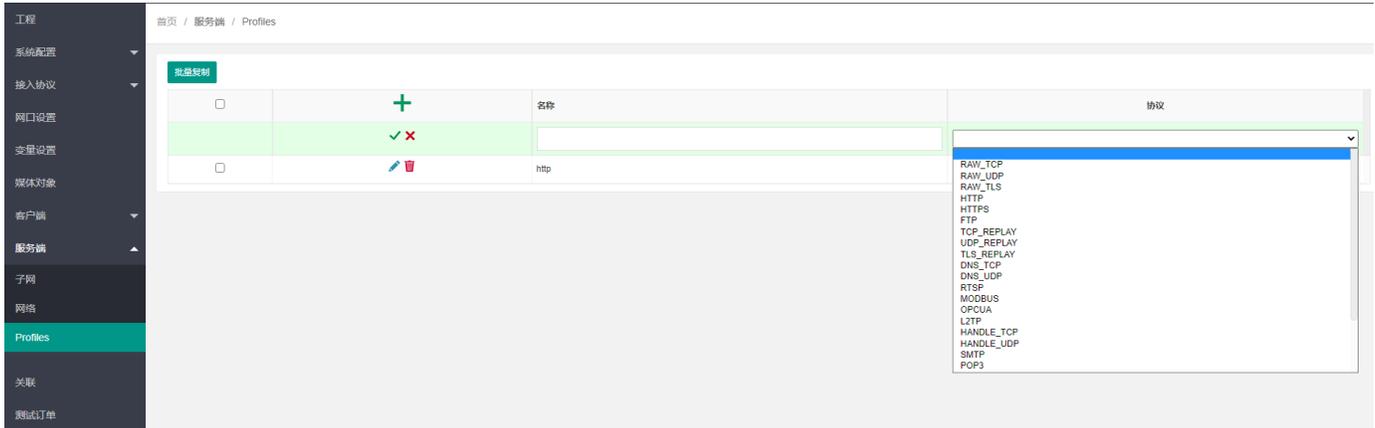
IP 时间戳：该功能是在 ip option 上打上时间戳来计算链路时延（双单臂需要客户端和服务端同时开启 ip 时间戳才会统计时延）

3.8.3 服务端 Profiles 配置

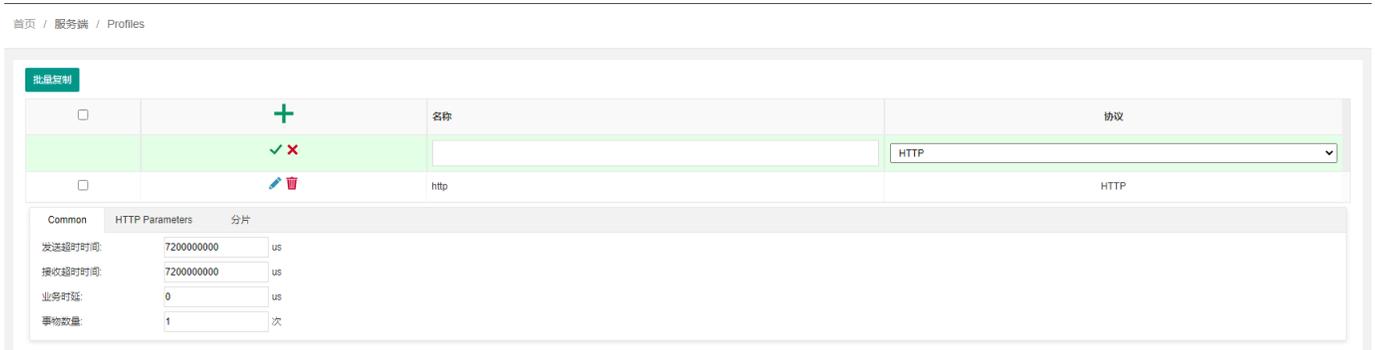
Profiles 用来配置网络协议仿真时，所仿真协议的 Server 端一侧的基本配置，部分仿真动作如网络攻击仿真不需要 server，所以无需配置服务端。页面可添加多个动作，并可编辑和删除已有 Profiles。



点击 **+** 按钮添加新的 profile 后，可以选择所需仿真的协议。



a) 通用配置



Profiles 名称：配置该 Profile 的名称

发送超时时间：单位 us，如在该时间范围内未将需要发送的内容发送出去，则认为发送失败

接收超时时间：单位 us，如服务端在该时间范围内未收到客户端请求的全部内容，则认为接收失败

Think Time：表示服务端在收到客户端请求事务时，延迟所设置的时间再发送事务响应，如客户端发起 HTTP GET 请求，此时服务端会延迟此处所配置的时间后才发送 Reponse 响应。

事务数量：配置服务端响应的事务数量，当事务数量为 2 时，表示在一个 TCP 连接中，客户端会发起 2 次相同的业务请求，服务端也会响应两次。

首页 / 服务端 / Profiles

The screenshot shows the 'Profiles' configuration page. At the top, there is a 'Batch Copy' (批量复制) button and a table with columns for 'Name' (名称) and 'Protocol' (协议). Below the table, there are tabs for 'Common', 'HTTP Parameters', and 'Fragmentation' (分片). The 'Fragmentation' tab is active, showing settings for 'Start Fragmentation' (开启分片), 'Fragment Type' (分片类型), 'Fragment Size' (分片大小), 'Fragment Count' (分片数量), 'Fragment Processing Method' (分片处理方式), 'Fragment Send Order' (分片发送顺序), and 'Only Send Packets' (仅发送数据包).

开启分片：当打开该功能开关时，服务端将依据设置的规则对 IP 报文进行分片

分片类型：当前支持分片大小与分片数量两种分片方式，当分片类型为“分片大小”时，服务端将按照设置的值对 IP 报文进行分片操作，如设置的分片大小为 100 字节，实际报文大小为 1200 字节，则该 IP 报文将会被分为 12 个 IP 分片。当分片类型为“分片数量”时，服务端将按照设置的数量对原始 IP 报文进行分片，如设置的“分片数量”为 5，实际 IP 报文大小为 1000 字节，则该 IP 报文会被分为 5 个等长的 IP 分片。

分片大小：当“分片类型”设置为分片大小时。该处配置有效，用来配置每个 IP 分片的长度

分片处理方式：当前仅支持自动分片，该处配置默认即可

分片发送顺序：当前支持正序发送分片与倒序发送分片两种方式，正序发送是指按照分片包的顺序先后发送，即按照第一个分片、第二个分片、第 N 个分片的顺序发送，倒序发送则是先发送第 N 个分片，再发送第 N-1 个分片，直至最后发送第一个分片。

b) RAW TCP/UDP/TLS 配置方法

The screenshot shows the 'RAW_TCP Parameters' configuration page. It has tabs for 'Common', 'RAW_TCP Parameters', and 'Fragmentation' (分片). The 'RAW_TCP Parameters' tab is active, showing settings for 'Whether to measure delay' (是否测量时延), 'Packets collected per second' (每秒采集包数), 'Request size' (请求大小), and 'Response size' (响应大小).

请求大小（客户端请求内容长度校验）：用来服务端对比校验客户端发送的内容长度与应该接收的内容长度是否一致，服务端会根据此处配置的大小来校验客户端的请求是否正确。

响应大小（客户端请求响应内容长度）：设置服务端响应客户端请求的响应内容长度大小，客户端收到后会与其配置的“响应大小”进行对比，如两者一致，则认为事务结束。

服务端与客户端仅对双方发送内容的长度进行校验，不对内容是否一致进行校验。



服务端与客户端的请求大小与响应大小必须一致，即服务端的请求大小与客户端的请求大小一致，服务端的响应大小与客户端的响应大小一致。

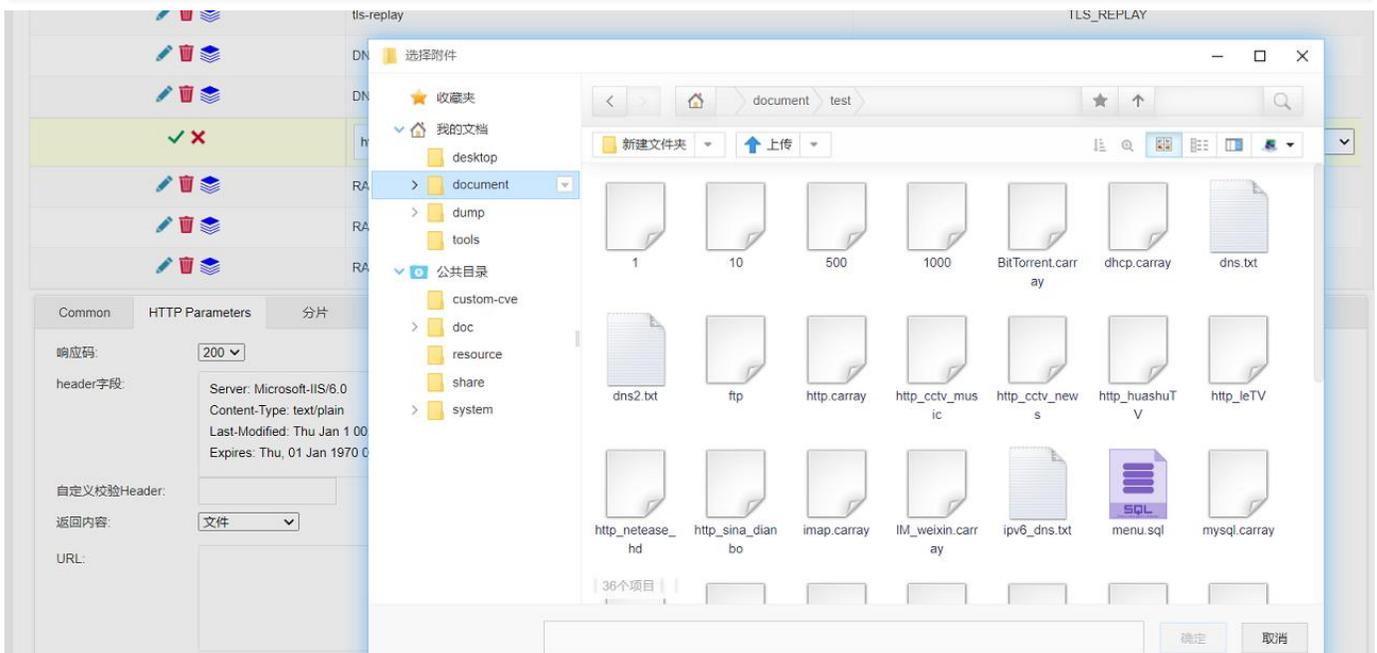
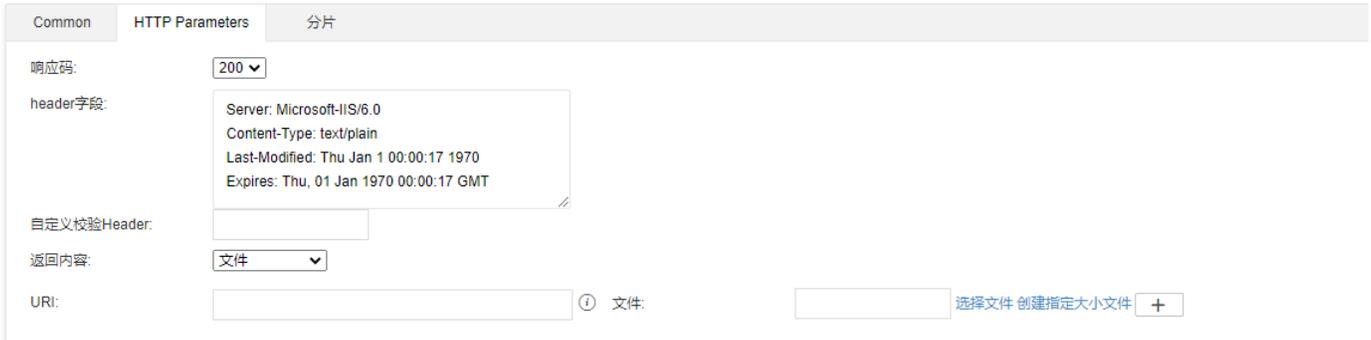
c) HTTP/HTTPS 配置方法

HTTP/HTTPS 协议仿真时主要区别为当仿真 HTTPS 时，系统会自动完成 SSL 的协商及加密通道的建立过程，具体配置方法完全一致。

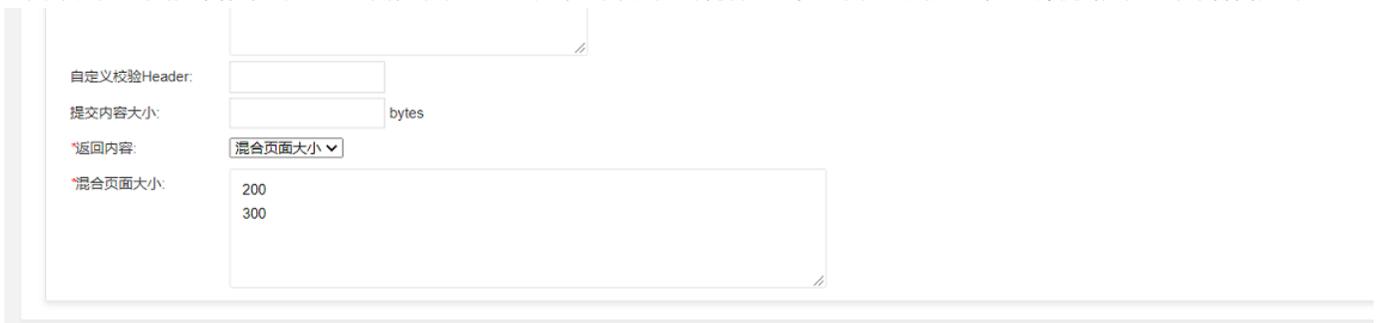
当服务端返回内容类型为“页面大小”时，服务端会随机伪造“响应大小”配置项中设定长度的内容



当服务端返回内容类型为“文件”时，服务端会加载“文件”配置项中选择的文件作为内容返回给客户端



当服务端返回内容类型为“混合页面大小”是，服务端会将配置中混合大小按照轮询顺序依次返回给客户端



当服务端返回类容类型为“指定目录”时，服务端会加载指定目录下的文件名作为 uri 返回给客户端，此时客户端配置的 uri 也必须是该目录下的 uri 名称

Common	HTTP Parameters	分片
响应码:	<input type="text" value="200"/>	
header字段:	<pre>Server: Microsoft-IIS/6.0 Content-Type: text/plain Last-Modified: Thu Jan 1 00:00:17 1970 Expires: Thu, 01 Jan 1970 00:00:17 GMT</pre>	
自定义校验Header:	<input type="text"/>	
返回内容:	<input type="text" value="指定目录"/>	
目录:	<input type="text" value="/test/test"/>	

响应码: 设置服务端响应客户端请求时的响应码，当前支持 200 和 404

Header 字段: 服务端 Response 报文的 header 字段，可自定义标准及非标准字段。

文件: 配置服务端响应客户端请求该 URI 时使用指定文件返回给客户端，当配置该项时，“响应大小”字段不生效。

自定义校验 Header: 用来验证客户端所配置 header 字段与服务端 header 字段是否一致，如不一致，则认为请求非法。



当“指定目录”的目录大小大于 1G 时，请使用 HTTP Dir 子系统进行测试。

d) FTP 配置方法

Common	FTP Parameters	分片
*开启认证:	<input type="checkbox"/>	
用户名:	<input type="text" value="anonymous"/>	
密码:	<input type="text"/>	
数据传输端口范围:	<input type="text" value="40001"/> - <input type="text" value="65000"/>	
上传下载类型:	<input type="text"/>	
突发大小:	<input type="text" value="50000"/> bytes	
突发间隔:	<input type="text" value="2"/> ms	

开启认证: 是否启用登陆认证，开启认证后，客户端用户名和密码必须和服务端保持一致。

用户名: 设置客户端登陆 FTP 服务器的账号，账号需要和服务端配置保持一致

密码: 设置客户端登陆 FTP 服务器的密码，密码需要和服务端保持一致

数据传输端口范围: 用来配置 FTP 数据连接时所使用的端口的范围

上传下载类型:

支持文件大小和文件路径，选择为文件大小时，直接输入大小数值即可。

选择为文件路径时，需配置 URI，然后选择资源管理器中任意文件。

e) TCP/UDP/TLS REPLAY 配置方法

Common	TCP_REPLAY Parameters	分片
*回放文件:	<input type="text" value="选择资源管理器文件"/>	
*回放样包:	<input type="text"/> 选择文件	
开启HOST替换:	<input type="checkbox"/>	
HOST替换:	<input type="text"/>	

TCP/UDP/TLS 回放功能分别用来回放基于 TCP/UDP/TLS 的标准应用或非标准应用，仿真模块会自动构建 4 层的状态信息，实现带 4 层状态的回放，**当前支持单个数据包中仅有 1 条流的回放，不支持单个数据包中含有多条流。**

回放文件：目前支持选择 资源管理文件(carray 文件) 和 L7 回放样包(pcap/cap 文件)。

回放样包：当回放文件是选择资源管理器文件时，回放时要求数据包格式为 C Arrays，因此对于常规的 PCAP/CAP 包，因此需借助 wireshark 将其转换成 C Arrays 格式。

开启 HOST 替换：是否替换回放文件中的 host

HOST 替换：要替换的 HOST



当回放某个指定的应用时，此时客户端与服务端需配置同一个数据包文件。



当前版本仅支持单个数据包文件中只包含 1 条流。

f) DNS_TCP/DNS_UDP 配置方法

Common	DNS_TCP Parameters	分片
*Host文件:	<input type="text" value="上传文件"/>	<small>支持一个域名对应多个IP，最多支持20个IP</small>
*上传Host文件:	<input type="text"/> 选择文件 ⓘ	
*TTL生存时间(s):	<input type="text" value="0"/>	

Common	DNS_TCP Parameters	分片
*Host文件:	<input type="text" value="手动创建"/>	
*手动创建host文件:	<input type="text"/> <input type="button" value="+"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>	
*TTL生存时间(s):	<input type="text" value="0"/>	

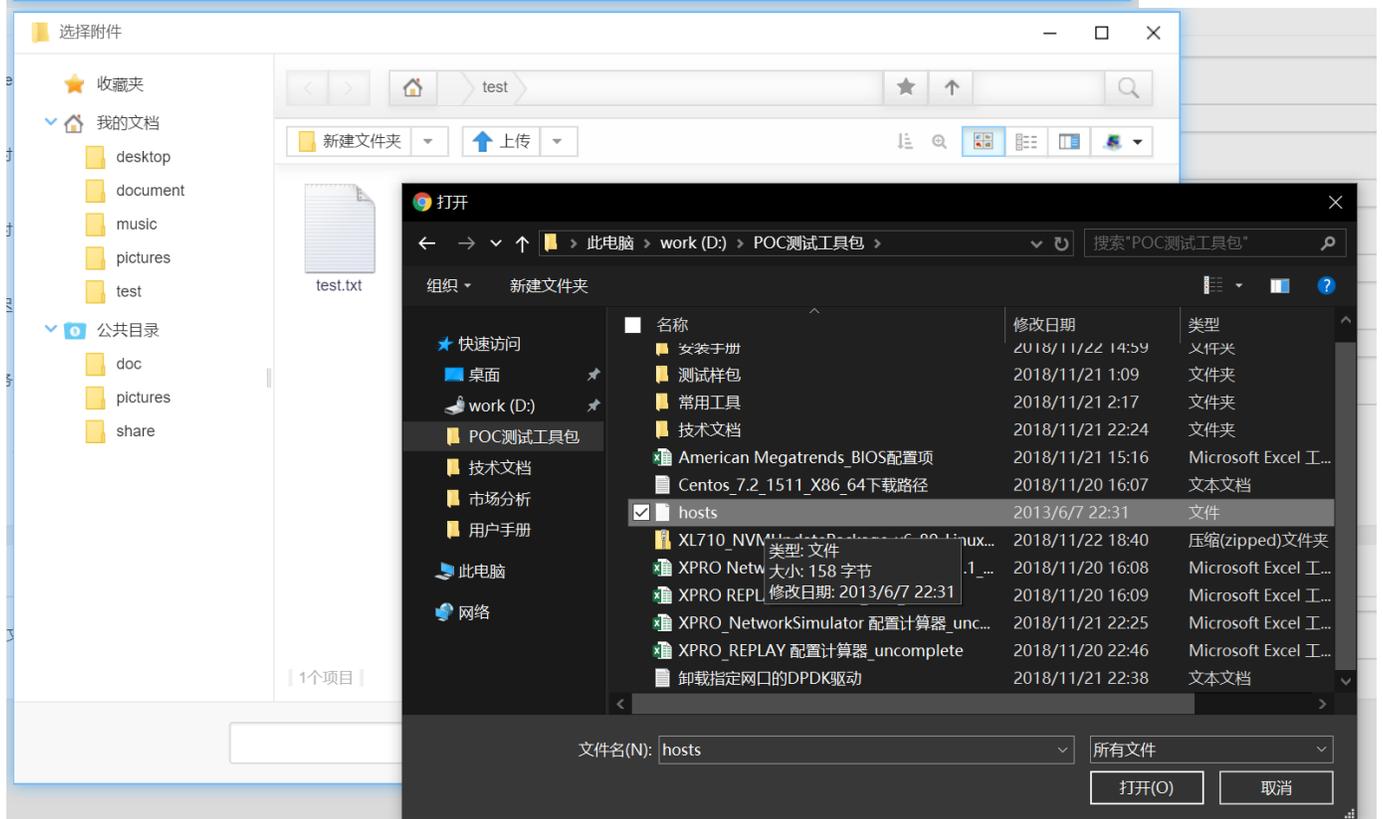
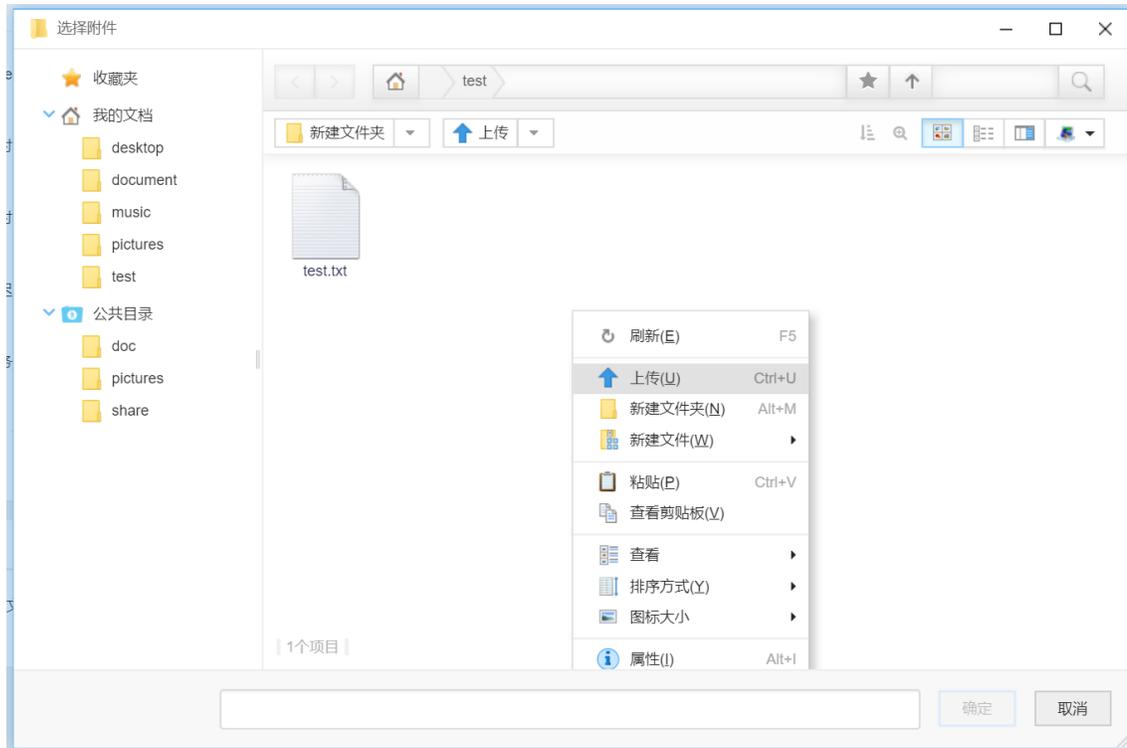
DNS_TCP/DNS_UDP 用来配置域名与 IP 的对应关系

Host 文件：用来添加记录有域名与 IP 对应关系的 Host 文件，当接收到客户端发起的域名解析请求时，服务端将查询 host 文件，根据 host 文件中记录的域名与 IP 对应关系，响应客户端的域名解析请求。支持 上传文件 和 手动创建

手动创建 host 文件：当 Host 文件选择 手动创建 时，展示 **手动创建 host 文件**，点击 + 号可以手动创建 host 文件，并支持修改和删除。

上传 Host 文件：当 Host 文件选择 上传文件时，展示上传 Host 文件，点击选择文件即可从资源管理器中选择一上传的 host 文件，Host 文件类型及域名填写方式参照 Linux 下的 hosts 文件，可直接下载 linux 系统/etc 目录下的 hosts 文件进行编辑添加 DNS 记录后上传至仪表。上传方式如下：

STEP 1: 点击输入框，点击“上传”上传已完成配置的 hosts 文件。



g) RTSP 配置方法

RTSP 服务端配置中，仅需要配置服务端播放的流媒体文件。

流媒体支持两种模式

文件：自主上传的流媒体文件，目前仅支持 H264 格式的文件。

媒体对象：即媒体对象中配置的虚拟视频媒体文件，下拉选择即可。

h) MODBUS 配置方法

MODBUS 服务端配置中，需要配置工作模式和协议传输模式

控制端负载数据	终端负载数据	
0100030013	0103CD6B05	删除
0100030014	0103CD6B05	删除
0100030015	0103CD6B05	删除
0100030016	0103CD6B05	删除
0100030017	0103CD6B05	删除
0100030018	0103CD6B05	删除
0100030019	0103CD6B05	删除

工作模式： modbus 支持串口模式和 tcp/ip 模式传输，此开关用于配置是否开启串行链路。开启串行链路则支持 ASCII 模式

modbusid： 配置 modbus client 的设备 id

req/rsp： 配置控制器和终端的负载数据，可以配置 1 条，也可以配置多条

i) OPCUA 配置方法

Common	OPCUA Parameters	分片
key/value:		
*key/value: 添加 清空列表		
key	value	
key_test	12345678	删除

Key 值可以填写中文、英文、数字、符号等混合

Value 值只能填写数字

注意：需与客户端填写保持一致

j) L2TP 配置方法

□	+	名称	协议
	✓ ×		L2TP

Common	L2TP Parameters	分片
本端隧道名称前缀:	dotouch	
隧道密码认证:	<input checked="" type="checkbox"/>	
隧道密码:	
确认隧道密码:	
认证域:	不认证 + ↗ ⊗	
L2TP认证模式:	CHAP&PAP ▼	
用户地址分配:	ip_pool + ↗ ⊗	
保活时间:	60 s	

edit ×

*名称 ip_pool 服务器地址为服务器承载协议目

用户地址池分配(最多200个)

No.	*本端IP	*服务器地址	*地址池起始地址	*地址池结束地址	*首选DNS	*备选DNS	+
1	172.16.100.5	10.1.1.1	10.1.1.100	10.1.1.110	10.1.1.1	8.8.8.8	添加 删除

本端地址填写服务器子网地址段内ip

地址池为与承载协议目的地址同段地址

本端隧道名称：配置本端隧道名称，默认与客户端一致即可

隧道密码认证：是否开启隧道密码认证

隧道密码：client 和 server 协商 L2TP 隧道的密码，2 侧需要保持一致

认证域：添加用户认证用户名和密码

L2TP 认证模式：支持 CHAP/PAP/CHAP&PAP 三种模式

PPP 用户接入：接入类型

用户地址分配：配置 server 分配给用户的 ip 信息,可以新增, 修改, 删除

保活时间：隧道保活时间, 超过该时间还未建立隧道, 则关闭隧道, 默认 60S

k) HANDLE (TCP/UDP) 配置方法

The screenshot displays the configuration interface for HANDLE (TCP/UDP). It is divided into several sections:

- HANDLE Parameters:**
 - 命令 (Command): Query
 - 名称 (Name): test
 - index: 1
 - value: HS_ADMIN
 - type: HS_SITE
 - type: HS_NA_DELEGATE
- Preview:** A JSON object showing the configuration details:


```

      {
        "Index": 1,
        "TimeStamp": 56789434,
        "TTLType": 1,
        "TTL": 34523454,
        "Permission": 15,
        "Type": "HS_ADMIN",
        "Data": {
          "AdminPermission": 15,
          "AdminRef": {
            "RefHandleName": "1234/2345",
            "RefIndex": 1
          }
        }
      }
      
```
- Handle认证 (Handle Authentication):**
 - 服务端认证 (Server Authentication):**
 - 认证 (Authenticative):
 - 需要认证 (Need Authentication):
 - 秘钥字符串 (Secret String): 123456
 - DSA密钥文件 (DSA Key File): [选择文件]
 - HASH算法 (Hash Algorithm): SHA1
 - 凭证 (Certify):**
 - 凭证方式 (Certificate Type): HS_SIGNED
 - DSA密钥文件 (DSA Key File): /var/www/KODEplorer/ [选择文件]
 - RSA密钥文件 (RSA Key File): /var/www/KODEplorer/ [选择文件]
 - HASH算法 (Hash Algorithm): SHA1
 - 会话秘钥字符串 (Session Secret String): 123654
 - 摘要 (Digest):**
 - 摘要方式 (Digest Method): MD5

命令：添加查询命令和对应的名称

Index：对应查询命令的索引

type：对应查询命令的类型, 可支持单个或以上

Value：对应查询值, 可支持单个或以上

Handle 认证：客户端与服务端认证信息配置, 保持一致即可

DSA 密钥文件: /var/www/KODEplorer/data/Group/public/home/doc/handle_cert/dsakey.pem

RSA 密钥文件: /var/www/KODEplorer/data/Group/public/home/doc/handle_cert/rsapubkey.pem

l) SMTP 配置方法

Common	SMTP Parameters	分片	TLS
开启服务端认证: <input type="checkbox"/>			
*SMTP用户名: <input type="text"/>			
*SMTP密码: <input type="text"/>			

开启服务端认证: 是否认证开关, 需和客户端保持一致。开启后报文中会出现 SMTP 认证报文

SMTP 用户名/密码: 与客户端配置保持一致

m) POP3 配置方法

Common	POP3 Parameters	分片	TLS
*账号: <input type="text"/>			
*密码: <input type="text"/>			

账号/密码: 与客户端配置保持一致

n) SIP(TCP/UDP)配置方法

快速访问

工程

系统配置

接入协议

网口设置

变量设置

媒体对象

客户端

服务端

子网

网络

Profiles

关联

测试订单任务栏

首页 / 服务端 / Profiles

批量复制

+
✓✗
✂

		名称	协议
<input type="checkbox"/>		<input type="text"/>	SIP_TCP
<input type="checkbox"/>		http-server	HTTP

Common	SIP_TCP Parameters	分片
被叫UA Number前缀:	<input type="text" value="189"/>	
*被叫UA Number起始值:	<input type="text" value="200000000"/> ⓘ	
*被叫UA Number步长:	<input type="text" value="10"/>	
*语音文件:	<input type="text" value="自定义音频"/>	
*编码格式:	<input type="text" value="G.711A"/>	
*采样率:	<input type="text" value="8000"/> HZ	
*比特率:	<input type="text" value="64"/> kbps	
*RTP 流的发包间隔:	<input type="text" value="40"/> ms ⓘ	

版权所有: 北京触点互动信息技术有限公司 京ICP备19037780号

订单未运行

被叫 UA Number 前缀:被叫 UA Number 的前缀, 仅支持数字, 英文字母, 下划线

被叫 UA Number 起始值:被叫 UA Number 的起始值, 仅支持数字

被叫 UA Number 步长:被叫 UA Number 的步长, 在起始值基础上递增

语音文件:仿真的语音文件, 支持 选择标准的 wav 文件 、自定义音频。

编码格式:自定义音频中的配置项, 支持 G.711A,G.711U

采样率:自定义音频中的配置项, 单位 Hz

比特率:自定义音频中的配置项, 单位 Kbps

RTP 流发包间隔:单位 ms, RTP 流发包间隔需要大于或等于 10ms



服务端与客户端的 被叫 UA, 语音文件 相关配置需保持一致。

o) MQTT_TCP 配置方法

Common	MQTT_TCP Parameters	分片
*认证方式	[用户名/密码认证] ⓘ	
*用户名:	admin ⓘ	
*密码:	123456 ⓘ	
*角色	[发布者]	
服务端:		
*命令:	[添加] [清空列表]	
func:	[CONNACK] [删除]	
msgid(0~65536)	1	
func:	[PINGRESP] [删除]	
msgid(0~65536)	1	
func:	[PUBACK] [删除]	
msgid(0~65536)	1	

认证方式: 选择客户端认证方式 (目前支持不认证、用户名密码认证、客户端 ID 认证三种认证方式)

角色: 仿真 MQTT 协议中的角色 (目前仅支持发布者)

命令: 添加对应的指令信息, 支持添加和删除。

p) COAP_UDP 配置方法

Common	COAP_UDP Parameters	分片
服务端:		
*自动回复	<input type="checkbox"/>	
*响应:	[添加] [清空列表]	
	[删除]	
method	[GET]	
type	[SUCCESS-VALID]	
options	coap://	
payload		
	[删除]	
method	[POST]	
type	[SUCCESS-CREATED]	
options	coap://	
payload		

自动回复: 开启自动回复, 开启后根据客户端请求命令自动响应。

响应: 添加对应的请求, 也可以删除, 请求选项和载荷可配置。

3.9 关联

3.9.1 服务端和客户端关联

关联配置项用来绑定最终客户端的各项配置，包括客户端关联页和服务端关联页，分别绑定前面配置的客户端和服务端各项参数。

名称	关联类型	子网类型	子网	协议类型	动作	网络	开启全局负载	负载	权重
pppoe	接入网[pppoe-ipv4]						<input type="checkbox"/>	负载	100
SIP-UDP	用户面	IPv4	client	标准协议	SIP-UDP	sip	<input type="checkbox"/>	负载	100
SIP-TCP	用户面	IPv4	client	标准协议	SIP-TCP	sip	<input type="checkbox"/>	负载	100
HANDLE-UDP	用户面	IPv4	client	标准协议	HANDLE-UDP	handle	<input type="checkbox"/>	负载	100
pop3	用户面	IPv4	client	标准协议	pop3	pop3	<input type="checkbox"/>	负载	100
smtp	用户面	IPv4	client	标准协议	smtp	smtp	<input type="checkbox"/>	负载	100
ftp	用户面	IPv4	client	标准协议	ftp	ftp	<input type="checkbox"/>	负载	100
RAW-TLS_v6	用户面	IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS	<input type="checkbox"/>	负载	100
RAW-UDP_v6	用户面	IPv6	client_v6	标准协议	RAW-UDP	client	<input type="checkbox"/>	负载	100
RAW-TCP_v6	用户面	IPv6	client_v6	标准协议	RAW-TCP	client	<input type="checkbox"/>	负载	100
rtsp	用户面	IPv4	client	标准协议	RTSP	RTSP	<input type="checkbox"/>	负载	100
udp_replay	用户面	IPv4	client	标准协议	UDP_REPLAY	udp	<input type="checkbox"/>	负载	100
tcp_replay	用户面	IPv4	client	标准协议	TCP_REPLAY	udp	<input type="checkbox"/>	负载	100
https	用户面	IPv4	client	标准协议	https	https	<input type="checkbox"/>	负载	100
HANDLE-TCP	用户面	IPv4	client	标准协议	HANDLE-TCP	handle	<input type="checkbox"/>	负载	100

点击 **+** 按钮添加关联，可以添加多条关联，并可编辑和删除已有关联

名称	关联类型	子网类型	子网	协议类型	动作	网络	开启全局负载	负载	权重
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>						
pppoe	接入网[pppoe-ipv4]						<input type="checkbox"/>	负载	100
SIP-UDP	用户面	IPv4	client	标准协议	SIP-UDP	sip	<input type="checkbox"/>	负载	100
SIP-TCP	用户面	IPv4	client	标准协议	SIP-TCP	sip	<input type="checkbox"/>	负载	100
HANDLE-UDP	用户面	IPv4	client	标准协议	HANDLE-UDP	handle	<input type="checkbox"/>	负载	100
pop3	用户面	IPv4	client	标准协议	pop3	pop3	<input type="checkbox"/>	负载	100
smtp	用户面	IPv4	client	标准协议	smtp	smtp	<input type="checkbox"/>	负载	100
ftp	用户面	IPv4	client	标准协议	ftp	ftp	<input type="checkbox"/>	负载	100
RAW-TLS_v6	用户面	IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS	<input type="checkbox"/>	负载	100

名称：配置客户端关联名称

关联类型：配置客户端关联类型

子网类型：配置客户端子网类型

子网：配置客户端子网，选择在“子网”中已配置子网

协议类型：配置客户端使用协议类型

动作：选择在“动作配置”中已配置动作

网络：配置客户端的网络

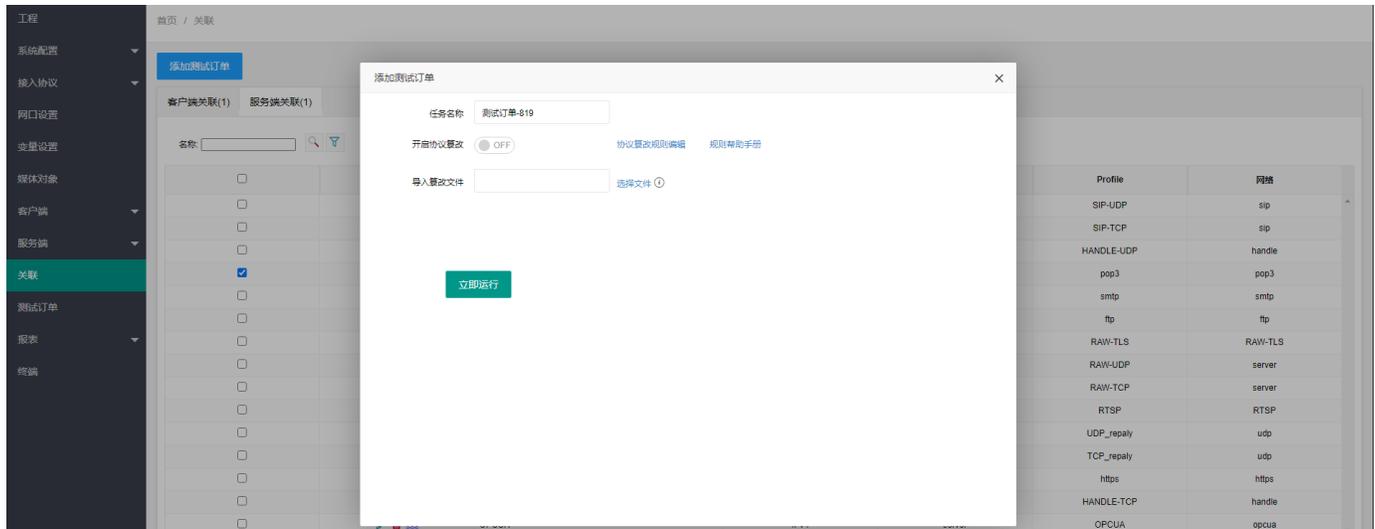
开启全局负载：配置是否开启全局负载

负载：选择在“负载”中一配置负载

权重：配置该动作的权重，在进行一次测试时，可同时仿真多种业务流量，如同时仿真 HTTP、FTP、DNS 等，此时可通过设置权重值来配置不同业务仿真流量所占比例，当前支持按照新建的权重设置。

3.9.2 添加测试订单

新建测试订单时，需要首先勾选客户端关联和服务端关联项，然后点击 **添加测试订单** 按钮，就会弹出一个生成测试订单的弹窗。



所属任务栏：任务栏名称可以自定义填写

开启协议篡改：点击开启协议篡改可以自定义修改协议，详细规则见 3.9.3 节。

立即运行：提交订单，并立即运行

3.9.3 协议篡改规则配置

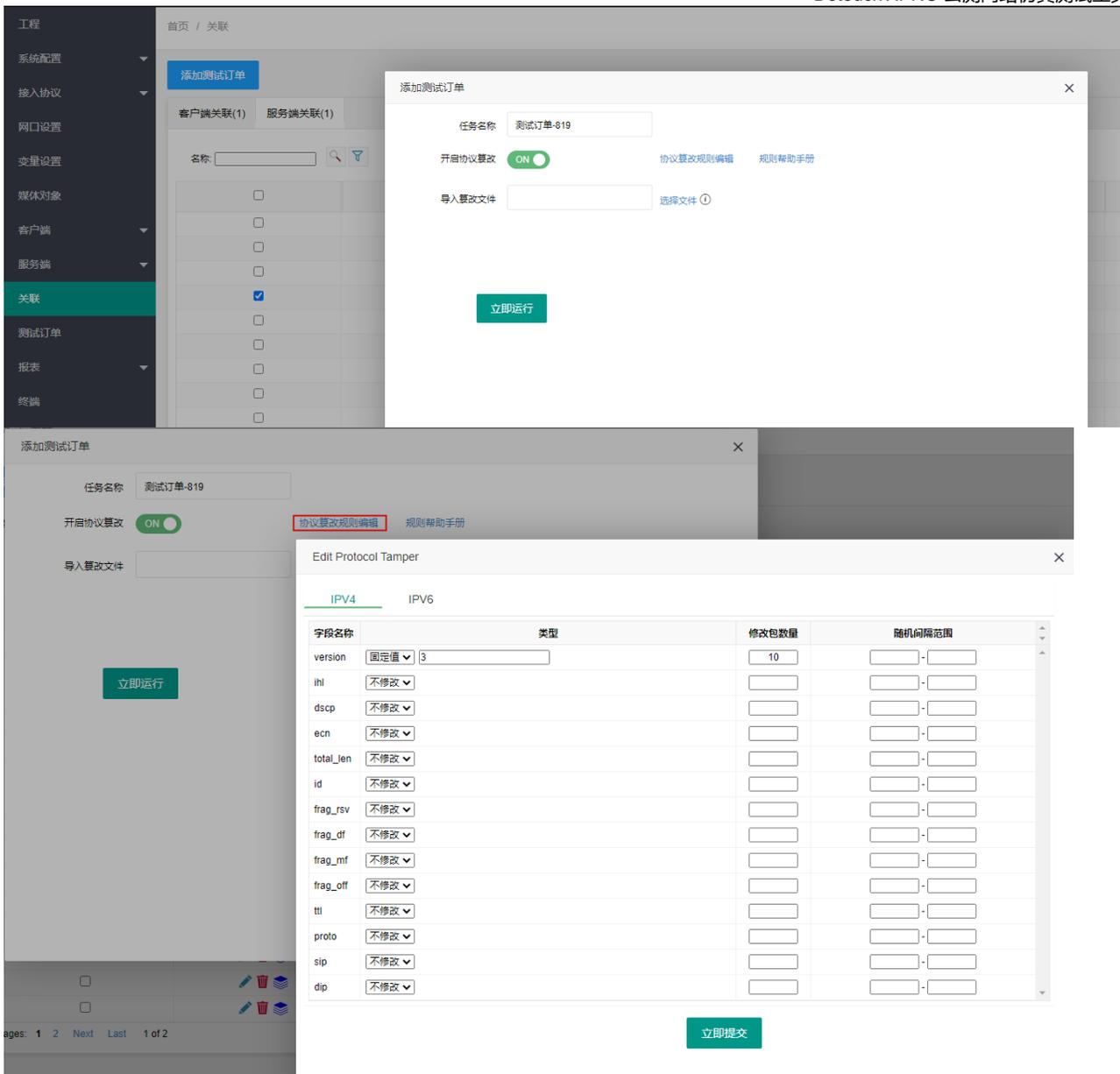
网络协议模糊测试是在 XPRO 云测网络仿真测试工具已有协议栈基础之上的叠加功能，可以给管理员提供灵活的数据包修改功能进行协议的模糊化测试，测试被测设备的协议健壮性。

目前支持的改包协议包括：

- 2 层协议：以太网
- 3 层协议：IPV4 / IPV6
- 4 层协议：TCP / UDP
- 7 层协议：通过脚本自定义规则进行匹配和修改。

配置栏在生成测试订单的页面，如下图所示：

开启协议篡改后，点击协议篡改规则编辑进入规则编辑页面



IPv4 和 IPv6 的协议篡改目前都已经支持。支持修改的协议字段在列表中可以选修改方式，包括 3 种方式

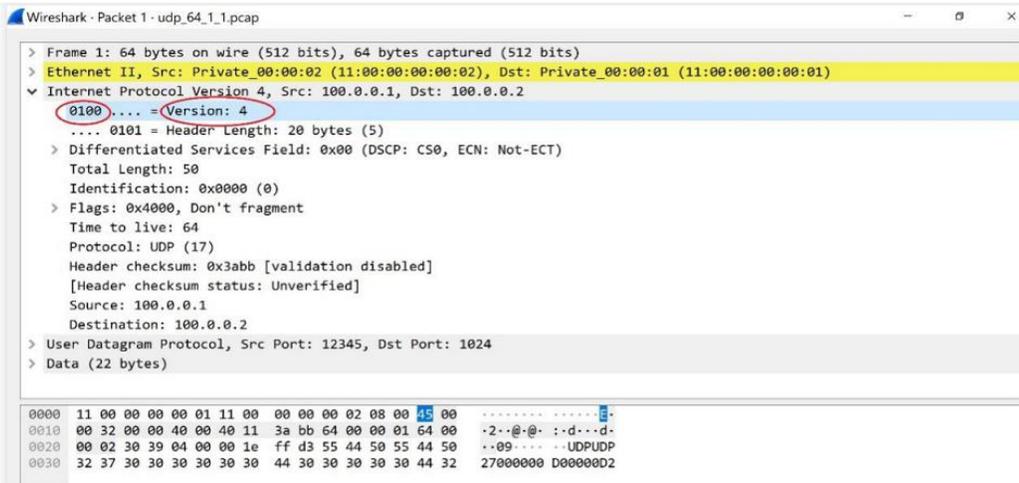
字段名称	类型	修改包数量	随机间隔范围
version	递增	10	[0, 100]
ihl	不修改		
dscp	不修改		
ecn	不修改		
total_len	不修改		
id	不修改		
frag_rsv	不修改		
frag_df	不修改		
frag_mf	不修改		
frag_off	不修改		
ttl	不修改		
proto	不修改		
sip	不修改		
dip	不修改		

固定值：将协议中的该参数修改为一个自定义的固定值

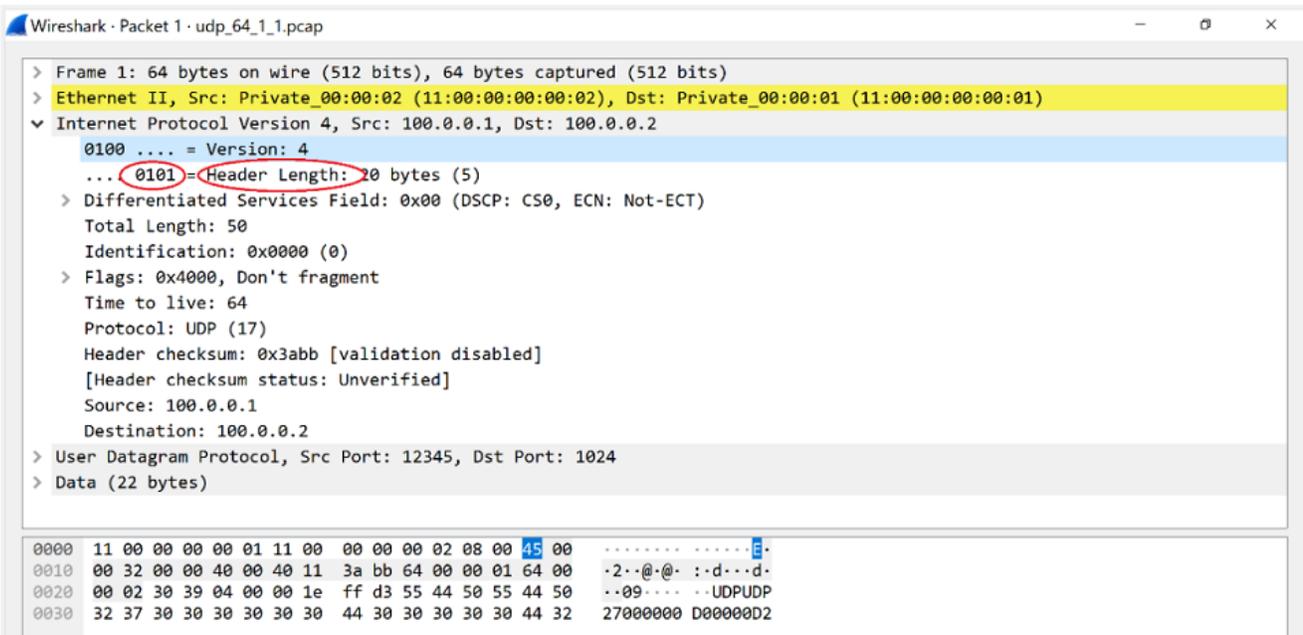
随机值：配置一个范围后，参数在该范围内随机改变，每个报文的参数值随机改变

递增：在设置的范围内，该参数按照配置的步长参数，每个报文的参数值依次递增

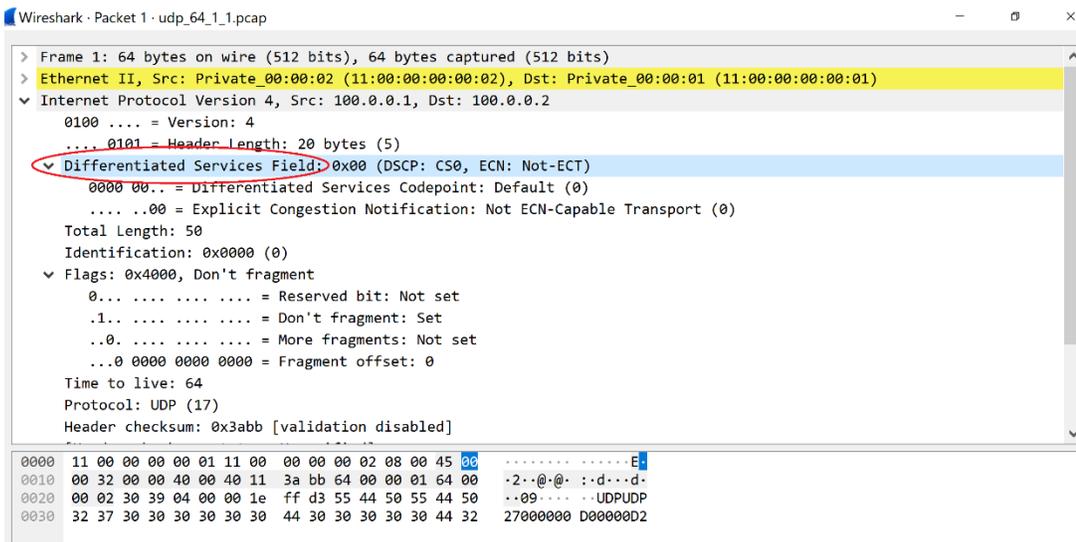
例如 IPv4 的 ver 参数，对应的是数据报文中的这个部分。



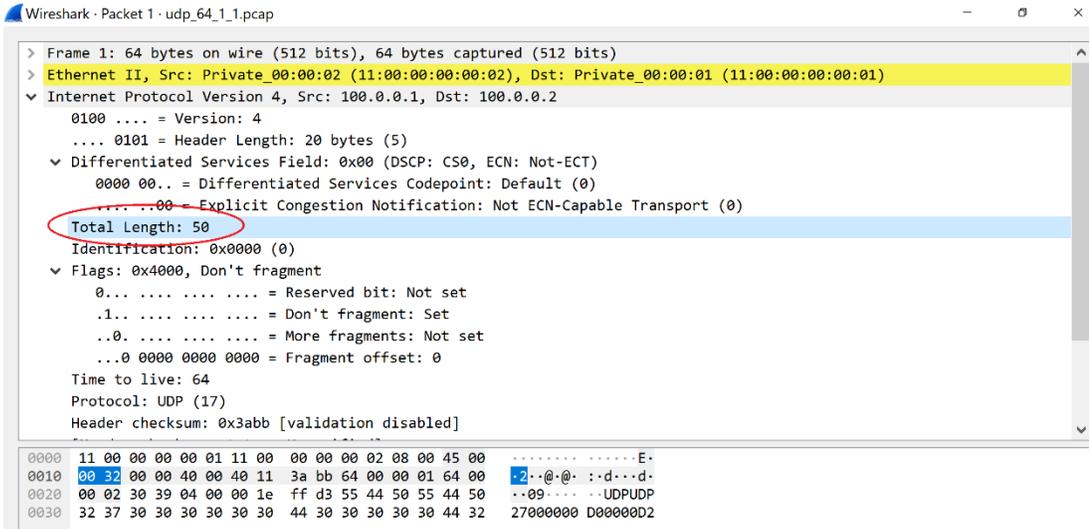
Ipv4的ihl 对应的是数据报文的这个部分:



Ipv4.dscp 对应的是数据报文的这个部分:



Ipv4.tota_lenl 对应的是数据包的如下报文:



以此类推，管理员可以通过 wireshark 工具分析数据包结构来对应系统里的触发条件的变量。按照变量定义顺序查找 wireshark 样包就可以一一对应上具体字段。目前系统已经预置好了如下包头的定义：

- 以太网
- 带 VLAN 以太网
- IPV4
- IPV6
- TCP
- UDP

3.10 测试订单

测试订单用来对当前运行及历史的测试订单进行管理。

工程	系统配置	接入协议	网口设置	变量设置	媒体对象	客户端	关联	测试订单	报表	终端			
首页 / 测试订单													
订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作				
xpro_ns20210715164144_425	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志	详情	关联	删除	重新运行
xpro_ns20210715163837_424	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志	详情	关联	删除	重新运行
xpro_ns20210715163525_423	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志	详情	关联	删除	重新运行
xpro_ns20210715163134_422	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:31:54	2021-07-15 16:31:34	日志	详情	关联	删除	重新运行
xpro_ns20210715153129_421	RAW_TCP	RAW_TCP_多...	工单运行结束	UI创建	成功		2021-07-15 15:31:45	2021-07-15 15:31:29	日志	详情	关联	删除	重新运行
xpro_ns20210715152617_420	RAW_TCP	RAW_TCP_多...	工单运行结束	UI创建	成功		2021-07-15 15:26:36	2021-07-15 15:26:17	日志	详情	关联	删除	重新运行
xpro_ns20210715151154_419	RAW_TCP	RAW_TCP_V6	工单运行结束	UI创建	成功		2021-07-15 15:12:12	2021-07-15 15:11:54	日志	详情	关联	删除	重新运行
xpro_ns20210715150933_418	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 15:09:51	2021-07-15 15:09:33	日志	详情	关联	删除	重新运行
xpro_ns20210715150631_417	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 15:06:48	2021-07-15 15:06:31	日志	详情	关联	删除	重新运行
xpro_ns20210715150419_416	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 15:04:36	2021-07-15 15:04:19	日志	详情	关联	删除	重新运行
xpro_ns20210715150132_415	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 15:01:48	2021-07-15 15:01:32	日志	详情	关联	删除	重新运行
xpro_ns20210715145938_414	RAW_TCP	RAW_TCP_多...	工单运行结束	UI创建	成功		2021-07-15 14:59:57	2021-07-15 14:59:38	日志	详情	关联	删除	重新运行
xpro_ns20210715145527_413	RAW_TCP	RAW_TCP	工单运行结束	UI创建	成功		2021-07-15 14:55:46	2021-07-15 14:55:27	日志	详情	关联	删除	重新运行
xpro_ns20210702091921_253	RAW_TCP	RAW_TCP	工单运行结束	UI创建	成功		2021-07-02 09:19:37	2021-07-02 09:19:21	日志	详情	关联	删除	重新运行
xpro_ns20210701170402_247	RAW_TCP	RAW_TCP	工单运行结束	UI创建	成功		2021-07-01 17:04:19	2021-07-01 17:04:02	日志	详情	关联	删除	重新运行

在测试订单页面，点击 **日志** 按钮可以查看订单日志。

```

运行日志
err.log ns-run.stat ipsec.log

EAL: Detected 8 lcore(s)
EAL: Detected 1 NUMA nodes
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: Selected IOVA mode 'PA'
EAL: Probing VFIO support...
EAL: PCI device 0000:04:00:0 on NUMA socket -1
EAL: invalid NUMA socket, default to 0
EAL: probe driver: 8086:10d3 net_e1000_em
EAL: PCI device 0000:0b:00:0 on NUMA socket -1
EAL: probe driver: 15ad:7b0 net_vmxnet3
EAL: PCI device 0000:13:00:0 on NUMA socket -1
EAL: PCI device 0000:1b:00:0 on NUMA socket -1
USER1: INFO: can not open file /etc/xpro-ns/fpga.ini, fpga disabled
testpmd: create a new mbuf pool <mbuf_pool_socket_0>: n=15360, size=2176, socket=0
testpmd: preferred mempool ops selected: ring_mp_mc
USER1: qmap port 0 at cores[ 3 4 5]
USER1: qmap port 1 at cores[ 3 4 5]
USER1: dmap port 0 at cores[ 2]
USER1: dmap port 1 at cores[ 2]
USER1: vnic port0 created, queues to 1 back 3!
USER1: vnic port1 created, queues to 1 back 3!
USER1: Creating mempool global_cfg_mbuf-0 on core 0(size: 8192, obj_size: 2304, priv: 4 cache: 512)
USER1: Creating mempool global_pkt_mbuf-3 on core 3(size: 15360, obj_size: 2304, priv: 4 cache: 512)
USER1: Creating mempool global_pkt_mbuf_tx_hdr-3 on core 3(size: 102400, obj_size: 346, priv: 4 cache: 512)
USER1: Creating mempool global_pkt_mbuf_clone-3 on core 3(size: 30720, obj_size: 128, priv: 4 cache: 512)
USER1: Creating mempool tcb_pool-0-3 on core 3(size: 51200, obj_size: 1062, priv: 0 cache: 0)
USER1: Found 2 Ethernet ports to start.
USER1: Started 2 Ethernet ports.
USER1: Starting test management loop on lcore 1, core index 1
USER1: Starting receive packet loop on lcore 3, core index 3
USER1: Starting receive packet loop on lcore 5, core index 5
USER1: Starting receive packet loop on lcore 4, core index 4
USER1: Checking link statuses...
USER1: Port0 Link Up, speed 1000 Mbps, full-duplex
USER1: Port1 Link Up, speed 1000 Mbps, full-duplex
USER1: Test Case 0 started on port 1
USER1: INFO: dailer 0_read 3000330 users, on port 0
USER1: Test Case 0 started on port 0
USER1: Port 1, Test Case 0 'PASSED'!
USER2: ./xpro-ns ready for test! gogo...

```

在测试订单页面，点击按钮可以 [详情](#) 进入订单详情页面，查看订单的运行状态和订单相关信息。

其中“**订单详情**”标签，可查看集中呈现的订单详细配置关联信息

工程 / 测试订单管理 / 订单详情

订单详情 监控 负载 关联统计

版本 : 1

- 工程信息
- 客户端关联详情
 - RAW_TCP_分片数量_正序_V6
 - 启用 : 否
 - 网口名 : port0
 - 服务端网卡 : port1
 - 子网类型 : IPv6
 - 权重 : 6
 - 启用全局负载 : 否
 - 名称 : RAW_TCP_分片数量_正序_V6
 - 类型 : 标准
 - 客户端子网
 - 网络
 - 动作
 - 负载
 - 运行配置
 - 网卡

点击“**监控**”标签，可查看订单运行的实时统计信息，包括客户端/服务端的会话数，tx /rx pps, tx/rx bps, tx/rx pkts 等信息

工程 / 测试订单管理 / 监控

订单详情 监控 负载 关联统计

1 2 3 4 5 6 7

订单执行

Global	Test Stages(Client)	Test Stages(Server)
start_time 2021-08-19 09:46:08	APP	APP
curr_time 2021-08-19 09:46:25	connection/s 0	connection/s 0
run_time 16s	concurrent 0	concurrent 0
remain_time 0s	sessions 300	sessions 300
max_core_usage 0%	requests 300	requests 300
port0-dump write fail 0 other fail 0	responses 300	responses 300
port1-dump write fail 0 other fail 0	invalid-msg 0	invalid-msg 0
	invite-msg 0	invite-msg 0
	no-len 0	no-len 0
	trans-enc 0	trans-enc 0
	closed-no-req 0	closed-no-req 0
	closed-no-resp 0	closed-no-resp 0
	req/s 0	req/s 0
	resp/s 0	resp/s 0
	ssl_failed 0	ssl_failed 0
	ssl_verify_err 0	ssl_verify_err 0
	connect_fail 0	open_fail 0
	min-lat 0	min-lat 0
	max-lat 0	max-lat 0
	avg-lat 0	avg-lat 0
	smin-lat 0	smin-lat 0
	smax-lat 0	smax-lat 0
	smin-avg 0	smin-avg 0
	min_delay 0	min_delay 0
	max_delay 0	max_delay 0
	avg_delay 0	avg_delay 0

点击“负载”标签，可查看图形化呈现的新建会话、并发会话、流速及包速信息

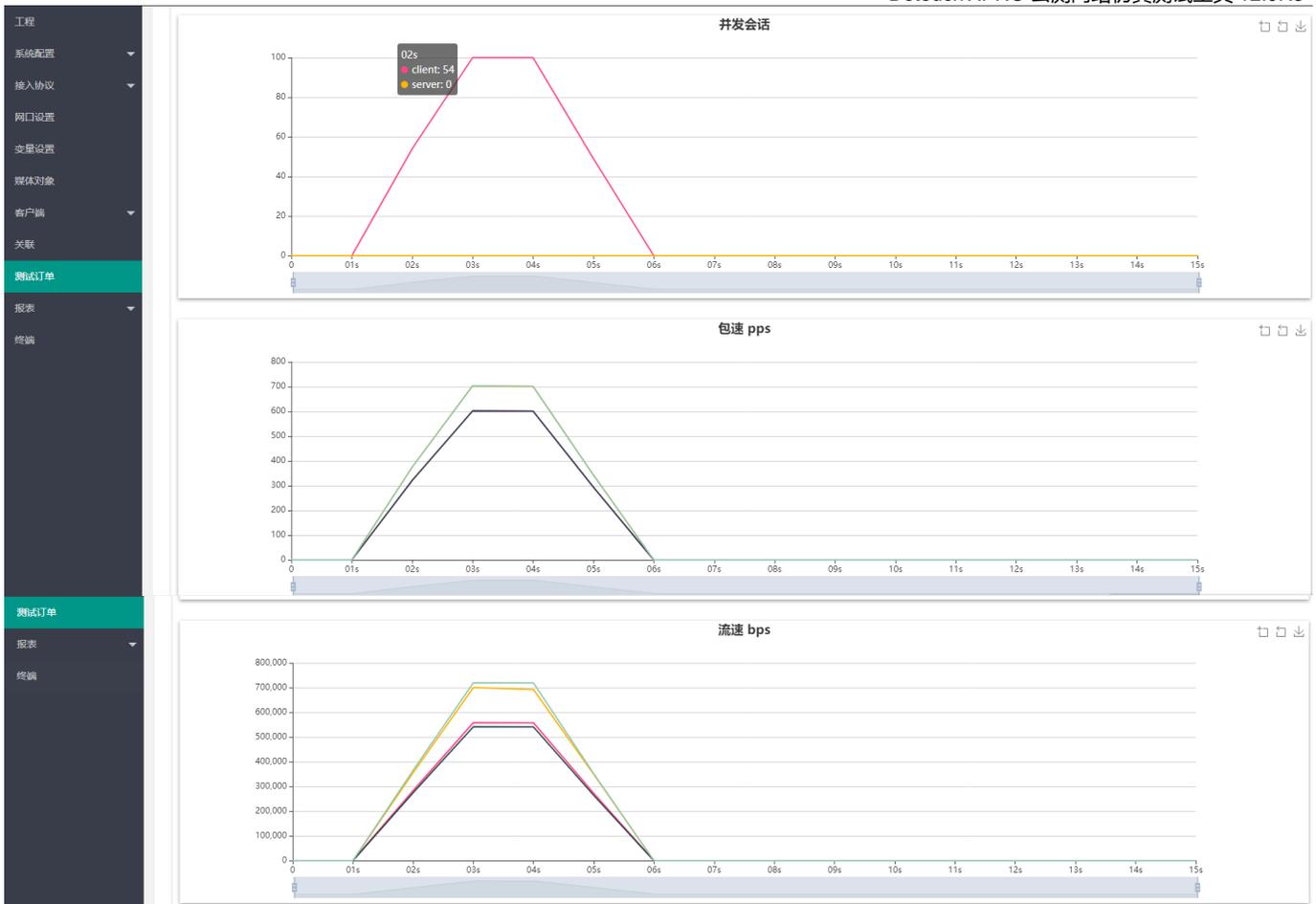
工程 / 测试订单管理 / 负载

订单详情 监控 负载 关联统计

刷新间隔 5秒

新建会话

时间 (s)	新建会话数
0	0
01s	0
02s	40
03s	100
04s	100
05s	60
06s	0
07s	0
08s	0
09s	0
10s	0
11s	0
12s	0
13s	0
14s	0
15s	0



在测试订单页面，点击 **关联** 按钮可以查看订单关联。

首页 / 测试订单

订单编号	关联ID	关联名称	子网名称	网络	动作	负载	创建时间	操作
xpro_ns20210715164144_425	1783	RAW_TCP_分片数...	ipv6	raw_tcp	RAW_TCP_分片数...	raw_tcp	2021-07-15 16:41:44	日志 详情 关联 删除 重新运行
xpro_ns20210715163837_424							2021-07-15 16:38:37	日志 详情 关联 删除 重新运行
xpro_ns20210715163525_423							2021-07-15 16:35:25	日志 详情 关联 删除 重新运行
xpro_ns20210715163134_422							2021-07-15 16:31:34	日志 详情 关联 删除 重新运行
xpro_ns20210715153129_421							2021-07-15 15:31:29	日志 详情 关联 删除 重新运行
xpro_ns20210715152617_420							2021-07-15 15:26:17	日志 详情 关联 删除 重新运行
xpro_ns20210715151154_419							2021-07-15 15:11:54	日志 详情 关联 删除 重新运行
xpro_ns20210715150933_418							2021-07-15 15:09:33	日志 详情 关联 删除 重新运行
xpro_ns20210715150631_417							2021-07-15 15:06:31	日志 详情 关联 删除 重新运行
xpro_ns20210715150419_416							2021-07-15 15:04:19	日志 详情 关联 删除 重新运行
xpro_ns20210715150132_415							2021-07-15 15:01:32	日志 详情 关联 删除 重新运行
xpro_ns20210715145938_414							2021-07-15 14:59:38	日志 详情 关联 删除 重新运行
xpro_ns20210715145527_413							2021-07-15 14:55:27	日志 详情 关联 删除 重新运行

在测试订单页面，点击 **删除** 按钮可以删除订单。

首页 / 测试订单

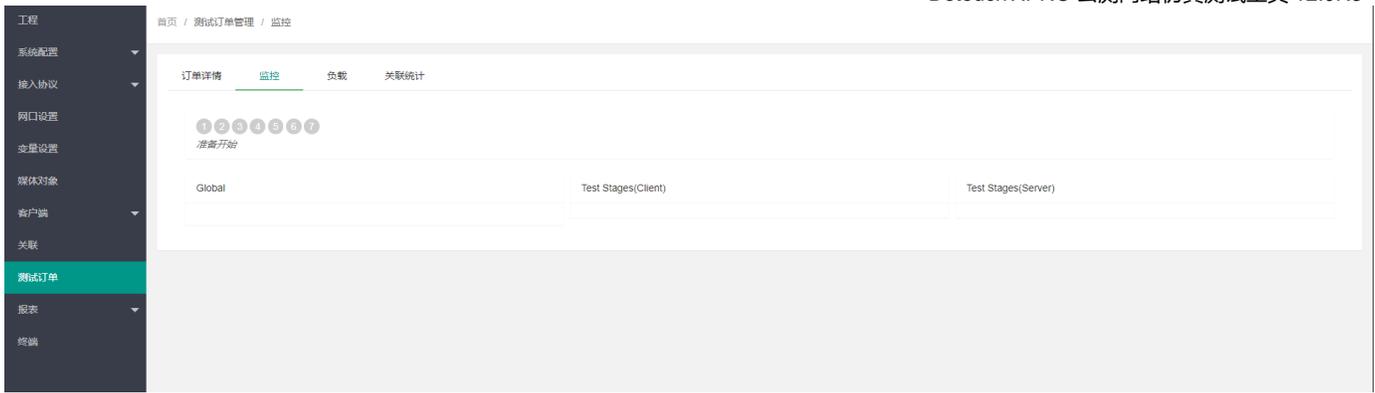
订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
xpro_ns20210818180240_819	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-08-18 18:02:59	2021-08-18 18:02:40	日志 详情 关联 删除 重新运行
xpro_ns20210715164144_425	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志 详情 关联 删除 重新运行
xpro_ns20210715163837_424	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志 详情 关联 删除 重新运行
xpro_ns20210715163525_423	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志 详情 关联 删除 重新运行
xpro_ns20210715163134_422	RAW_TCP	RAW_TCP_分...	工单运行	UI创建	成功		2021-07-15 16:31:54	2021-07-15 16:31:34	日志 详情 关联 删除 重新运行
xpro_ns20210715153129_421	RAW_TCP	RAW_TCP_多...	工单运行	UI创建	成功		2021-07-15 15:31:45	2021-07-15 15:31:29	日志 详情 关联 删除 重新运行
xpro_ns20210715152617_420	RAW_TCP	RAW_TCP_多...	工单运行	UI创建	成功		2021-07-15 15:26:36	2021-07-15 15:26:17	日志 详情 关联 删除 重新运行
xpro_ns20210715151154_419	RAW_TCP	RAW_TCP_V6	工单运行	UI创建	成功		2021-07-15 15:12:12	2021-07-15 15:11:54	日志 详情 关联 删除 重新运行
xpro_ns20210715150933_418	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 15:09:51	2021-07-15 15:09:33	日志 详情 关联 删除 重新运行

在测试订单页面，点击按 **重新运行** 按钮可以重新运行订单。重新运行订单时，会询问是否保留原订单数据，

首页 / 测试订单

订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
xpro_ns20210818180240_819	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-08-18 18:02:59	2021-08-18 18:02:40	日志 详情 关联 删除 重新运行
xpro_ns20210715164144_425	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志 详情 关联 删除 重新运行
xpro_ns20210715163837_424	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志 详情 关联 删除 重新运行
xpro_ns20210715163525_423	RAW_TCP	RAW_TCP_分...	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志 详情 关联 删除 重新运行
xpro_ns20210715163134_422	RAW_TCP	RAW_TCP_分...	工单运行	UI创建	成功		2021-07-15 16:31:54	2021-07-15 16:31:34	日志 详情 关联 删除 重新运行
xpro_ns20210715153129_421	RAW_TCP	RAW_TCP_多...	工单运行	UI创建	成功		2021-07-15 15:31:45	2021-07-15 15:31:29	日志 详情 关联 删除 重新运行
xpro_ns20210715152617_420	RAW_TCP	RAW_TCP_多...	工单运行	UI创建	成功		2021-07-15 15:26:36	2021-07-15 15:26:17	日志 详情 关联 删除 重新运行
xpro_ns20210715151154_419	RAW_TCP	RAW_TCP_V6	工单运行	UI创建	成功		2021-07-15 15:12:12	2021-07-15 15:11:54	日志 详情 关联 删除 重新运行

可以根据实际需求选择是否保留，选择完成后，会跳转到订单运行详情页



 仪表同时只能执行一个测试任务，当需要启动其他测试任务时，需先停止当前正在运行的任务后方可启动其他测试任务。

 当提交了多个任务时，会按照排队顺序依次执行排队订单。

3.11 报表

报表模块用来查看各测试订单的汇总统计报表，当前支持 11 种类型的报表

3.11.1 网口报表

网口报表功能用来从网口维度统计测试信息，包括网口的接收字节数，网口的接收报文数，网口的发送字节数，网口的发送报文数，网口的工作速率等，可拖拉滚动条查看从网口维度统计的全部信息。

ID	订单编号	网卡名	网卡ID	创建时间	工程ID	接收字节	接收报文	发送字节	发送报文	网卡速度
1549	xpro_ns202108190...	port0	0	2021-08-19 09:46:34	237	204676	1818	212582	2110	1000
1550	xpro_ns202108190...	port1	1	2021-08-19 09:46:34	237	263222	2110	161044	1818	1000
1547	xpro_ns202108181...	port0	0	2021-08-18 18:03:24	237	204676	1818	212582	2110	1000
1548	xpro_ns202108181...	port1	1	2021-08-18 18:03:24	237	263222	2110	161044	1818	1000
839	xpro_ns202107151...	port0	0	2021-07-15 16:42:31	237	204676	1818	212582	2110	1000
840	xpro_ns202107151...	port1	1	2021-07-15 16:42:31	237	263222	2110	161044	1818	1000
837	xpro_ns202107151...	port0	0	2021-07-15 16:39:19	237	204676	1818	212582	2110	1000
838	xpro_ns202107151...	port1	1	2021-07-15 16:39:19	237	263222	2110	161044	1818	1000
835	xpro_ns202107151...	port0	0	2021-07-15 16:36:07	237	230476	2118	286982	3310	1000
836	xpro_ns202107151...	port1	1	2021-07-15 16:36:07	237	366422	3310	179644	2118	1000
833	xpro_ns202107151...	port0	0	2021-07-15 16:32:19	237	230476	2118	286982	3310	1000
834	xpro_ns202107151...	port1	1	2021-07-15 16:32:19	237	366422	3310	179644	2118	1000

3.11.2 测试用例报表

测试用例报表功能用来从测试用例维度统计测试信息，包括该测试用例的执行状态、运行时长、打开会话\关闭会话数，测试用例中各网口的接收字节数，接收报文数，发送字节数，发送报文数，可拖拉滚动条查看全部信息。

ID	订单编号	网卡名	网卡ID	测试用例ID	创建时间	工程ID	动作名称	网络	子网	动作/profile
1650	xpro_ns202108190...	port0	0	1783	2021-08-19 09:46:34	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
1651	xpro_ns202108190...	port1	1	1783	2021-08-19 09:46:34	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
1648	xpro_ns202108181...	port0	0	1783	2021-08-18 18:03:24	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
1649	xpro_ns202108181...	port1	1	1783	2021-08-18 18:03:24	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
967	xpro_ns202107151...	port0	0	1783	2021-07-15 16:42:31	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
968	xpro_ns202107151...	port1	1	1783	2021-07-15 16:42:31	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
965	xpro_ns202107151...	port0	0	1782	2021-07-15 16:39:19	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
966	xpro_ns202107151...	port1	1	1782	2021-07-15 16:39:19	237	RAW_TCP_分片数...	raw_tcp	ipv6	RAW_TCP_u5206u...
963	xpro_ns202107151...	port0	0	1781	2021-07-15 16:36:07	237	RAW_TCP_分片大...	raw_tcp	ipv6	RAW_TCP_u5206u...
964	xpro_ns202107151...	port1	1	1781	2021-07-15 16:36:07	237	RAW_TCP_分片大...	raw_tcp	ipv6	RAW_TCP_u5206u...
961	xpro_ns202107151...	port0	0	1780	2021-07-15 16:32:19	237	RAW_TCP_分片大...	raw_tcp	ipv6	RAW_TCP_u5206u...
962	xpro_ns202107151...	port1	1	1780	2021-07-15 16:32:19	237	RAW_TCP_分片大...	raw_tcp	ipv6	RAW_TCP_u5206u...

3.11.3 URL 统计报表

URL 统计报表功能统计 订单创建时间，view.idx、网络、子网、动作/profile、请求、响应、view.host、view.path 等信息，可拖拉滚动条查看全部信息。

ID	订单编号	测试用例ID	子网	动作/profile	请求	响应	view host	view.p
10	xpro_ns202104261...	640	ipv4	http	10	10	0	/index

3.11.4 应用统计报表

应用统计报表统计应用协议及收发包字节数，会话数等。

ID	订单编号	测试用例ID	工程ID	网络	子网	动作/profile	接收字节
419737	xpro_ns202104261...	640	29:10:183	http	ipv4	http	738
419738	xpro_ns202104261...	640	29:10:183	http	ipv4	http	738
419739	xpro_ns202104261...	640	29:10:183	http	ipv4	http	738
419740	xpro_ns202104261...	640	29:10:183	http	ipv4	http	738
419741	xpro_ns202104261...	640	29:10:183	http	ipv4	http	738
419742	xpro_ns202104261...	640	29:10:183	http	ipv4	http	0
419743	xpro_ns202104261...	640	29:10:183	http	ipv4	http	0
419744	xpro_ns202104261...	640	29:10:183	http	ipv4	http	0
419745	xpro_ns202104261...	640	29:10:183	http	ipv4	http	0

版权所有：北京触点互动信息技术有限公司 京ICP备19037780号

订单号运行

3.11.5 RTCP 报表

RTCP 报表统计 RTSP 相关执行状态、运行时间、接收字节、接收报文、发送字节、发送报文信息

订单编号	工程ID	网卡ID	测试用例ID	创建时间	网卡名	类型	预期执行时间	执行状态
xpro_ns202104161...	62	1	0	2021-04-16 15:38:16	port1	TCP SRV	1	PASS
xpro_ns202104161...	62	0	0	2021-04-16 15:38:16	port0	TCP CL	40	PASS
xpro_ns202104161...	62	1	0	2021-04-16 15:34:13	port1	TCP SRV	1	PASS
xpro_ns202104161...	62	0	0	2021-04-16 15:34:13	port0	TCP CL	40	PASS
xpro_ns202104161...	62	1	0	2021-04-16 15:30:34	port1	TCP SRV	1	PASS
xpro_ns202104161...	62	0	0	2021-04-16 15:30:34	port0	TCP CL	40	PASS
xpro_ns202104161...	62	1	0	2021-04-16 15:27:43	port1	TCP SRV	1	PASS
xpro_ns202104161...	62	0	0	2021-04-16 15:27:43	port0	TCP CL	40	PASS
xpro_ns202104161...	62	1	0	2021-04-16 15:23:06	port1	TCP SRV	1	PASS

版权所有：北京触点互动信息技术有限公司 京ICP备19037780号

订单号运行

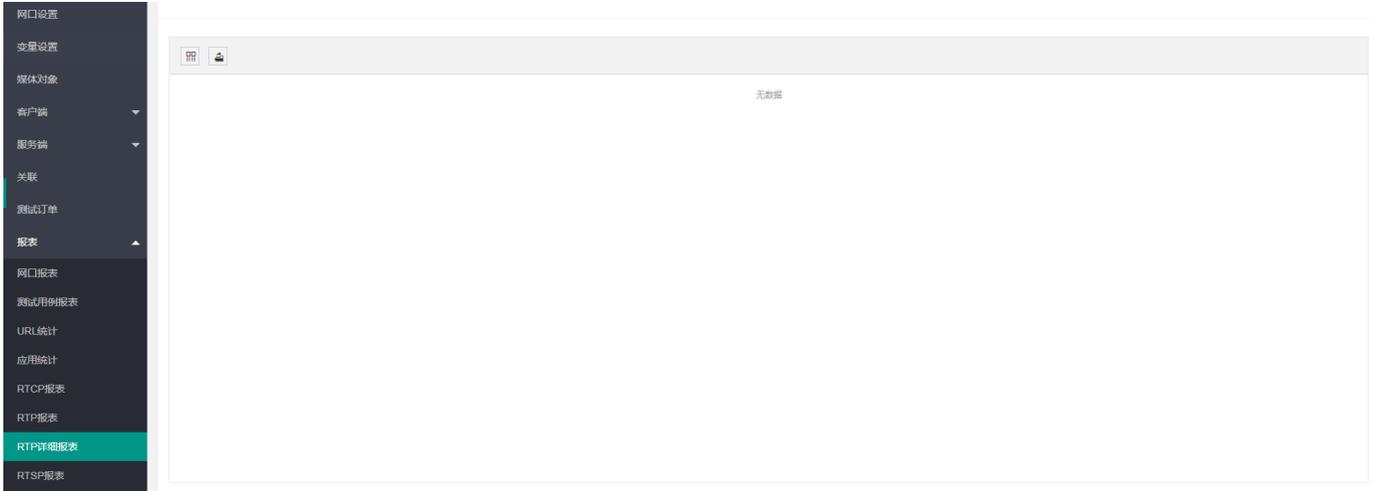
3.11.6 RTP 报表

RTP 统计报表功能是用来统计 RTSP 协议中 RTP 流信息，统计信息有类型、运行时间、接收字节、接收报文、发送字节、发送报文、视频播放质量

订单编号	工程ID	网卡ID	测试用例ID	创建时间	网卡名	类型	预期执行时间	执行状态	运行时间	接收字节
xpro_ns202106291...	261	0	0	2021-06-29 11:02:05	port0	TCP CL	32	PASSED	45.98	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:02:03	port0	TCP CL	32	RUNNING	45.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:02:03	port0	TCP CL	32	RUNNING	44.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:02:01	port0	TCP CL	32	RUNNING	43.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:02:01	port0	TCP CL	32	RUNNING	42.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:59	port0	TCP CL	32	RUNNING	41.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:59	port0	TCP CL	32	RUNNING	40.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:57	port0	TCP CL	32	RUNNING	39.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:57	port0	TCP CL	32	RUNNING	38.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:56	port0	TCP CL	32	RUNNING	37.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:55	port0	TCP CL	32	RUNNING	36.00	6906600
xpro_ns202106291...	261	0	0	2021-06-29 11:01:53	port0	TCP CL	32	RUNNING	35.00	6906600

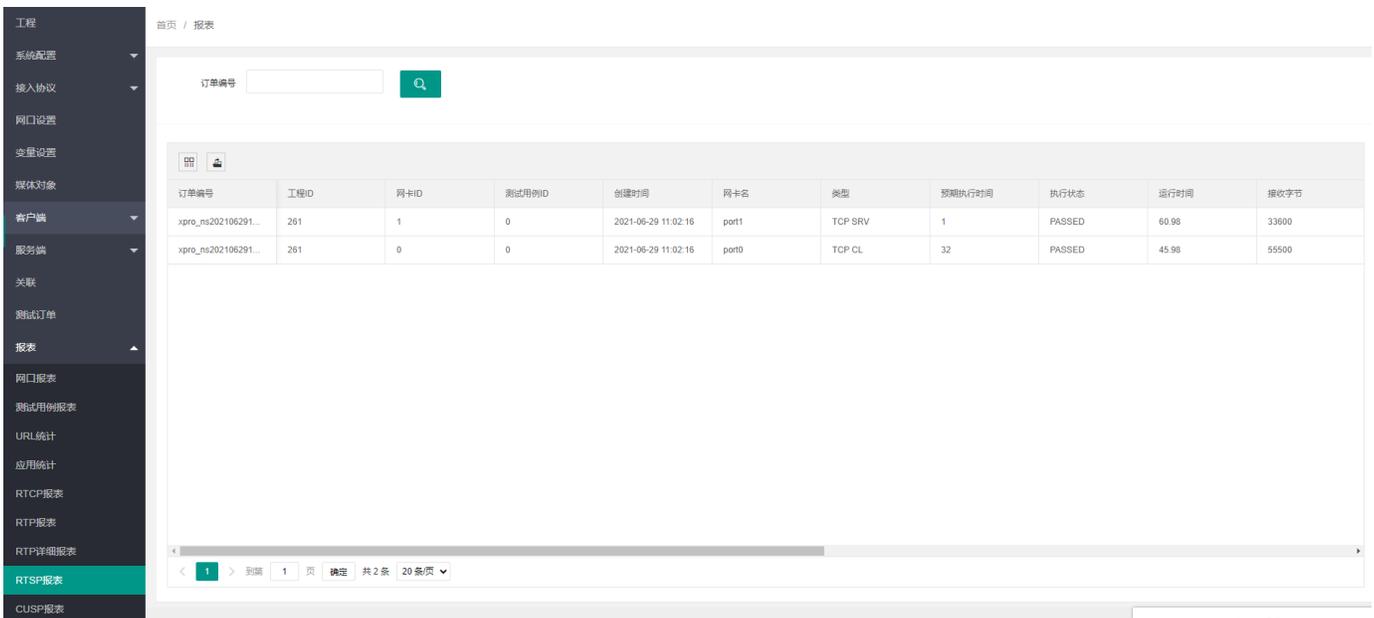
3.11.7 RTP 详细报表

RTP 详细报表是用来统计 RTSP 协议中传输 RTP 流相关信息



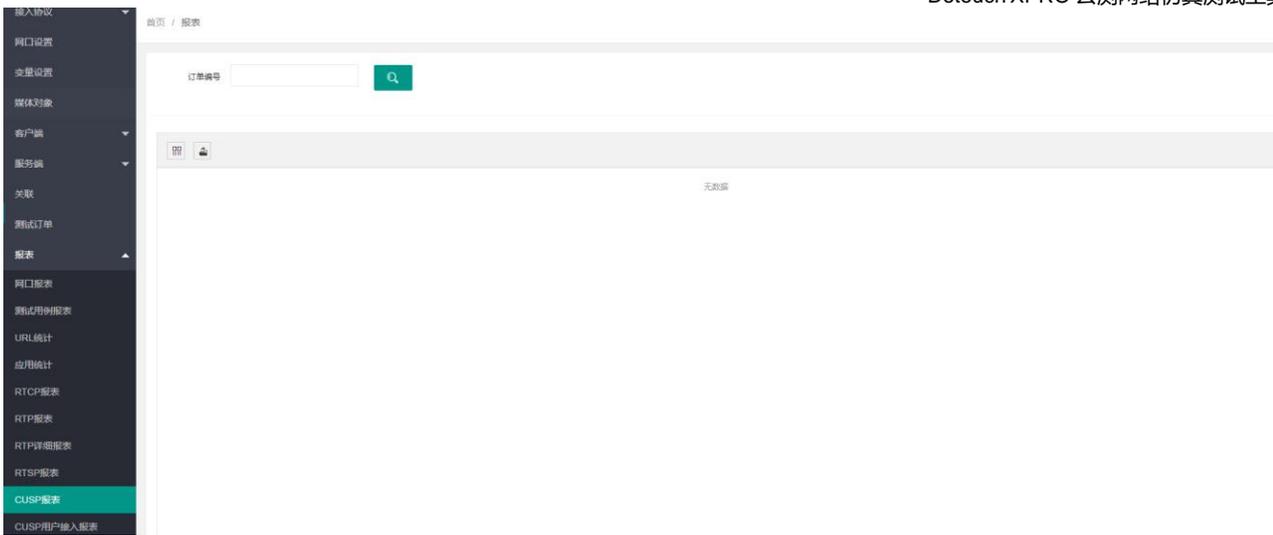
3.11.8 RTSP 报表

RTSP 报表统计 RTSP 协议中网卡接收数据，包含类型、预期执行时间、执行状态、运行时间、接收字节、发送字节、请求数、响应数等信息



3.11.9 CUSP 报表

Cusp 报表统计 CUSP 协议订单中网卡收发字节数，请求和响应的数量及状态等信息。



3.11.10 CUSP 用户接入报表

CUSP 用户接入报表统计 UP 控制口 IP、用户接入口 ID、用户接入协议类型，用户上下线数量，及用户在线数量等信息。

订单编号	控制口 IP	用户上线次数	用户建立连接次数	用户下线次数	用户在线数	成功获取ipv4数	成功获取ipv6数	接收IAP数
xpro_ns202104261...	3000	1000	100	100	100	1000	10000	10000
xpro_ns202104261...	3000	1000	100	100	100	1000	10000	10000
xpro_ns202104261...	3000	1000	100	100	100	1000	10000	10000
xpro_ns202104261...	3000	1000	100	100	100	1000	10000	10000

Page 1 of 1, 1 page, Confirm, Total 4 rows, 20 rows/page

版权所有：北京触点互动信息技术有限公司 京ICP备19037780号 订单未运行

3.11.11 用户接入报表

用户接入报表统计 PPPoE 和 DHCP 协议中 用户接入协议类型、用户上线次数、用户建立连接次数、用户下线次数、用户在线数 及 PPPoE 和 DHCP 会话数量 和状态统计。

订单编号	测试用例ID	创建时间	网卡名	用户接入协议类型	用户上线次数	用户建立连接次数	用户下线次数
xpro_ns202103241...	1	2021-03-24 17:16:47	port0	PPPOEv4	110	110	0
xpro_ns202103241...	1	2021-03-24 11:20:06	port0	PPPOEv4	110	110	0
xpro_ns202103241...	1	2021-03-24 10:59:03	port0	PPPOEv4	0	0	0
xpro_ns202103241...	0	2021-03-24 10:46:27	port0	PPPOEv4	110	110	0
xpro_ns202103241...	0	2021-03-24 10:42:36	port0	PPPOEv4	110	110	0

Page 1 of 1, 1 page, Confirm, Total 5 rows, 20 rows/page

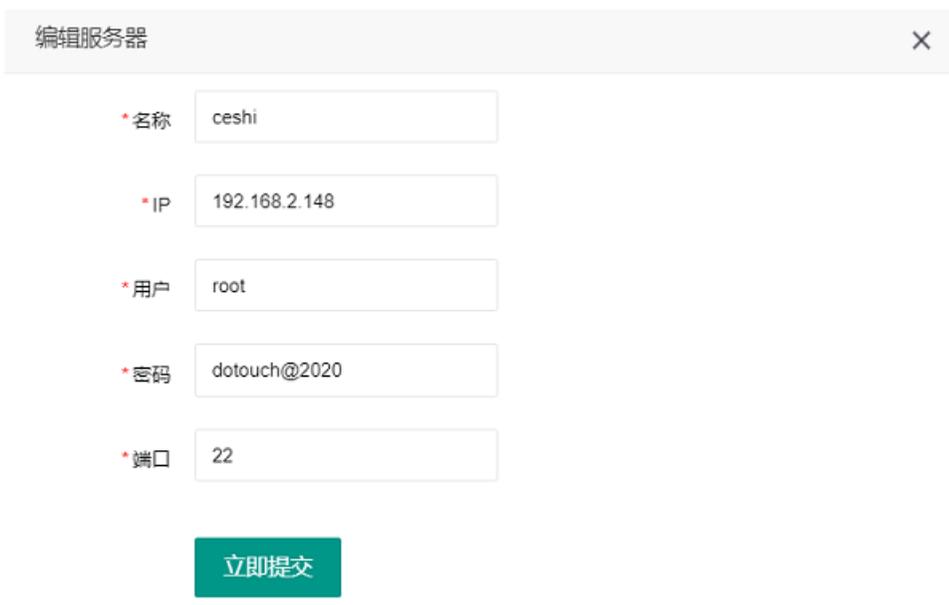
版权所有：北京触点互动信息技术有限公司 京ICP备19037780号 订单未运行

3.12 终端

终端功能是模拟 ssh 登陆仪表服务器后台执行一些查询或者启动关闭服务的操作，便于在电脑未安装 ssh 工具的情况下对仪表进行维护和检查

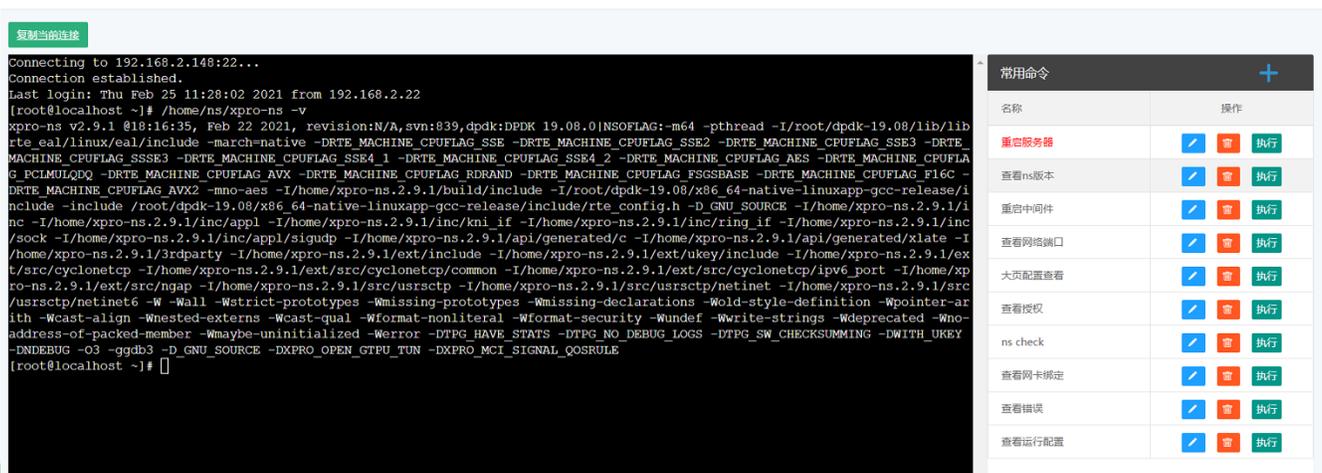


点击编辑按钮，输入对应服务器 ssh 连接的相关信息，点击连接即可远程连接到服务器后台



右边列表列举了一些常用命令，点击命令后面的执行按钮，即可执行当前操作，操作支持添加、编辑、删除和执行操作，维护人员可根据自己使用情况进行添加维护

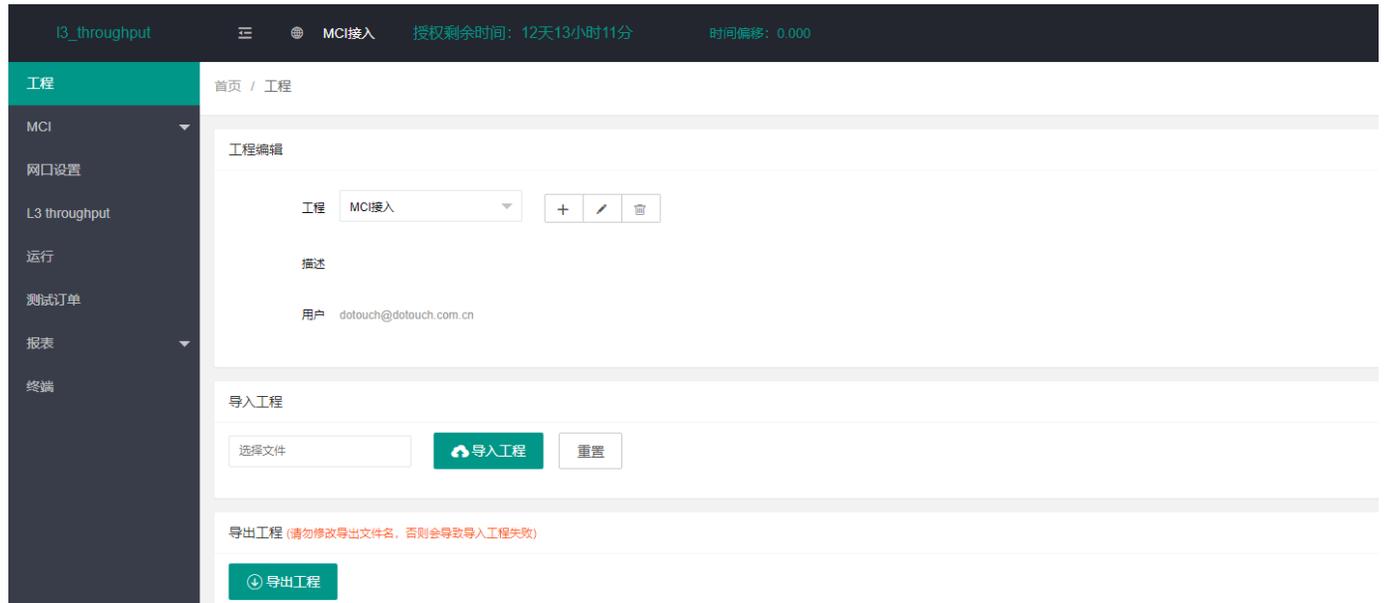
终端 - 192.168.2.148



第4章 L3 Throughput 配置指南

4.1 工程

配置参考 3.1



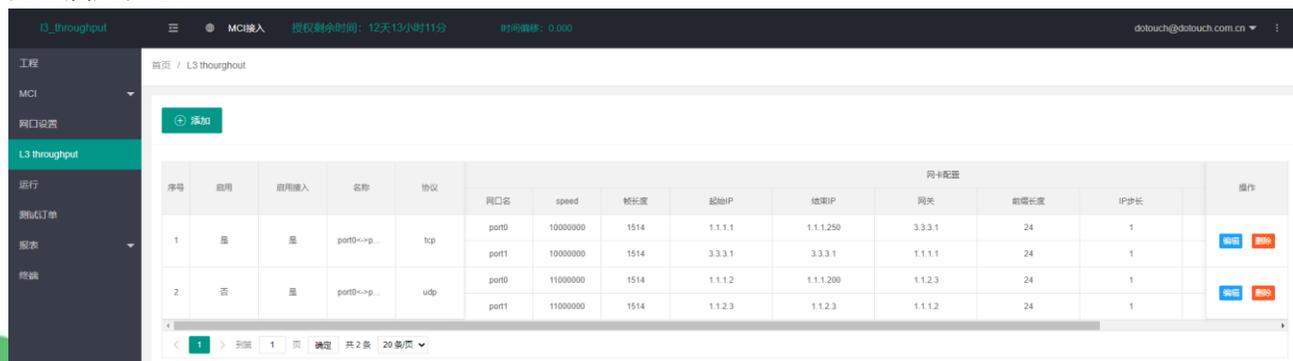
4.2 网口设置

配置参考 3.4



4.3 L3 Throughput

L3 吞吐测试设置页面。点击  添加 按钮，进入配置页面，可以增加多个配置项，但是只能有一个配置项处于启用状态。



L3 throughput set

启用

启用接入模式

* 协议

port_1 port_2

* 网卡

* speed kbps

* 帧长度 Byte

IP

* IP段 ~

* 前缀长度

* 网关

* 步长

sport

* 起始端口

* 结束端口

* 步长

启用： 是否启用该配置项开关。

启用接入模式： 是否启用接入。

协议： 选择三层承载协议，支持 TCP 和 UDP。

网卡： 选择测试时使用的网卡。

Speed： 设置发包速率

帧长度： 设置数据帧的长度

IP 段： 测试时使用的 IP 地址段

前缀长度： 配置该网口 IP 地址的前缀

网关： 配置该网口的下一跳 IP 地址

 port1 设置的网关需要在 port2 设置的 IP 段里。port2 设置的网关需要在 port1 设置的 IP 段里。

步长： IP 端递增步长

起始端口： 配置测试时使用端口起始值

结束端口： 配置测试时使用端口结束值

步长： 端口递增步长

 Port2 设置页面和 port1 一样。网卡需要选择不同的网卡。

4.4 运行

运行页面可以开始运行订单和停止订单运行。

点击  按钮，可以启动订单执行。



运行时长: 订单运行时长，单位秒

系统时间: 显示当前系统时间

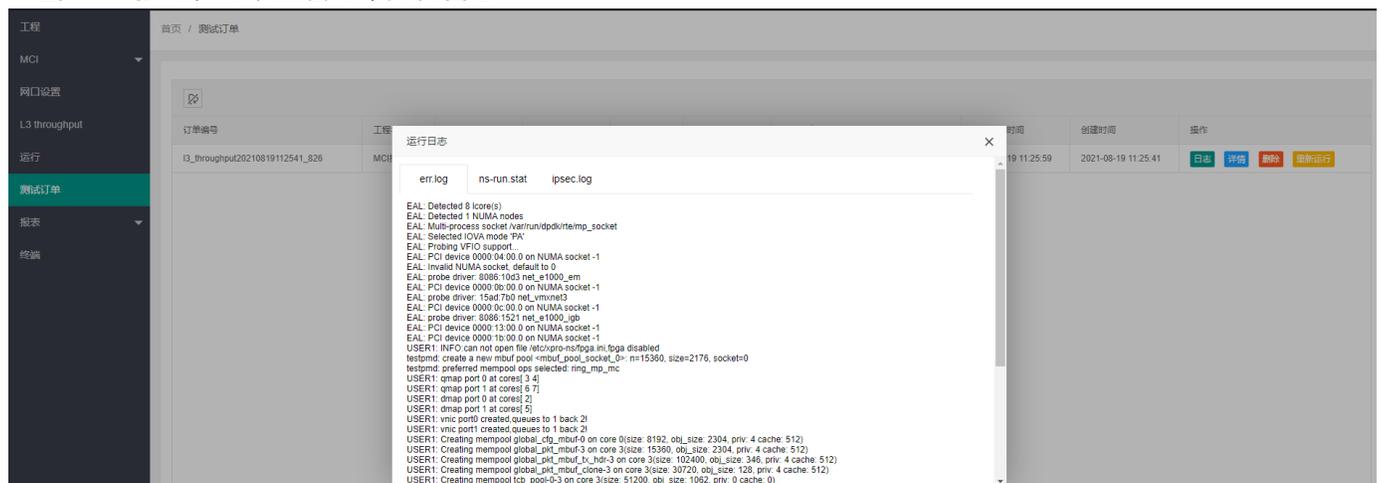
启动时间: 配置订单开始运行时间(距离当前时间需要大于 4 分钟)。

4.5 订单列表

订单列表页面，可以查看订单当前运行阶段，当前运行状态，运行开始时间，运行时长等。



点击  按钮，可以查看订单执行日志



点击 [详情](#) 按钮，可以查看订单运行监控，流速，包速等负载图表。

工程

MCI

网口设置

L3 throughput

运行

测试订单

报表

终端

首页 / 测试订单管理 / 监控

监控
负载

1234567

订单运行结束

Global	
start_time	2021-08-19 11:26:16
cur_time	2021-08-19 11:28:18
stop_time	2021-08-19 11:28:18
max_core_usage	0%
port0-dump	write fail 0 other fail 0
port1-dump	write fail 0 other fail 0

Test Stages	
port0	
port_pair	port0->port1
latency_min	2282ns
latency_avg	20138ns
latency_max	15669634ns
trans_fail	0
arp_rpkts	2
arp_rbytes	120
rx-pps	0
rx-bps	0
tx-pps	0
tx-bps	0
rx-pkts	97,868
rx-bytes	150,122,070
tx-pkts	98,349
tx-bytes	150,864,466
rx_err	0
rx_miss	0
rx_nobuf	0



4.6 报表

报表模块用来查看各测试订单的汇总统计报表，L3 Throughput 子系统当前支持 2 种类型的报表

网口报表：参考 3.11.1

ID	订单编号	网卡名	网卡ID	创建时间	工程ID	接收字节	接收报文	发送字节	发送报文	网卡速度
1561	I3_throughput20210...	port0	0	2021-08-19 11:28:17	217	150122070	97868	148504090	98349	1000
1562	I3_throughput20210...	port1	1	2021-08-19 11:28:17	217	150884466	98349	147777780	97868	1000

测试用例报表：参考 3.11.2

ID	订单编号	网卡名	网卡ID	测试用例ID	创建时间	工程ID	动作名称	类型	执行状态	运行时间
1661	I3_throughput20210...	port0	0		2021-08-19 11:28:17	217		RX_TX_PORT	PASSED	122.67
1662	I3_throughput20210...	port1	1		2021-08-19 11:28:17	217		RX_TX_PORT	PASSED	122.08

4.7 终端

参考 3.12

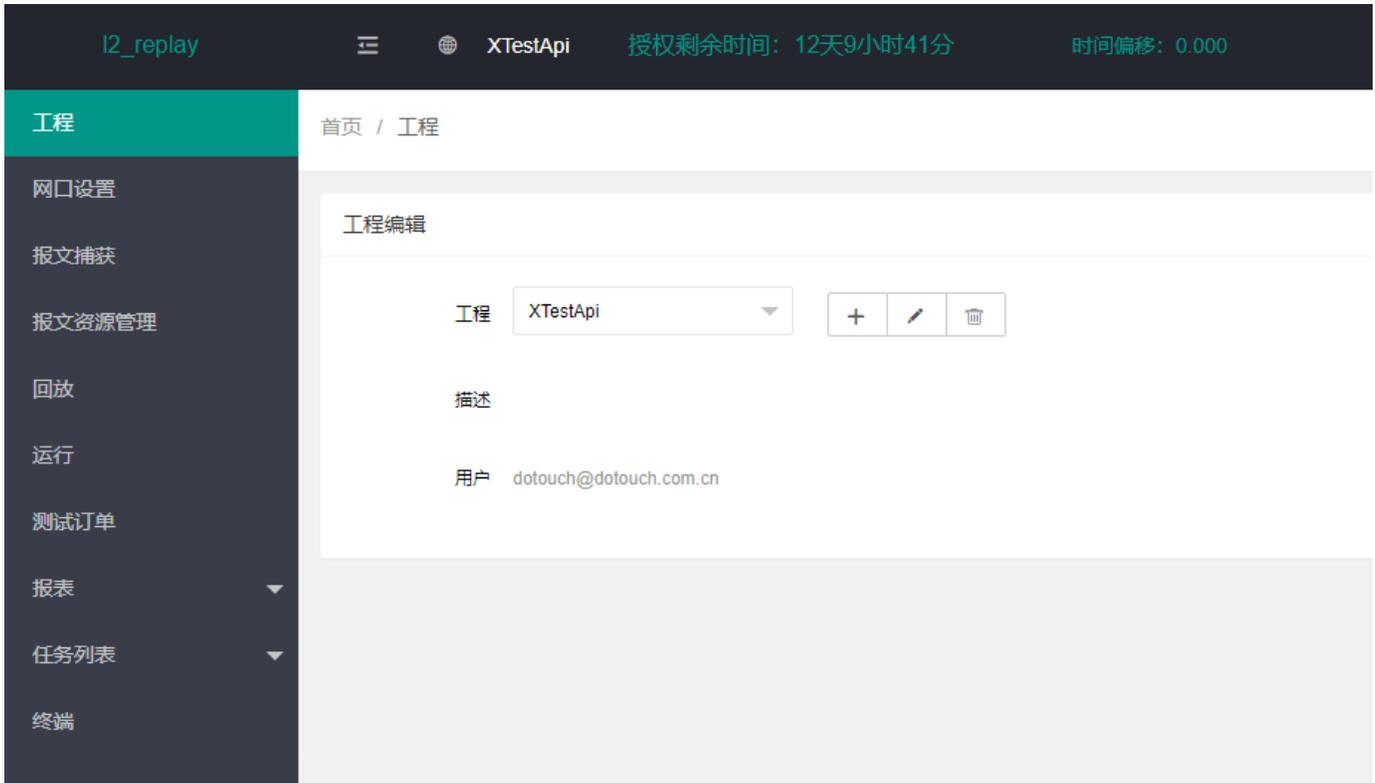
名称	IP	操作
虚拟机	192.168.2.142	✓ ✗ 连接

< 1 > 到第 1 页 确定 共 1 条 20 条页

第5章 L2 replay 配置指南

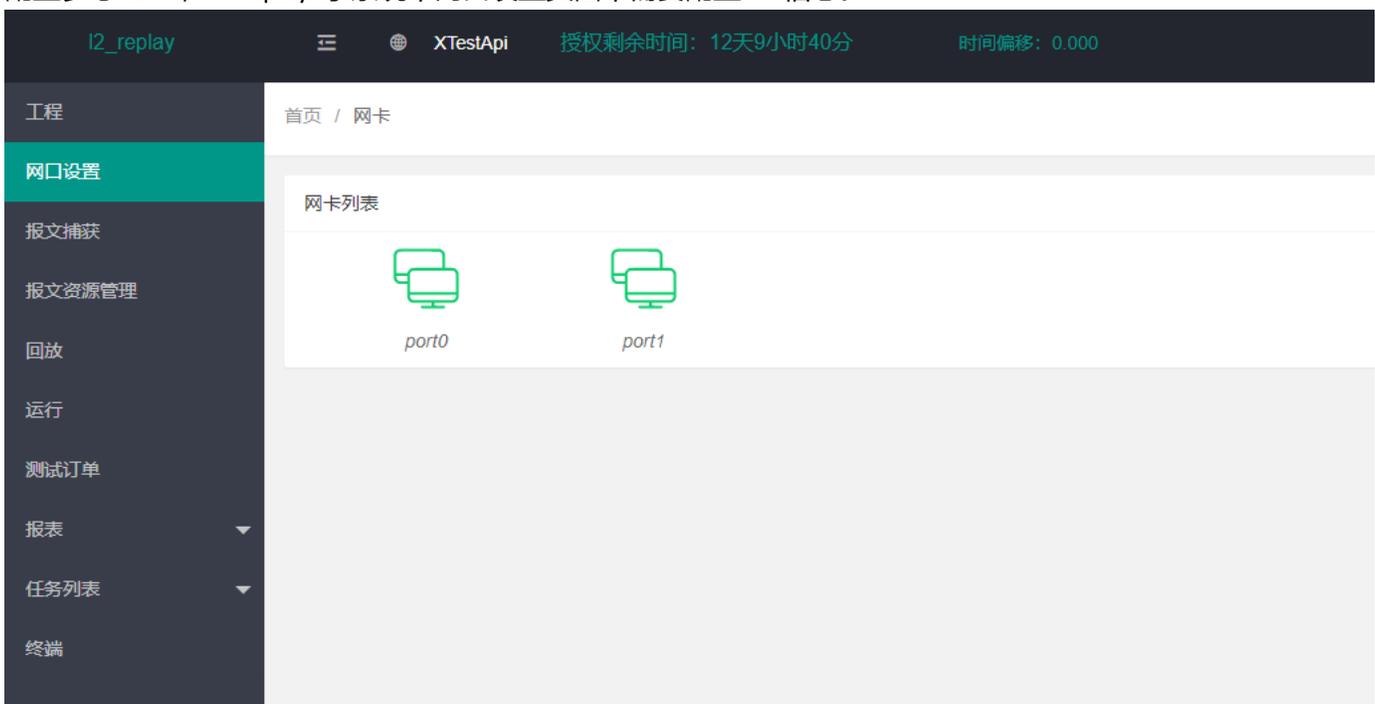
5.1 工程

配置参考 3.1



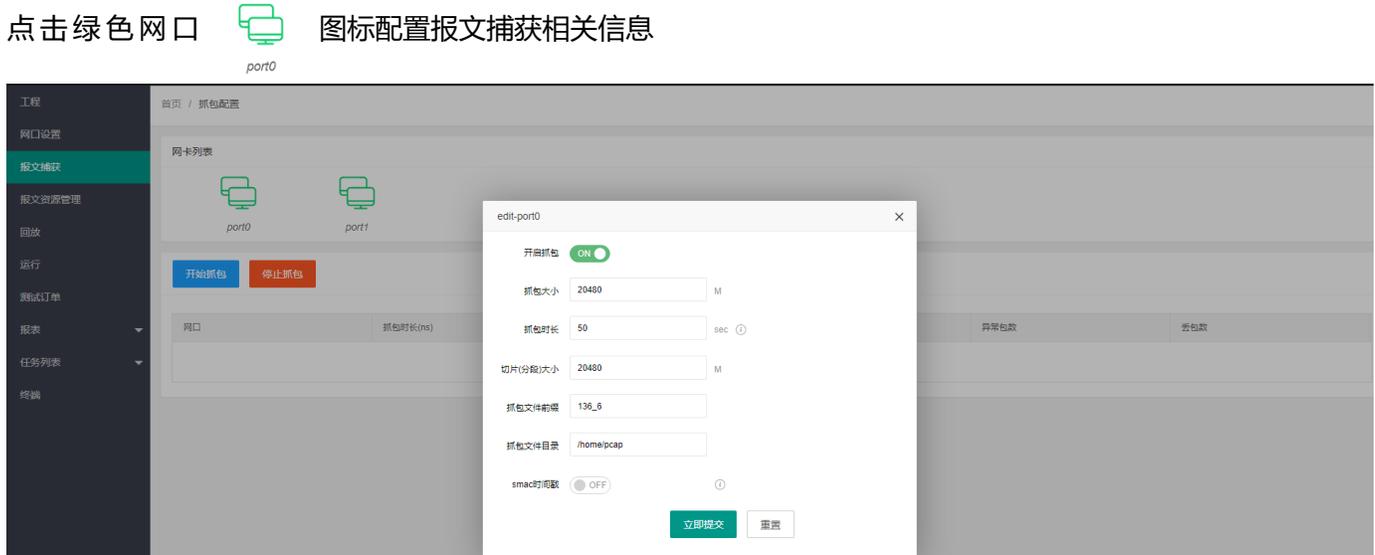
5.2 网口设置

配置参考 3.4 , L2 replay 子系统中网口设置页面不需要配置 IP 信息。



5.3 报文捕获

点击绿色网口图标配置报文捕获相关信息



开启抓包：是否在该网口开启抓包功能

抓包大小：配置需要捕获报文大小（单位 M）

抓包时长：配置需要抓取报文时长（单位 s），和抓包大小同时配置，达到二者其一则停止捕获。

切片/分段大小：配置每个抓包文件保存的大小。默认单位 M

抓包文件前缀：定义保存的抓包文件前缀名称（每次进行报文捕获时需要修改前缀名称）

抓包文件目录：配置抓包文件存储的服务器后台目录（如果需要捕获大量报文，建议目录配置在较大的磁盘空间中）

Smac 时间戳：配置是否开启高精度时间戳

开始抓包：在该网口上启用抓包订单（详细信息可在测试订单中查看）

5.4 报文资源管理

对网口捕获和手动导入的报文进行分析，以列表和图标的形式展示分析结果

样包名称	样包路径	报文序号	起始时间(ms)	持续时长(ms)	包总数	包大小(bytes)	有无索引	类型	备注	分析	操作
prefix_0.p...	/home/dump/prefix_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
136_6_0.p...	/home/pcap/136_6_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
136_4_0.p...	/home/pcap/136_4_0.pcapng	0	2021-08-03 14:24:11.339239...	200039372835	11087678	2147483647	有	网口抓包		分析	删除 备注 分析结果
136_1_0.p...	/home/pcap/136_1_0.pcapng	0	2021-08-03 13:59:22.619902...	200019633281	2220195	1842756824	有	网口抓包		分析	删除 备注 分析结果
1_4_0.pca...	/home/1_4_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
2_3_0.pca...	/home/2_3_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
1_3_0.pca...	/home/1_3_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
2_2_0.pca...	/home/2_2_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
1_2_0.pca...	/home/1_2_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果
2_1_0.pca...	/home/2_1_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除 备注 分析结果

绝对路径：填写服务器后台目录（点击导入按钮，会将该目录下以 pcap 和 pcapng 结尾的报文导入到系统，手动导入的包文件需要点击操作栏下的分析按钮进行分析）

删除：手动删除当前报文分析结果

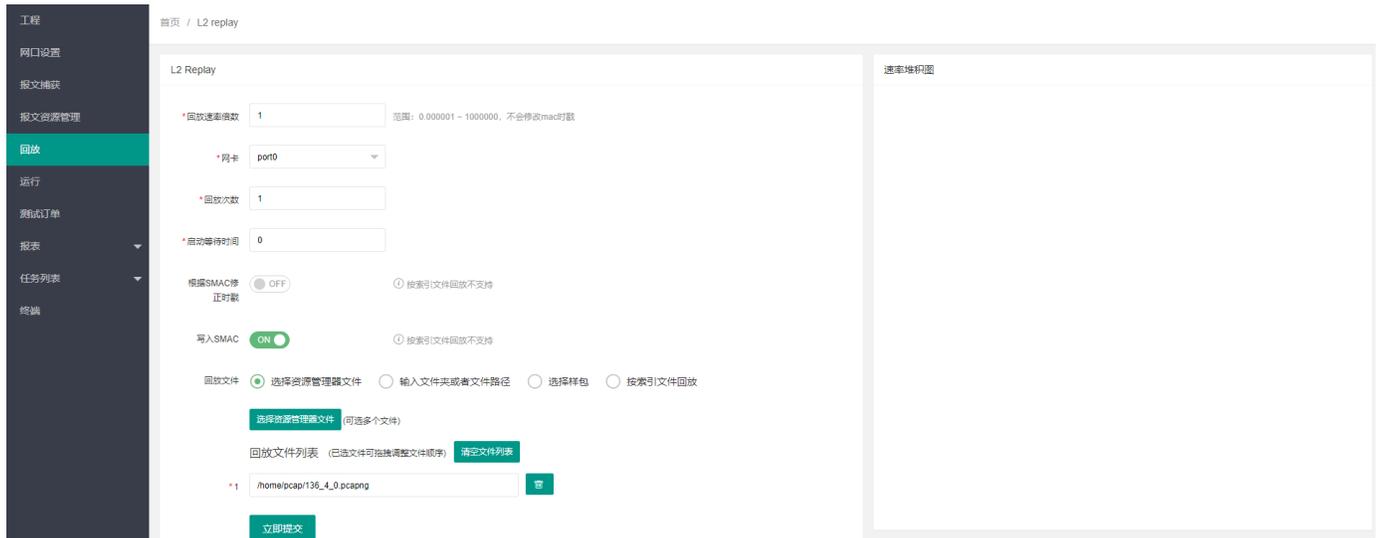
备注：可以对报文进行备注。

分析结果：查看当前抓包文件的 speed 曲线统计

5.5 回放

报文快速回放功能，可设置回放倍速和回放次数。回放任务在保存配置后在测试订单任务栏中点击进行新增回放任务

新增回放任务



回放速率倍速：测试时的发包速率对比源文件的播放速率，如 2 就是代表以 2 倍的速度发包

网卡：选择需要进行回放的网卡

回放次数：配置需要对原包进行多少次的回放

启动等待时间：配置多长时间后进行回放报文，默认单位：秒

根据 SMAC 修正时戳：开启此项，回放时读取 SMAC，根据 SMAC 的值校正 PCAP 报文得到的时间戳，不开启此开关，直接将 PCAP 报文得到的时间戳作为回放相关的时间戳使用。

写入 SMAC：SMAC 开关，开启时，回放时将时间戳信息写入 SMAC，关闭时，不修改 SMAC

回放文件：支持“选择资源管理器”、“输入文件夹或者文件路径”、“选择样包”，“按索引回放”进行回放。

清空文件列表：将当前选择的回放文件清空，进行重新选择

立即提交：将上述配置进行提交保存

 只有“选择样包”选项会有速率堆积图

5.6 运行

启动回放订单运行。

系统时间：显示当前系统时间

启动时间：配置订单开始运行时间(距离当前时间需要大于 4 分钟)。

点击  即可运行回放订单。

工程

网口设置

报文捕获

报文资源管理

回放

运行

测试订单

报表

任务列表

终端

首页 / 运行

运行参数

系统时间 2021-08-19 14:39:45

启动时间 ⓘ

▶ 开始运行

5.7 测试订单

对当前以及历史订单信息进行统计和展示，可进行日志查看、详情查看 和 删除订单信息，重新运行等操作

工程

网口设置

报文捕获

报文资源管理

回放

运行

测试订单

报表

任务列表

终端

首页 / 测试订单管理 / 测试订单

订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
l2_replay20210811143316_802	XTestApi		工单运行结束	UI创建	成功		2021-08-11 14:33:29	2021-08-11 14:33:16	日志 详情 删除 重新运行
20210806181626_781	XTestApi		工单运行结束	接口下单	用户主动发起...		2021-08-06 18:16:39	2021-08-06 18:16:26	日志 详情 删除
20210806181321_780	XTestApi		工单运行结束	接口下单	成功		2021-08-06 18:13:33	2021-08-06 18:13:21	日志 详情 删除
20210806161713_779	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-06 16:17:26	2021-08-06 16:17:13	日志 详情 删除
20210804162544_713	XTestApi	网口抓包	工单运行结束	UI创建	用户主动发起...		2021-08-04 16:25:55	2021-08-04 16:25:44	日志 详情 删除
20210803142354_700	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-03 14:24:10	2021-08-03 14:23:54	日志 详情 删除
20210803141625_699	XTestApi	网口抓包	工单运行结束	UI创建	用户主动发起...		2021-08-03 14:16:40	2021-08-03 14:16:25	日志 详情 删除
20210803140629_698	XTestApi	网口抓包	工单运行结束	UI创建	失败	USER1: ERROR write file /home/pcap1...	2021-08-03 14:06:43	2021-08-03 14:06:29	日志 详情 删除
20210803135908_697	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-03 13:59:21	2021-08-03 13:59:08	日志 详情 删除
20210723140819_846	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-07-23 14:08:43	2021-07-23 14:08:19	日志 详情 删除
20210723135103_645	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-07-23 13:51:27	2021-07-23 13:51:03	日志 详情 删除

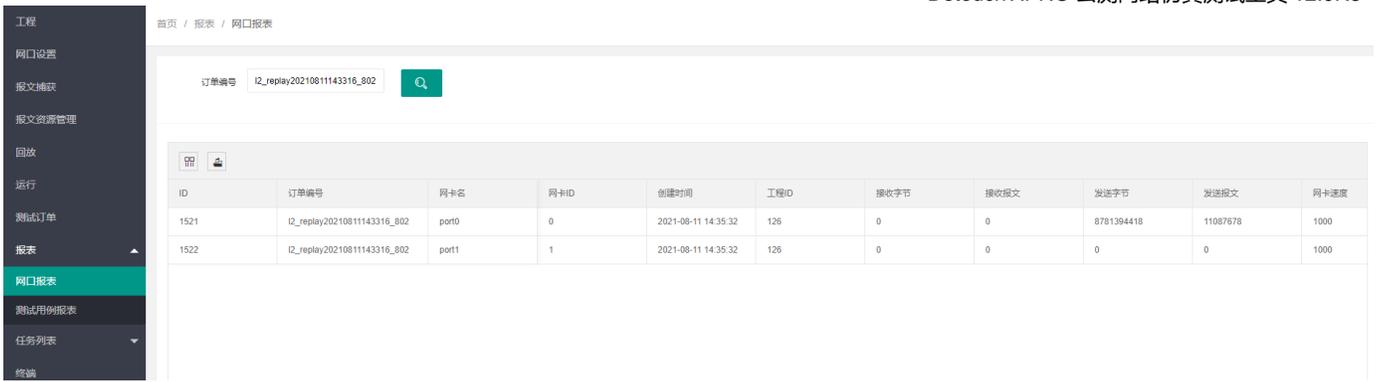


只有通过 UI 创建的 回放订单支持 重新运行。

5.8 报表

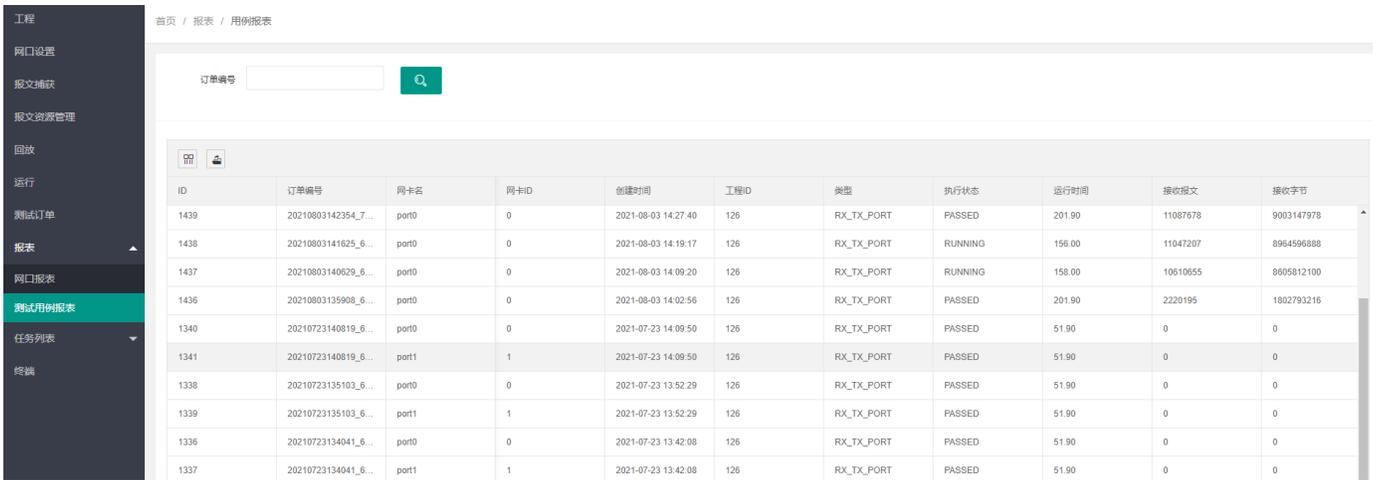
5.8.1网口报表

网口报表功能用来从网口维度统计测试信息，包括网口的接收字节数，网口的接收报文数，网口的发送字节数，网口的发送报文数，网口的工作速率等，可拖拉滚动条查看从网口维度统计的全部信息。



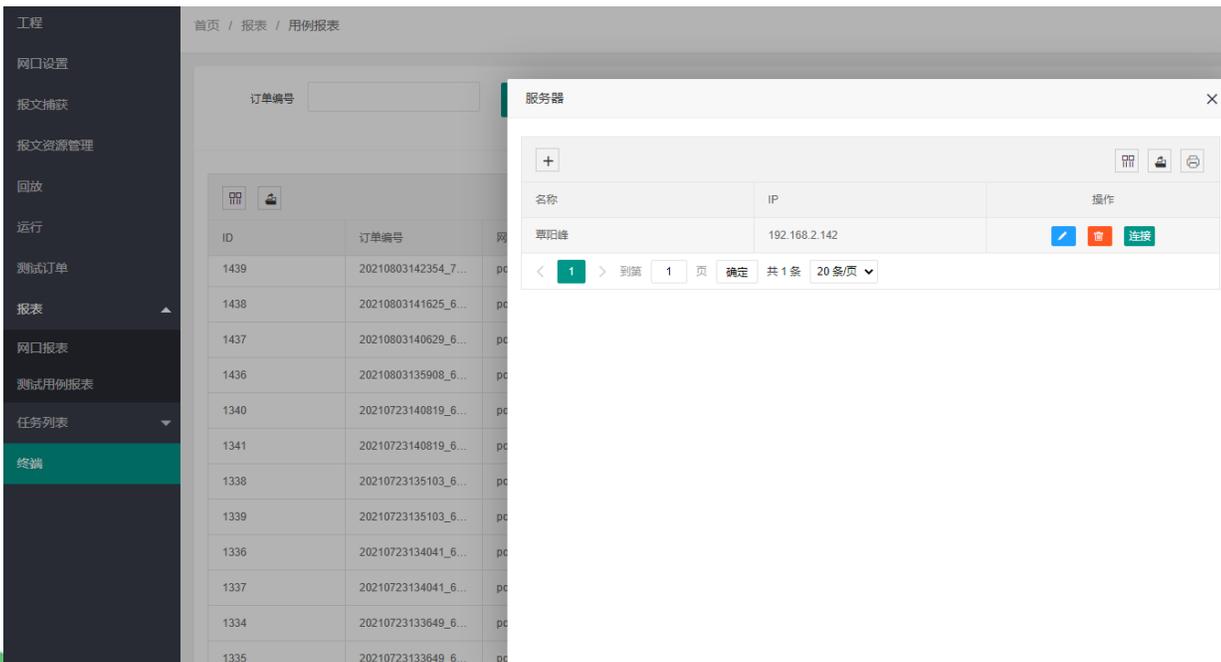
5.8.2 测试用例报表

测试用例报表功能用来从测试用例维度统计测试信息，包括该测试用例的执行状态、运行时长、打开会话\关闭会话数，测试用例中各网口的接收字节数，接收报文数，发送字节数，发送报文数，可拖拉滚动条查看全部信息。



5.9 终端

参考 3.12 终端



第6章 Attack 配置指南

L3 replay 子系统在使用上与 xpro_ns 子系统基本一致，在测试模式上采用双臂模式，只是在动作协议支持上增加了 l3 replay、ddos 和 attack play 类型，背景流与 xpro_ns 一致。此部分只介绍与 xpro_ns 子系统增加的 3 中协议部分。

6.1 工程

配置参考 3.1

6.2 系统配置

配置参考 3.2

6.3 接入配置

配置参考 3.3

6.4 网口配置

配置参考 3.4

6.5 变量设置

配置参考 3.5

6.6 媒体对象

配置参考 3.6

6.7 客户端

6.7.1 客户端子网配置

配置参考 3.7.1

6.7.2 客户端网络配置

配置参考 3.7.2

6.7.3 客户端负载配置

配置参考 3.7.3

6.7.4 客户端动作配置

a) ATTACK_PLAY 配置方法

attack_play 将系统集成进来的攻击库文件按照一定的配置规则进行仿真攻击，可用来检测被测设备的安全性。

✓ ✘	attack play	ATTACK_PLAY	系统攻击流
ATTACK_PLAY Parameters 分片			
*启用ip轮换:	<input type="checkbox"/>		
*类型:	播放次数 ▾		
等待时间(s):	0		
*播放次数:	1		
*播放速率(倍数):	10000		
播放间隔(ms):	5000		
启用5元组日志记录:	<input checked="" type="checkbox"/>		
启用重传:	<input checked="" type="checkbox"/>		
一级目录:	威胁对抗能力验证 ▾		
二级目录:	工业互联网 ▾		
*攻击文件列表 (已选文件可拖拽调整文件顺序)	清空文件列表		选择文件
1	远程代码执行/漏洞利用/2004-1315	🗑	
2	远程代码执行/漏洞利用/10-061	🗑	
3	域提权/漏洞利用/14-068	🗑	
4	远程代码执行/漏洞利用/09-050	🗑	

启用 ip 轮换: 是否开启 ip 轮换，不开启则所有的攻击报文只默认使用子网配置中的第一个源/目的 ip 进行仿真。

类型: 播放类型，包括按时间和按次数播放两种，配置按时间播放时设置时间后，在设置的时间里所选的攻击文件顺序轮播，时间结束时结束测试；配置按次数播放时，设置播放次数后，所选文件轮流播放该次数后结束测试。

等待时间: 配置启动等待时间

播放次数: 配置需要播放多少次报文

播放速率: 测试时的发包速率对比源文件的播放速率，如 2 就是代表以 2 倍的速度发包

播放间隔: 两次播放之间的间隔时间

启用五元组日志记录: 配置是否开启五元组日志记录

启用重传: 配置是否开启 tcp 重传

一级目录: 攻击库文件以及目录

二级目录: 攻击库文件二级目录

攻击文件列表: 显示当前选择后的攻击库文件

b) L3 replay 配置方法

L3 replay 回放功能用来回放基于用户上传的 pcap 包，将报文按照条件清洗后，仿真模块会自动构建 4 层的状态信息，修改源和目的 ip 地址进行回放。

	✓ ✕	l3_replay	L3_REPLAY	
<input type="checkbox"/>		attack_play	ATTACK_PLAY	系统攻击流

L3_REPLAY Parameters 分片

*启用ip轮换:

*类型:

等待时间(s):

*播放次数:

*播放速率(倍数):

播放间隔(ms):

启用5元组日志记录:

启用重传:

*回放文件列表 (已选文件可拖拽调整文件顺序)

1

启用 ip 轮换：每一次文件发送时使用的 ip 地址在子网配置的网段中轮换

类型：播放类型，包括按时间和按次数播放两种，配置按时间播放时设置时间后，在设置的时间里所选的攻击文件顺序轮播，时间结束时结束测试；配置按次数播放时，设置播放次数后，所选文件轮流播放该次数后结束测试。

等待时间：配置启动等待时间，开始进行测试

播放速率：测试时的发包速率对比源文件的播放速率，如 2 就是代表以 2 倍的速度发包

播放间隔：两次播放之间的间隔时间

启用五元组日志记录：配置是否开启五元组日志记录

启用重传：配置是否开启 tcp 重传

回放文件列表：在系统配置-L3 回放库管理页面导入的自定义 pcap 文件，可以选择一个，也可以选择多个

c) Ddos 配置方法

	✓ ✕	ddos-icmp-ping-flood	DDOS	
<input type="checkbox"/>		http	HTTP	
<input type="checkbox"/>		l3_replay	L3_REPLAY	
<input type="checkbox"/>		attack_play	ATTACK_PLAY	系统攻击流

DDOS Parameters

*运行时间(s):

*启动等待时间(s):

*每秒包数:

*回放样包:

运行时间：配置 ddos 攻击运行时间

启动等待时间：配置启动等待时间，开始进行测试

每秒包数：配置 ddos 每秒攻击的包数

回放样包：选择需要进行攻击的 ddos 样包（可以根据包构建器进行灵活配置对应的 ddos 攻击包构建，例如：ddos-icmp-ping-flood、ddos-tcp-syn-flood、ddos-udp-flood、ddos-udp-port-scan、arp-flood、ddos-evasive-udp）

d) Virus_attack 配置方法

<input type="checkbox"/>	+	名称	协议
<input checked="" type="checkbox"/>	✓ ✕	virus_attack	VIRUS_ATTACK
<input type="checkbox"/>	✕	http	HTTP

Common VIRUS_ATTACK Parameters 需要在服务端profiles配置好承载协议, 如: http

选择承载协议: http ⓘ

病毒文件: 清空文件列表 选择文件

URI: 文件: 🗨

URI: 文件: 🗨

选择承载协议: 病毒库承载的应用协议, 目前只支持承载 http 协议

清空文件列表: 清空当前选择的文件列表

选择文件: 选择病毒库文件

URI: URI 必须和客户端 URI, 服务端 URI 保持一致

文件: 病毒库文件 (双臂只支持一个病毒库文件, 双单臂可以配置多个病毒库文件)

6.8 关联

配置参考 3.9

6.9 测试订单

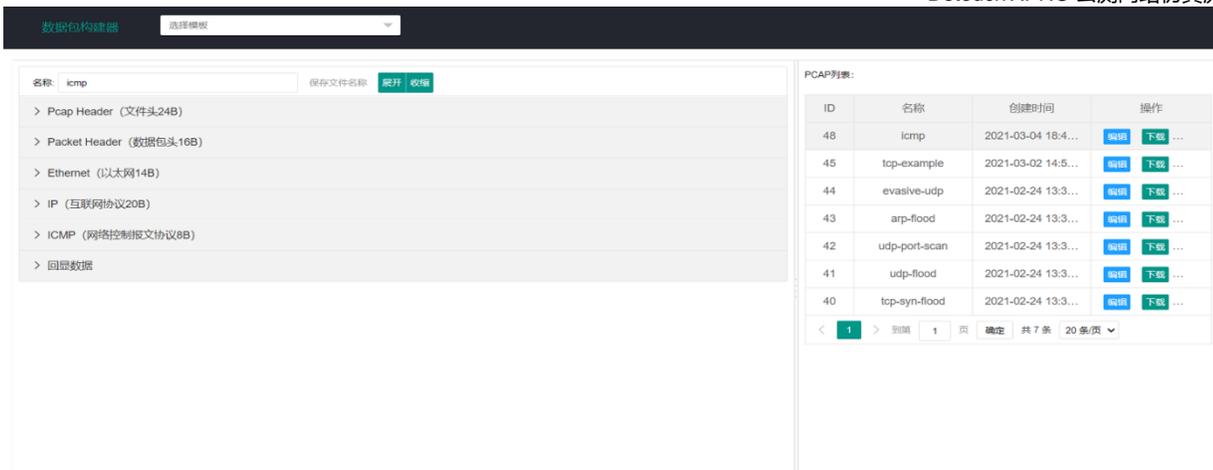
配置参考 3.10

6.10 报表

配置参考 3.11 报表

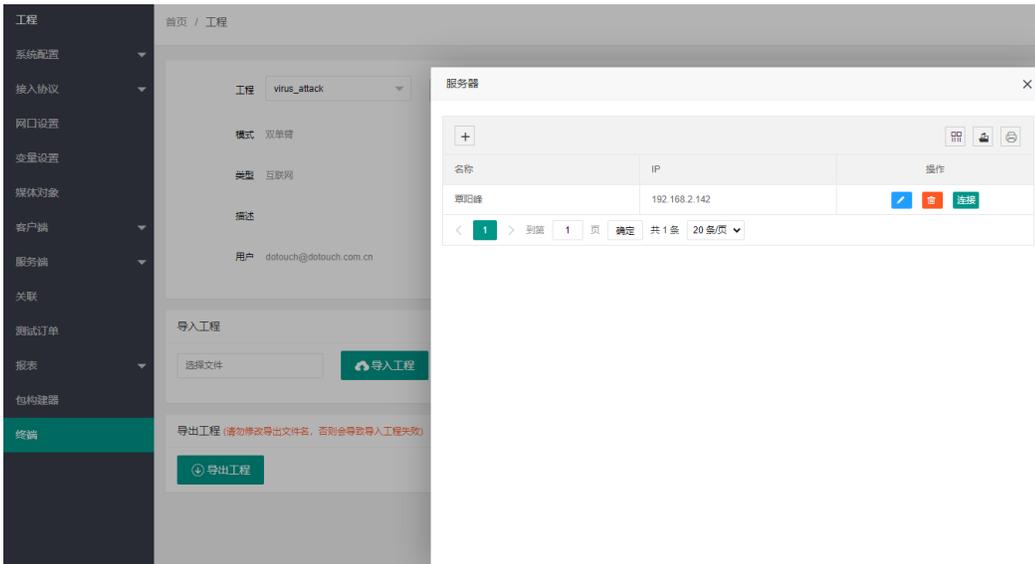
6.11 包构建器

按照规则进行数据包的构造, 构造的包用于 ddos 攻击中样包, 可按照模板中的包进行编辑保存样包。



6.12 终端

配置参考 3.12



第7章 RFC2544 配置指南

RFC2544 子系统与 xpro_ns 子系统配置基本一致，用于配置常规协议背景流，与 2544 配合使用，单独的 2544 配置在关联---RFC2544 中进行配置，且测试 2544 功能必须使用专用的 fpga 加速网卡。

7.1 工程

配置参考 3.1

7.2 系统配置

配置参考 3.2

7.3 接入配置

配置参考 3.3

7.4 网口配置

配置参考 3.4

7.5 变量设置

配置参考 3.5

7.6 媒体对象

配置参考 3.6

7.7 客户端

7.7.1客户端子网配置

配置参考 3.7.1

7.7.2客户端网络配置

配置参考 3.7.2

7.7.3客户端负载配置

配置参考 3.7.3

7.7.4客户端动作配置

配置参考 3.7.4

7.8 关联

关联配置项用来绑定最终客户端的各项配置，包括客户端关联页和 RFC2544 关联页，分别绑定前面配置的客户端各项参数。

客户端关联	RFC2544															
<div style="display: flex; justify-content: space-between;"> 批量复制 暂只支持单关联 </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;"></th> <th style="width: 10%;"></th> <th style="width: 40%;">*名称</th> <th style="width: 20%;">*测试模式</th> <th style="width: 25%;">*流量拓扑</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;">+</td> <td></td> <td></td> <td></td> </tr> <tr> <td style="text-align: center;">✓ ✕</td> <td></td> <td>rfc-2544-吞吐-ipv4-l2</td> <td>L2交换模式</td> <td>双向</td> </tr> </tbody> </table>				*名称	*测试模式	*流量拓扑	<input type="checkbox"/>	+				✓ ✕		rfc-2544-吞吐-ipv4-l2	L2交换模式	双向
		*名称	*测试模式	*流量拓扑												
<input type="checkbox"/>	+															
✓ ✕		rfc-2544-吞吐-ipv4-l2	L2交换模式	双向												
Pages: First Prev 1 2 2 of 2																
<div style="display: flex; justify-content: space-between;"> 基本配置 网口配置 吞吐量配置 </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>*运行时长(s): <input type="text" value="20"/></p> <p>*拖尾时长(s): <input type="text" value="1"/></p> <p>*使能地址学习: <input type="text" value="学习一次"/></p> <p>*选择测试项</p> <p>吞吐量测试: <input checked="" type="checkbox"/></p> <p>背景测试: <input type="checkbox"/></p> <p>时延测试: <input type="checkbox"/></p> <p>丢包率测试: <input type="checkbox"/></p> </div>																

基本配置:

运行时长: 运行时长，订单总的运行时长=测试次数*时长*帧长度的个数+运行时长

拖尾时长: 订单结束之前的拖尾时长

使能地址学习: 配置 mac 地址学习时只学习一次还是每次测试都学习

选择测试项：支持吞吐量、背靠背、时延和丢包率

基本配置	网口配置	吞吐量配置
*报文类型: <input type="text" value="ipv4"/>		
*接口地址数量: <input type="text" value="10"/>		
*网卡选择		
源接口网卡: <input type="text"/>		
目的接口网卡: <input type="text"/>		
*配置链路层		
MAC地址: <input type="text" value="00:00:42:01:01:1A"/>		
接口内跳变步长: <input type="text" value="00:00:00:00:00:01"/>		
端口间跳变步长: <input type="text" value="00:00:10:00:00:00"/>		
*配置网络层		
*IPv4地址		
IPV4地址: <input type="text" value="1.1.1.5"/>		
接口内跳变步长: <input type="text" value="0.0.0.1"/>		
端口间跳变步长: <input type="text" value="1.0.0.0"/>		
IPv4网关: <input type="text" value="1.1.1.1"/>		

网口配置：

报文类型：支持 ipv4 和 ipv6

接口地址数量：接口地址数量（目前版本最大支持 80 个地址跳变，超过 80 的部分无效）

网卡选择：选择需要进行 2544 测试的源和目的接口网卡

配置链路层：配置链路层 mac 地址规则

配置网络层：配置 ipv4 或者 ipv6 网络层地址规则

基本配置	网口配置	吞吐量配置
*测试时长		
测试次数: <input type="text" value="1"/>		
测试时长: <input type="text" value="时长(秒)"/>		
时长: <input type="text" value="10"/>		
*帧长度(字节)		
自定义: <input type="text" value="64,128,256,512,1024,1280,1"/> 多个以英文逗号分隔		
*负载		
速率下限(%): <input type="text" value="10"/>		
速率上限(%): <input type="text" value="100"/>		
初始速率(%): <input type="text" value="10"/>		
测试精度(%): <input type="text" value="10"/>		

吞吐量配置：

测试次数：配置需要进行测试的次数

测试时长：选择按照时长或者突发个数进行测试

时长：需要测试的时间

帧长度：配置测试的帧长度，支持单个或者多个

速率下限：二分法探测的速率下限

速率上限：二分法探测的速率上限

初始速率：二分法探测的初始速率

测试精度：二分法探测结束的速率标识

7.9 测试订单

配置参考 3.10

7.10 报表

配置参考 3.11 报表