AnaTraf

网络流量分析仪

软件使用手册

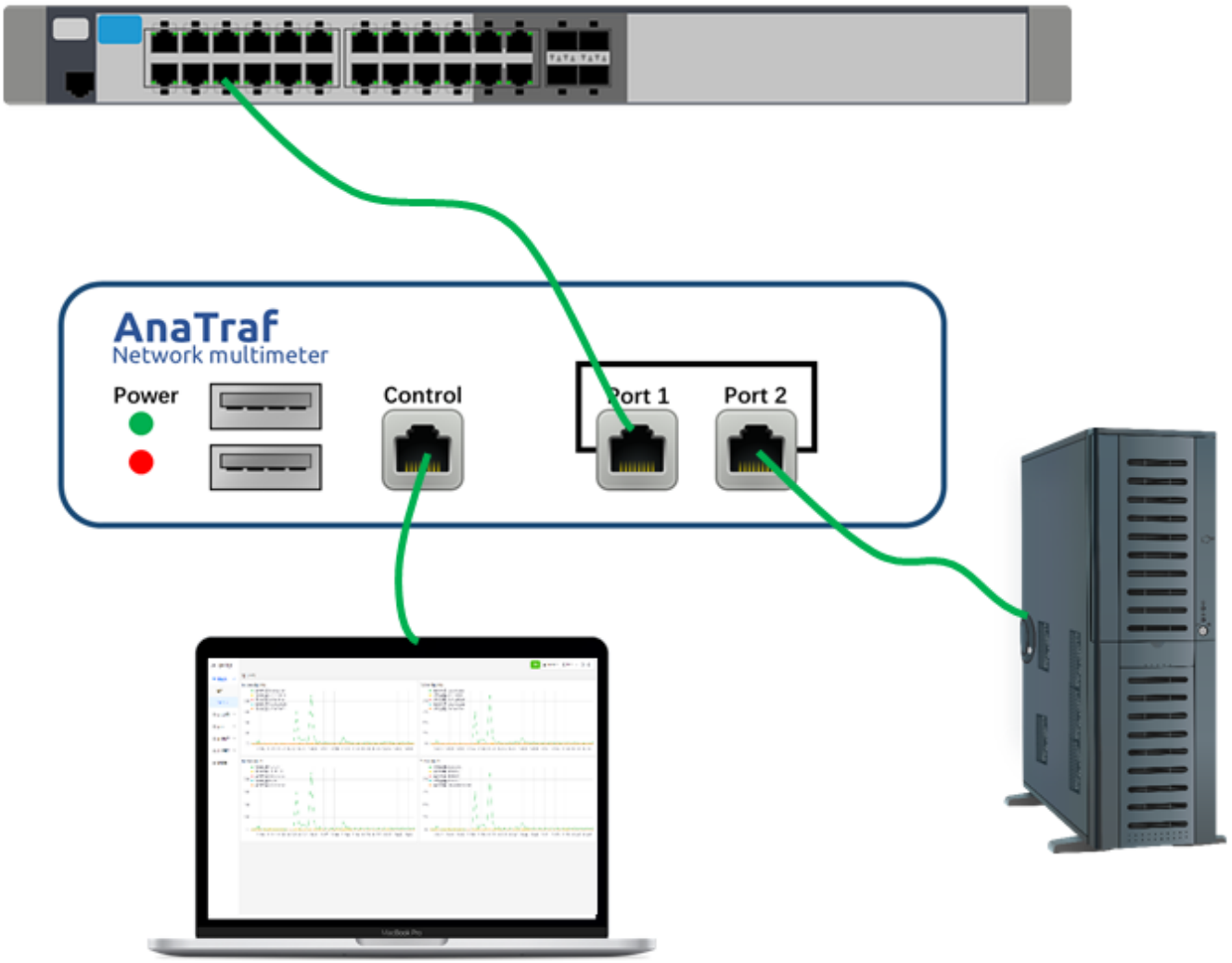
Version 1.8.1

1. 通用安装指南

简单易用是分析仪的特点之一。分析仪即插即用，无需配置，因此分析仪的安装步骤非常简单。

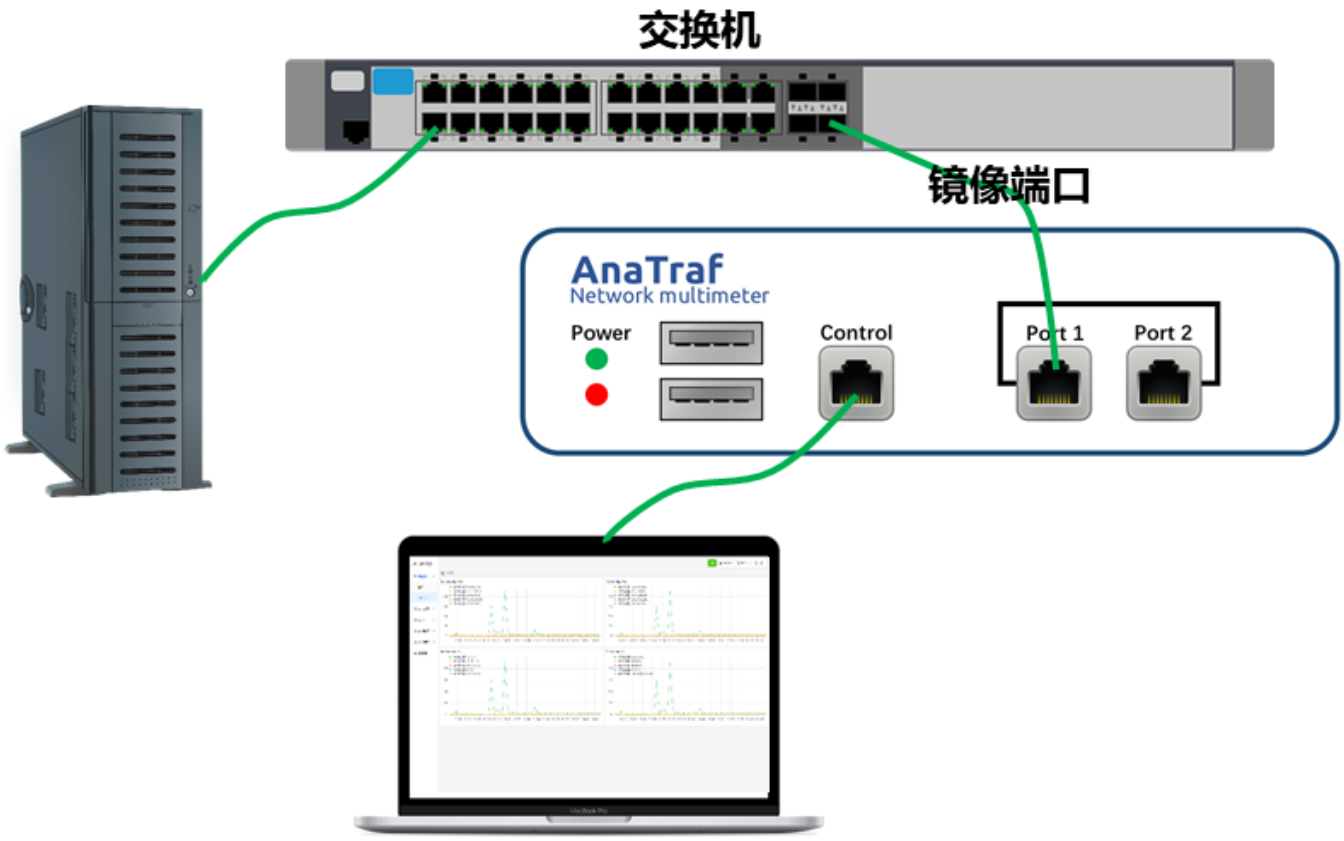
1. 使用电源线将分析仪连接到电源。
2. 使用网线连接分析仪的测量网口，分析仪可以在桥接、TAP 设备和端口镜像模式下工作。
3. 使用网线将终端设备连接到分析仪的管理网口。
4. 在终端设备上访问 GUI,开始分析网络。

1.1 串联

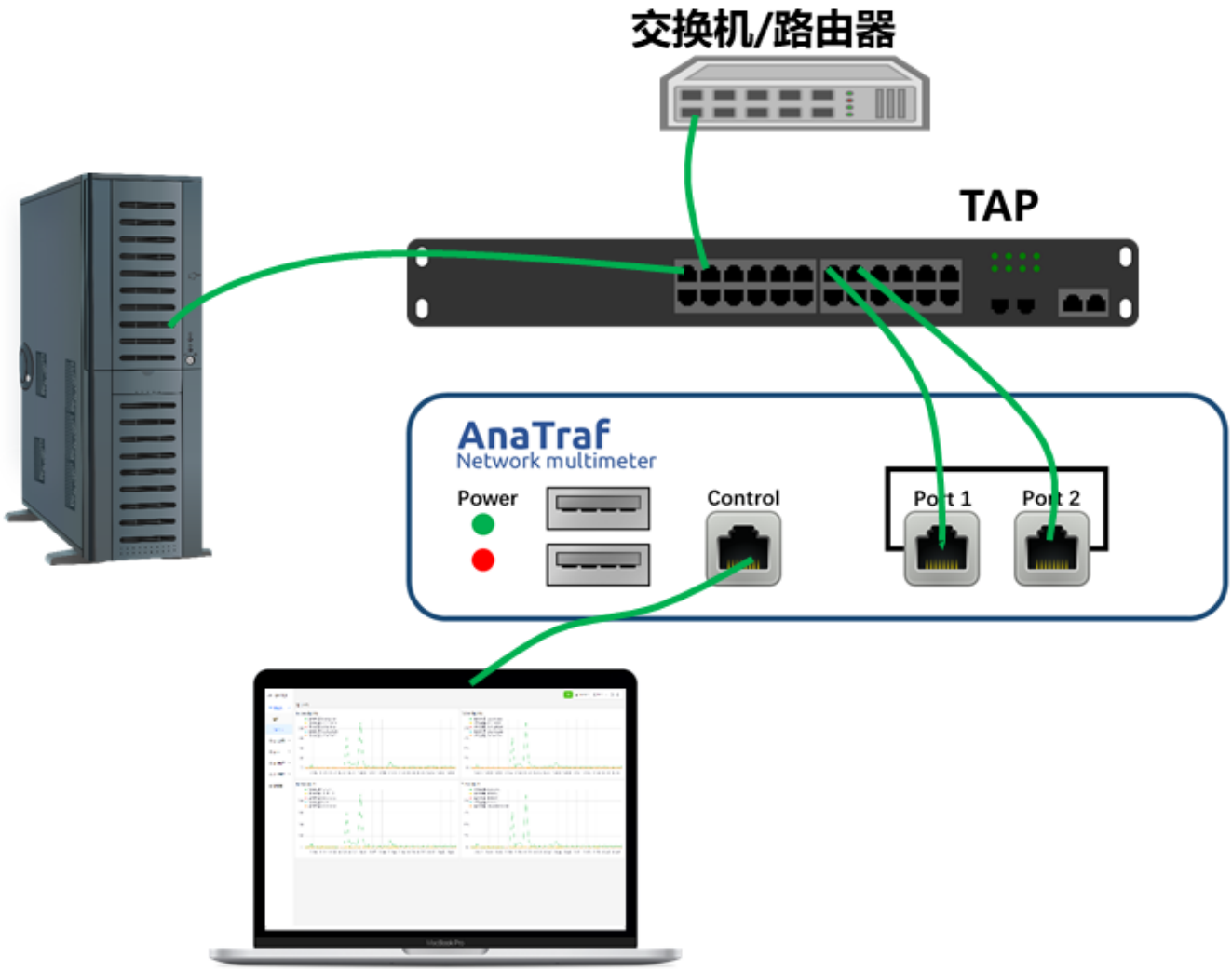


> **注意：** 串联模式将引入微小的延迟，如果链路对延迟敏感，不建议使用串联模式。建议使用镜像端口或TAP设备的方式连接分析仪。

1.2 镜像端口


交换机
镜像端口
AnaTraf
Network multimeter
Power
Control
Port 1
Port 2

1.3 TAP


交换机/路由器
TAP
AnaTraf
Network multimeter
Power
Control
Port 1
Port 2

2. AnaTraf流量分析仪介绍

AnaTraf 网络流量分析仪是一款实时的网络测量、流量分析工具，用于网络流量监控、识别网络性能瓶颈、快速排查网络问题。设备易于安装，即插即用，无需配置，并提供清晰、直观的 WEB GUI 深入分析网络流量。

该设备可以串联在千兆网络中，或者在路由器的镜像端口上运行。

OSI 七层模型将通信系统中的数据流划分为七个层，从分布式应用程序数据的最高层表示到跨通信介质传输数据的物理实现。每个中间层为其上一层提供功能，其自身功能则由其下一层提供。功能的类别通过标准的通信协议在软件中实现。OSI 七层模型划分层次清晰、标准统一，便于研究、分析计算机网络。

AnaTraf 网络流量分析仪按照 OSI 七层模型划分不同的分析模块，分析网络流量，展示网络参数，为用户提供清晰的网络流量分析与网络故障定位方法。

AnaTraf 网络流量分析仪将分析以下网络参数：

- **L2 / 以太网统计和分析**：MAC、ARP、VLAN、突发分析、数据包大小统计、QoS。
- **L3 / IP 统计和分析**：IP、IP Pairs、IP 地理信息、QoS、OSPF。
- **L4 / 传输层统计和分析**：连接、TCP。
- **L7 / 应用层统计和分析**：应用层协议、自定义协议、HTTP、DHCP、DNS、TLS。

AnaTraf 网络流量分析仪实时分析网络流量，所有的统计数据均可实时获取，包括每个 MAC 地址、每个 IP 的流量。此外，可以通过在图表中选取特定的时间范围，从而查看该特定的时间范围内的统计数据。

3. 快速上手

3.1 登录分析界面

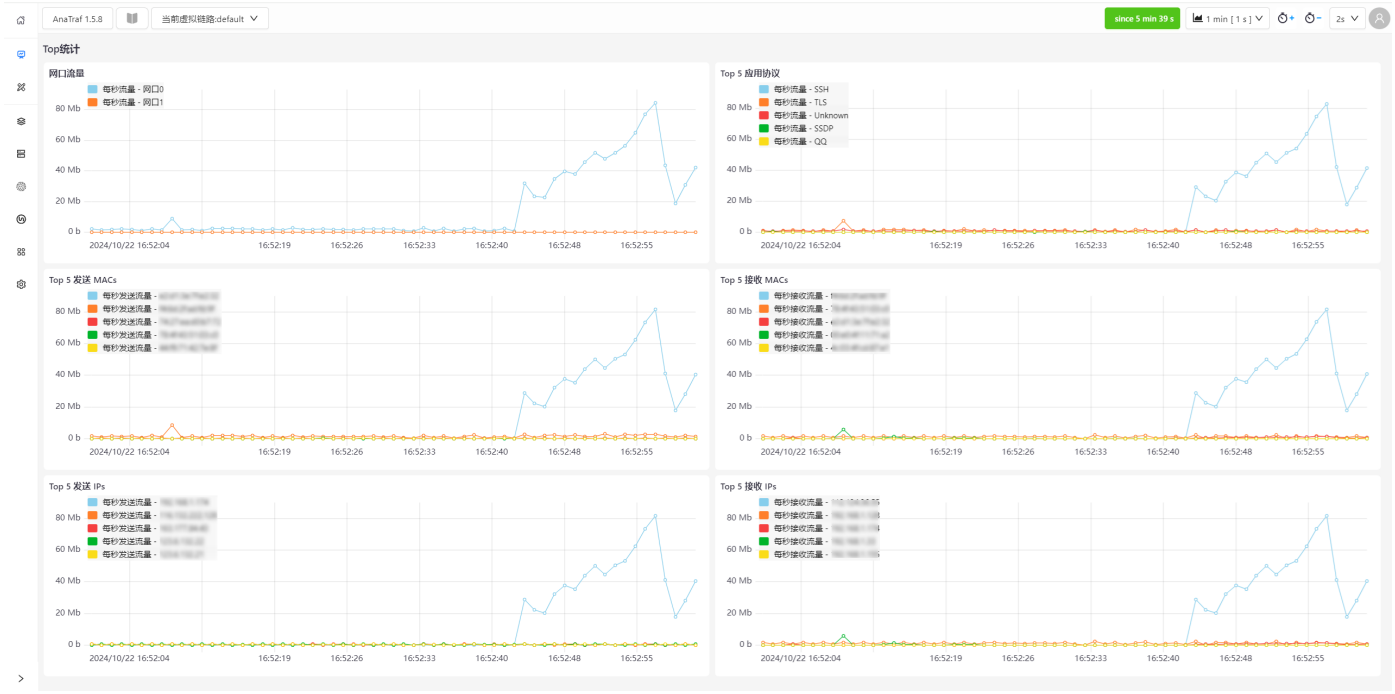
当分析仪安装到网络中并开始工作后，通过 **管理端口** 连接分析仪（如 PC 或者其他终端与分析仪的管理端口直接连接，请先把 PC 或者终端设备的 IP 地址设置为与分析仪 **同一子网** 下的 IP 地址）。

用一个标准的浏览器打开 192.168.1.210 ，将显示下图所示的登录界面。为保证良好的适用体验，推荐使用 **Google Chrome**。

> **注意：** 版本较旧的浏览器可能存在兼容性问题导致分析数据无法正常显示，推荐使用 >= 100.x 版本的谷歌浏览器。

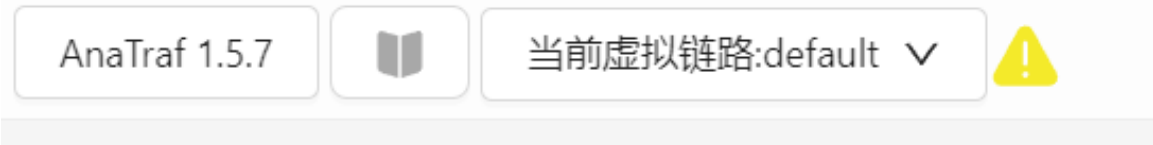
默认的用户名和密码:

- 用户名：**admin**
- 密码：**anatraf**



AnaTraf 网络流量分析仪提供简单直观的 WEB GUI 界面，高效的网络可视化支持分析、钻取实时流量以及历史的流量分析结果。

3.2 顶部工具栏

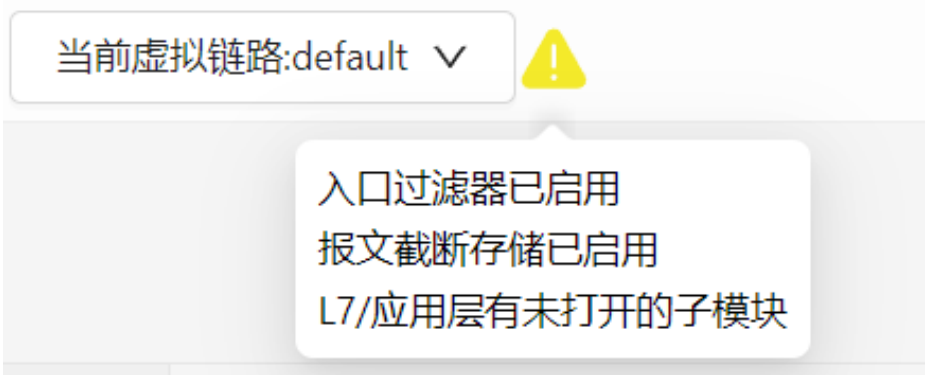


顶部左侧的工具栏自左向右依次为版本信息，用户手册，虚拟链路和提示。

点击版本号，可跳转至 **系统信息** 页面。

点击手册按钮，将打开分析仪的使用手册。

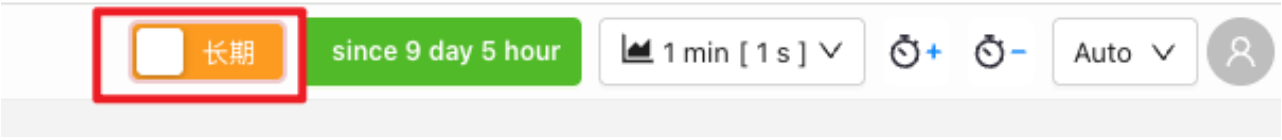
点击虚拟链路按钮，下拉菜单中将显示当前所有的虚拟链路信息。点击响应的虚拟链路将展示相应链路的统计数据。



当分析仪存在生效的 **入口过滤器**、**报文截断存储** 设置或未开启的 **分析模块** 时，顶部工具栏将出现一个警告提示标志。鼠标悬浮在标志上方将显示提示信息。

顶部右侧的工具栏用于显示、更改分析仪的分析模式（实时模式、历史模式）以及分析仪所显示的数据的时间范围。

长期数据库按钮：

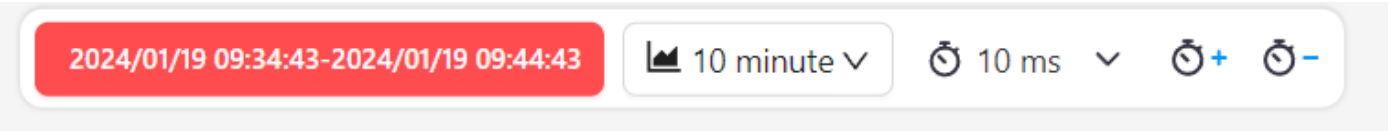


长期数据库按钮用于切换数据源。

按钮处于**实时**状态时，WEB 界面展示的数据来源于**内存数据库**。按钮处于**长期**状态时，WEB 界面展示的数据来源于**长期数据库**。

关于此部分的更多内容，可参考数据持久化 / 长期数据库。

Live按钮：



点击该按钮可以切换实时或者历史模式。

实时模式时，按钮颜色为绿色，按钮上总是显示为分析仪内存数据库内可用的数据时长，即可以在 WEB 界面上查看的统计数据的总时长。

历史模式时，按钮颜色为红色，按钮上显示的时间将变为时间范围的起点和终点时间。右侧的“时间范围选择”按钮，以及在曲线图上通过鼠标拖拽都可以更改历史模式下的时间范围。

例如，分析仪处于 10 分钟的实时模式时，点击“Live”按钮，分析仪将切换为历史模式，历史模式的时间范围为“最后 10 分钟”。

> **注意：** 历史模式时，GUI 界面的统计数据将“定格”为相应时间范围的数据，分析仪 **不中断流量分析** 。

时间范围选择下拉菜单：

点击“时间范围选择”按钮，将出现一个下拉菜单，可以选择实时时间范围统计和历史时间范围统计的时间跨度。选择实时时间范围统计的时间跨度时，分析仪为实时模式；选择历史时间范围统计的时间跨度时，分析仪为历史模式。

按钮上显示的时间表示：**“分析仪当前所选择的时间范围的长度 [以及分析仪此时的统计数据的粒度]”**

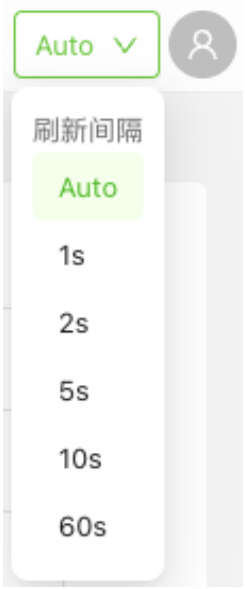
中括号里的内容表示分析仪此时的统计数据的粒度。关于统计数据的粒度，请参考图表数据聚合配置。

列表最下方显示最近 3 条选择过的时间范围。

"+ / -" 按钮：

两个带“+”和“-”的秒表按钮是时间缩放按钮。点击“+”按钮，将会使当前的时间范围扩大 1 倍，例如当前的状态时“1 分钟实时”，点击“+”按钮，时间范围将扩大至 2 分钟。点击“-”按钮，将会使当前的时间范围缩小一半。

刷新间隔下拉菜单：



最右侧的下拉菜单为刷新间隔菜单。这将决定实时模式下图表的刷新间隔。

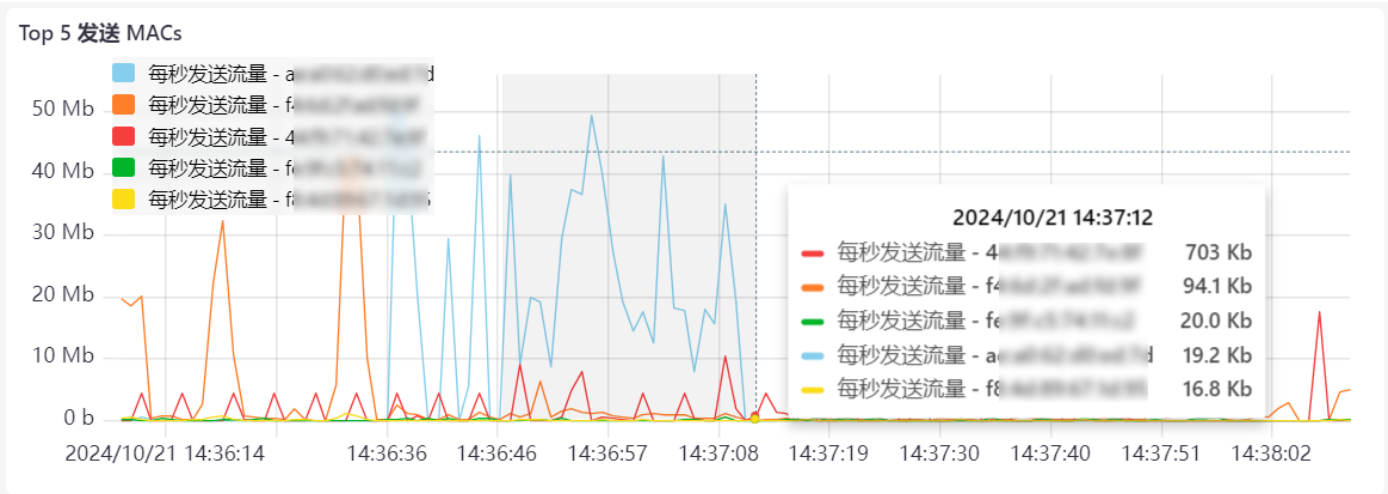
图表的刷新间隔默认为自适应 **（Auto）** 模式，与 **分析仪此时的统计数据的粒度** 保持一致。

当部署环境启用了云端智能助手且当前用户具备相应访问权限时，时间控制器左侧会显示 **智能助手** 入口（AI 图标）。点击后可在侧栏中与助手对话，并结合当前页面、时间范围与仪表板查询等上下文辅助解读流量与排障。详细说明见 AI 智能助手。

3.3 左侧导航栏

网页左侧的导航栏呈现了分析仪的各类功能和分析模块，包括仪表板、通用功能（如事件 / 告警、网口统计、存储管理、路径测量、PCAP 回溯、**报告** 等）、系统设置，以及按 OSI 2-7 层划分的 MAC、ARP、IP、IP Pair、OSPF、TCP、HTTP、TLS 等分析模块。其中 **报告** 用于生成面向指定时间范围（及可选目标 IP）的网络分析报告，详见 报告（网络分析报告）。

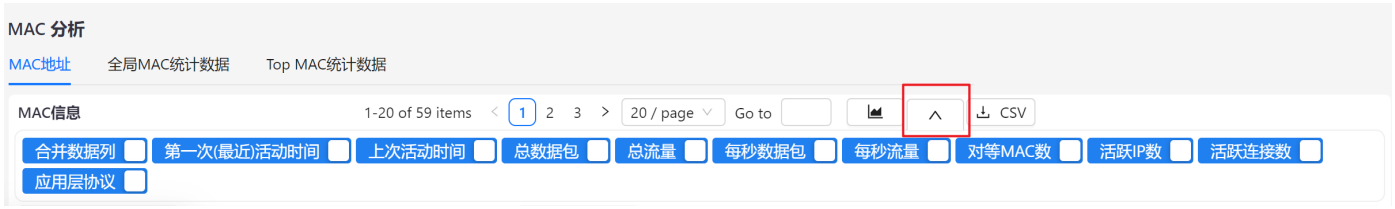
3.4 聚焦时间范围



当在图表中观察到感兴趣的内容时，例如一个流量突发的网络波动。可以通过选择（按住鼠标左键，滑动选取范围）图表的该部分来关注该特定时间范围内的数据。当选择了一个特定的时间范围后，该时间范围将全局生效，分析仪将切换为历史分析模式。分析仪将会立即重新计算所有的统计数据，以呈现该特定范围内的统计结果。

关于此部分的详细内容，请参考交互式图表。

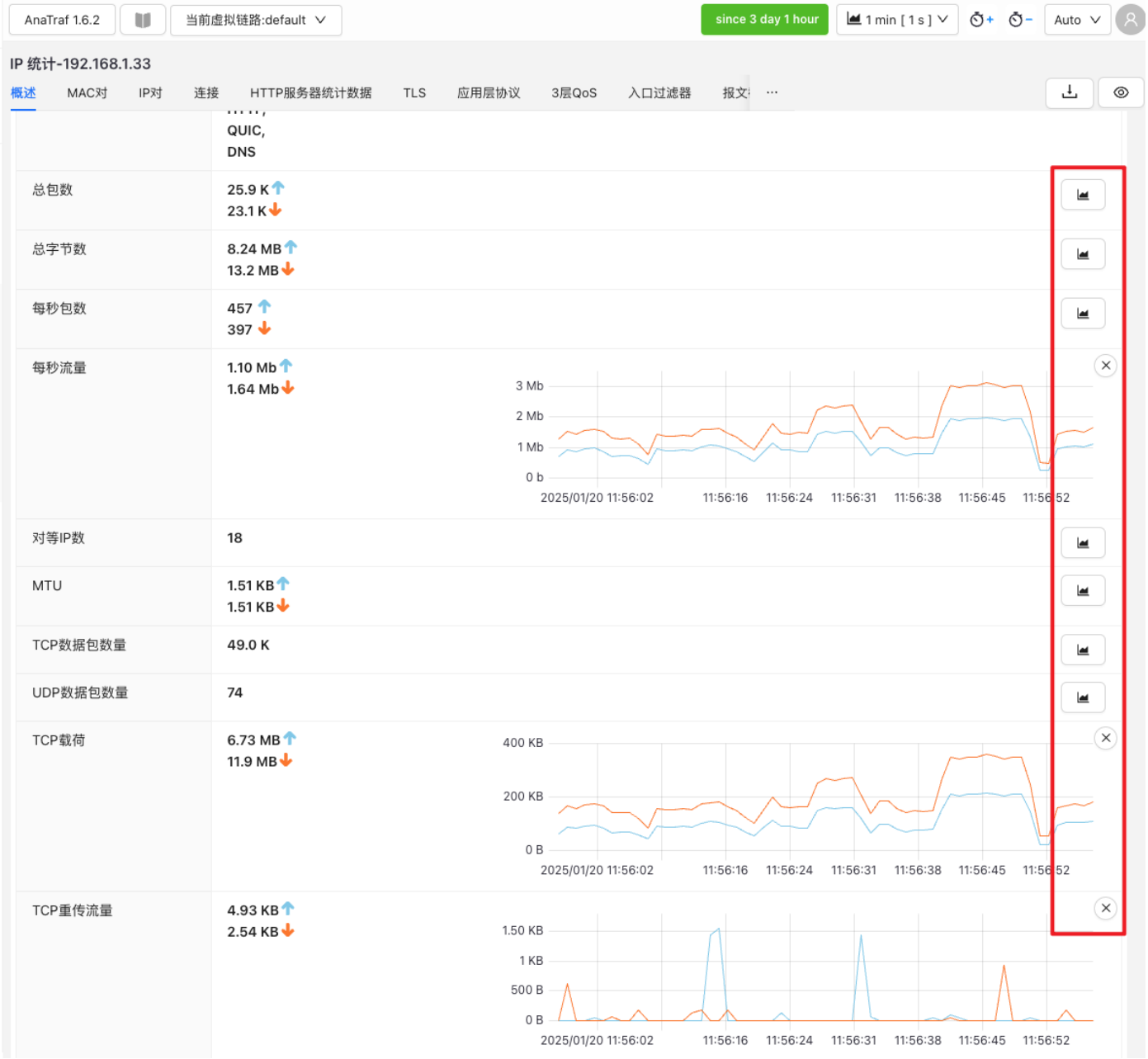
3.5 表格列开关



某些分析模块的数据表格可能具有非常多的统计指标，如 IP 数据表，Connections 数据表，所以这些模块的数据表格将会相对庞大。虽然表格提供了很多统计数据，但可能只对其中的一部分感兴趣。可以通过列开关，将不需要的表格列隐藏，从而只关注感兴趣的列。

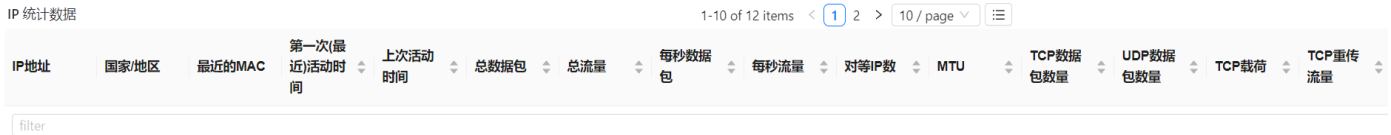
3.6 图开关

虽然表格提供了很多统计数据，但可能只对其中的一部分感兴趣。对于某些统计指标，可能更关心其历史的变化趋势，可以通过图开关，在显示配置中选择关注的指标，所选的指标将以图的形式呈现。



在某个特定的网络对象（如某个 IP、某个 MAC）的详细分析页面，可以点击统计指标右侧的图开关，显示 / 隐藏相应统计指标的历史曲线图。

3.7 表格过滤



表格中包含一个过滤表达式输入框，用于对表格进行过滤，从而关注感兴趣的内容。
关于表格过滤的详细内容，请参考高级表达式。

3.8 查看详细分析

分析仪界面上的许多位置都设置了跳转连接，如 IP 地址、MAC 地址等。可跳转内容显示为蓝色字体。点击跳转链接，能够进入相应内容的详细分析页面。例如，点击一个特定的 IP 地址，可以进入该 IP 地址的详细分析页面，获取更深入的分析结果。

3.9 下载 PCAP

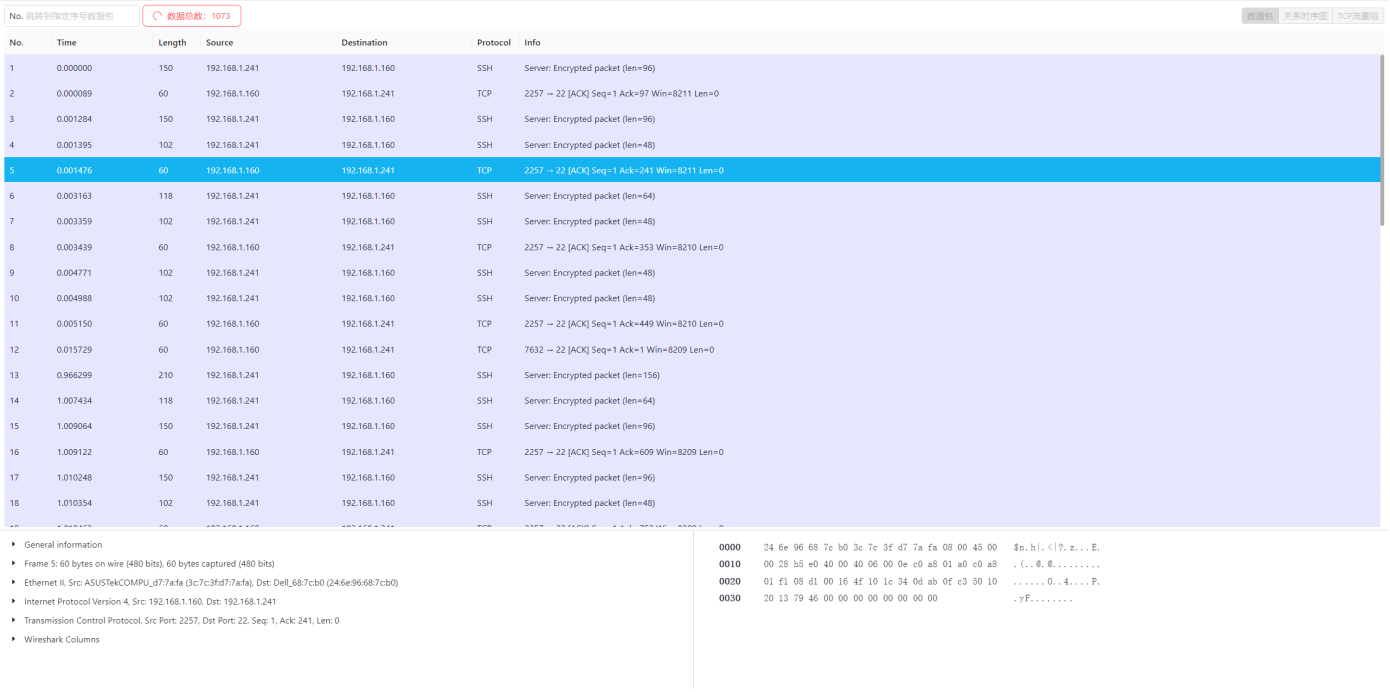
许多表格会提供“**PCAP 下载**”列，该列提供两个按钮，上方的是下载按钮，下方的是在线预览按钮。点击下载按钮将下载相应的网络对象的流量，且满足分析仪当前状态的时间范围，以及表格生效的过滤表达式。

当鼠标指针悬停在下载按钮上时，可预览过滤表达式。

> **注意：** PCAP下载功能需要开启“PCAP 存储开关”。当设备未开启 PCAP 存储功能时，将无法使用 PCAP 下载功能。您可在系统配置中更改此选项。

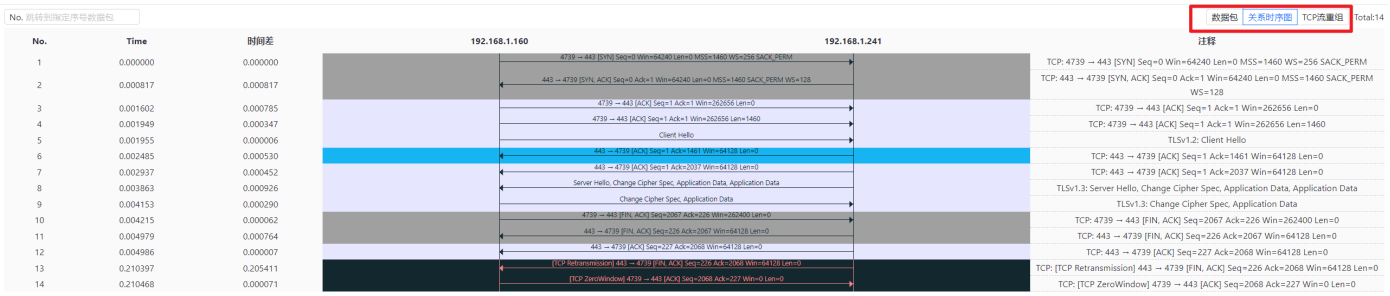
3.10 在线解码

许多表格会提供“**PCAP 下载**”列，该列提供两个按钮，上方的是下载按钮，下方的是在线预览按钮。点击在线预览按钮可以在 WEB 界面上对报文进行在线解码分析。



> **注意：** 关系时序图和 TCP 流重组功能需报文加载完毕才能使用。如报文数量过大，可以点击左上角 **数据总数** 按钮，停止加载后续的报文。

3.10.1 关系时序图



在线解码界面的右上角可以选择切换显示**关系时序图**。关系时序图将显示连接双方的数据包交互情况。

3.10.2 TCP 流重组

在线解码界面的右上角可以选择切换显示**TCP 流重组**。TCP 流重组界面将显示连接传输的内容。

> **注意：** TCP 流重组功能仅支持 TCP 连接。

4. 统计数据展示说明

简而言之，分析仪显示**时间窗口内，分析仪观测到的统计数据**。

4.1 实时模式

实时模式下，界面上呈现的数据都是一个不断向前滑动的时间窗口内的统计结果，该时间窗口的大小为所设置的时间范围，滑动的频率和步长由刷新间隔决定。

实时类指标（每秒流量、每秒数据包等），信息类指标（替代名称、活动时间等）均显示为“上一秒的统计结果”，不论实时模式所设置的时间范围以及图表刷新间隔。

总量类指标（总数据包、应用层协议等），均显示为时间窗口内的统计值。因此，当时间窗口不断向前滑动时，可能出现总流量下降的情况。

如果一个 IP 地址、MAC地址在时间窗口内没有观测到任何流量数据，那么该地址将不会在界面上显示，也不会被过滤表达式检索。例如某个 IP 地址在过去一小时前观测到存在流量数据，随后都没有流量数据，那么在 1 分钟实时模式下，IP 信息表中不会出现此 IP 地址，且无法通过过滤表达式检索此 IP 地址。

4.2 历史模式

历史模式下，界面上呈现的数据是一个静止的时间窗口内的统计结果，该时间窗口的大小为所设置的时间范围。

实时类指标（每秒流量、每秒数据包等），不论所设置的时间范围，均显示为**平均值**。计算平均值时的**除数（分母）**是该对象在所选的时间范围内**真正活跃的时间**。

总量类指标（总数据包、应用层协议等），均显示为时间窗口内的统计值。

同样，如果某个网络对象（某个 IP 地址、MAC 地址）在相应时间窗口内未观测到流量数据，那么该对象将不会在界面上显示，也不会被过滤表达式检索。

4.3 多粒度数据

按照时间的由近到远，提供 1 秒，10 秒，1 分钟，10 分钟，1 小时粒度的历史数据。各种粒度的数据可用时长可在系统设置 - 图表数据聚合配置中设置。

当前所呈现的数据粒度显示在顶部工具栏 - 时间范围选择下拉菜单。

当以实时模式查看不同粒度的数据时，实时数据的刷新间隔将根据数据的粒度自动切换。

比如，当实时查看 10 秒粒度的数据时，数据的刷新间隔将自动切换为 10 秒。可以手动将数据的刷新间隔设置为 1 秒，由于每 10 秒产生一个最新的数据点，1 秒的刷新间隔的效果与 10 秒没有差别，但产生了许多无效的请求。

4.4 数据持久化 / 长期数据库

最近一段时间、最新的数据存储在内存中，即**内存数据库**。当内存数据库存储的数据达到了内存的使用限制时，内存数据库将会删除最旧的数据，以存储最新的数据。

内存数据库中的数据可用的时长，取决于内存的大小、网络流量中对象的数量以及数据颗粒度的设置。分析仪始终将最近一段时间、最新的数据存储在内存中，这部分数据能够快速的检索。内存数据库中的数据会因设备重启、断电、系统崩溃而丢失。

长期数据库作为内存数据库的拓展，将数据存储在高速硬盘中，从而增加数据可用的时长。相比于内存数据库中的数据，长期数据库的数据检索速度较慢，但能够提供细颗粒度（高精度）的历史数据。

5. 仪表板

仪表板提供了分析仪所处理、分析的流量的快速概览。

5.1 TOP 统计

分析仪在此部分预设了一些曲线图，显示了分析仪观测到的最活跃的网络对象。

TOP User 仪表板提供了网络流量中最活跃的网络对象的快速概览。
该仪表板包含 3 部分：

1. 总流量概览
2. 最活跃的 5 个 IP 地址
3. 最活跃的 5 个 MAC 地址
4. 最活跃的 5 个 L7 应用层协议

在实时模式下，显示的是实时模式对应的时间范围内最活跃的网络对象。例如，在 1 分钟实时模式下，显示的是最近 1 分钟字节数最多的 IP 地址。

在历史模式下，显示的是历史模式对应的时间范围内最活跃的网络对象。例如，在过去某一个跨度为 1 小时的时间范围，显示的是该范围内字节数最多的 IP 地址。

5.2 自定义仪表板

除了能够在 TOP 统计中查看最活跃的网络对象外，分析仪还支持自定义仪表板，您可以在此页面添加感兴趣的图表。

6. 交互式图表

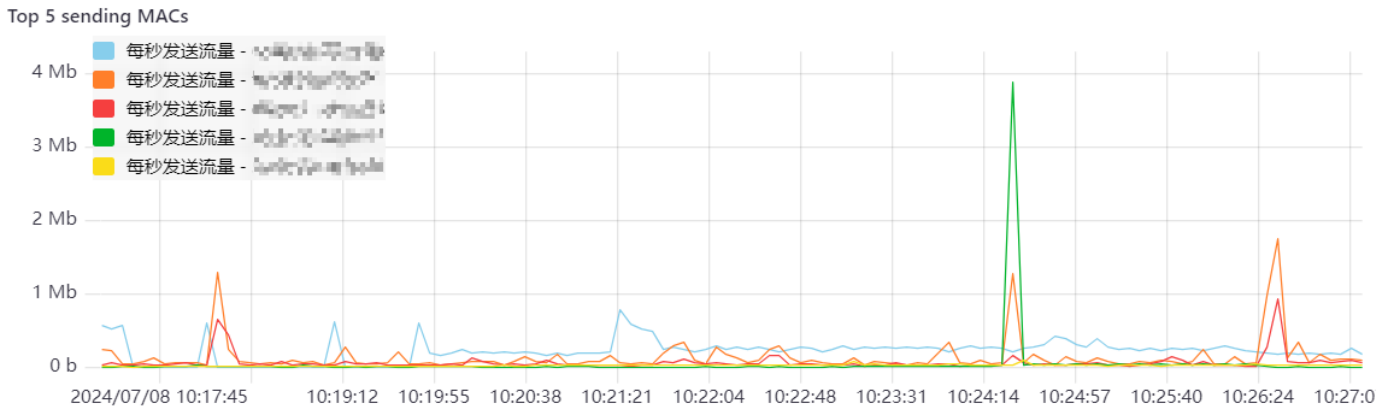
AnaTraf 网络流量分析仪提供直观、高效的界面来监控和分析网络活动。实时地将复杂的网络数据转换为易于理解的视觉表示，即时呈现网络流量的动态变化，极大提高了网络监控和故障排除效率。

分析仪提供的图表主要有如下几类：

- 曲线图
- 数据表

图表都提供了方便快捷的交互方式，便于钻取网络流量信息，深入了解网络。

6.1 曲线图



曲线图显示了特定的网络对象在“一段时间”中的变化趋势。例如，某个 IP 地址在最近 10 分钟的接收流量变化图。

“一段时间”所指的时间范围和实时模式或历史模式所对应的时间范围一致。

6.1.1 显示 / 隐藏曲线

当一个曲线图中绘制了多个网络对象时，多条曲线可能重叠。
您可以点击图例上的网络对象，可以显示 / 隐藏对应的曲线。
被隐藏的曲线其图例将显示为灰色。

6.1.2 聚焦时间范围

可以通过选择（鼠标左键，滑动选取范围）图表的该部分来关注该特定时间范围内的数据。当选择了一个特定的时间范围后，该时间范围将全局生效，分析仪将切换为历史分析模式。分析仪将会立即重新计算所有的统计数据，以呈现该特定范围内的统计结果。

6.2 数据表

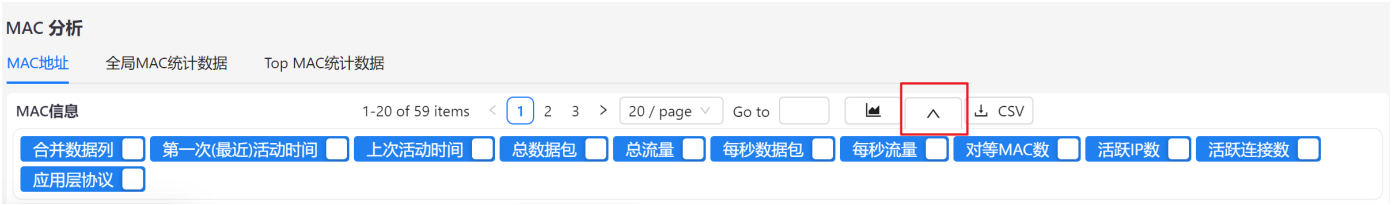
数据表格能够提供更加全面的流量分析结果。主要包括以下几类数据：

- 实时数据：如每秒的流量速率统计
- 总量数据：如总接收字节数，显示的值是所选的时间范围内的统计结果。
- 曲线图：表格中嵌套的曲线图，如流量速率图。

表格中有许多内容都是可跳转的链接，点击链接，可以跳转到相应的详细分析页面。

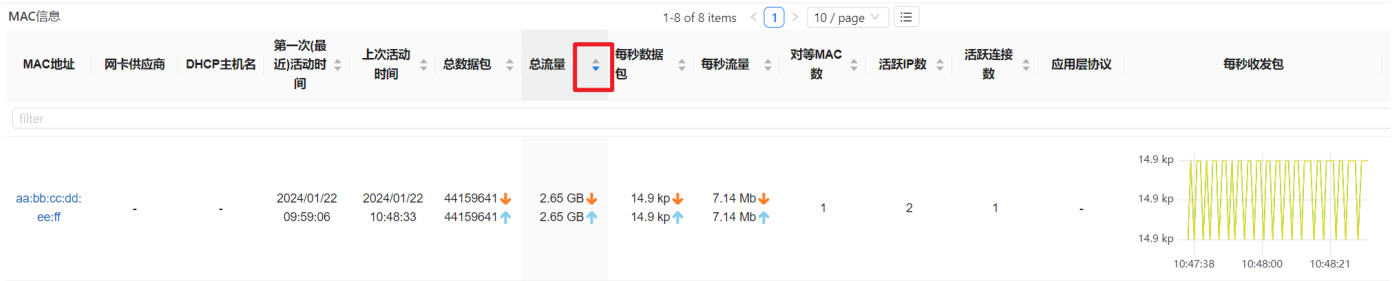
6.2.1 列开关

某些分析模块的数据表格可能具有非常多的统计指标，如 IP 数据表，Connections 数据表，所以这些模块的数据表格将会相对庞大。虽然表格提供了很多统计数据，但可能只对其中的一部分感兴趣。可以通过列开关，将不需要的表格列隐藏，从而只关注感兴趣的列。



点击表格上方的收放按钮，可以显示/隐藏表格的列开关。打开/关闭列开关可以显示/隐藏对应的表格列。

6.2.2 表格排序



表格的一些列可以进行排序，可排序的列具有一个可排序的标记。当需要根据某一列对表格进行排序时，只需点击该列即可。

6.2.3 IP 过滤

表格中的 IP 列提供了 IP 地址的过滤，点击 IP 列的过滤按钮即可查看可选的过滤方式，点击相应的过滤条件即可过滤内网、外网，IPv4、IPv6 地址。

6.2.4 内容匹配

表格中包含一个过滤表达式输入框，用于对表格进行过滤。

可以输入单个值进行过滤，例如，在 IP 模块，可以在输入框中输入“192.168.1.1”（不需要引号），按下回车键后，表格将匹配输入的 IP 地址，表格会立即更新。更新后的表格将显示被“192.168.1.1”匹配的内容。

> **注意：**
>
> 1. 输入单个值的匹配为文本匹配，范围为整个表格。例如在 IP Pairs 模块表格的过滤表达式输入框中输入“192.168.1.1”（不需要引号），按下回车后，更新后的表格将显示被“192.168.1.1”匹配的内容，被匹配的是“IP 地址”或者“对等 IP”两列中包含所输入 IP 的行。
> 2. 过滤表达式支持输入中文。

6.2.5 高级表达式

在输入框中可以输入高级表达式（键值对形式）从而实现更加精准、更加强大的表格过滤。

通过高级表达式的形式，可以将匹配的范围限定为特定的字段（列）。

例如，例如在 IP Pairs 模块表格的过滤表达式输入框中输入“ip_peer == 192.168.1.1”（不需要引号），按下回车后，更新后的表格将显示“对等 IP”这一列列被“192.168.1.1”匹配的内容，即过滤出“对等 IP”为“192.168.1.1”的行。

在表格的过滤表达式输入框中进行输入时，会对输入进行实时检查，如果输入不符合过滤表达式的语法，输入框的边缘将显示为红色，以提示语法错误。

> **注意：** 各分析模块表格过滤功能支持的关键词请参考附录一：表格过滤关键字。

6.2.6 模糊查询与精确查询

在需要对字符串类型的数据（如域名）进行过滤时，模糊匹配和精确查询能实现更灵活的过滤。

通过高级表达式的 **全等运算符（===）** 可以实现精确查询，**==** 运算符实现模糊查询。

可以通过模糊查询所有包含 “baidu.com” 字段的域名解析记录，如下图所示。

可以通过精确查询“baidu.com”这一特定域名的解析记录，如下图所示。

6.2.7 表格数据导出

点击表格顶端的 **下载 csv** 按钮可以将表格的数据导出 csv 文件。

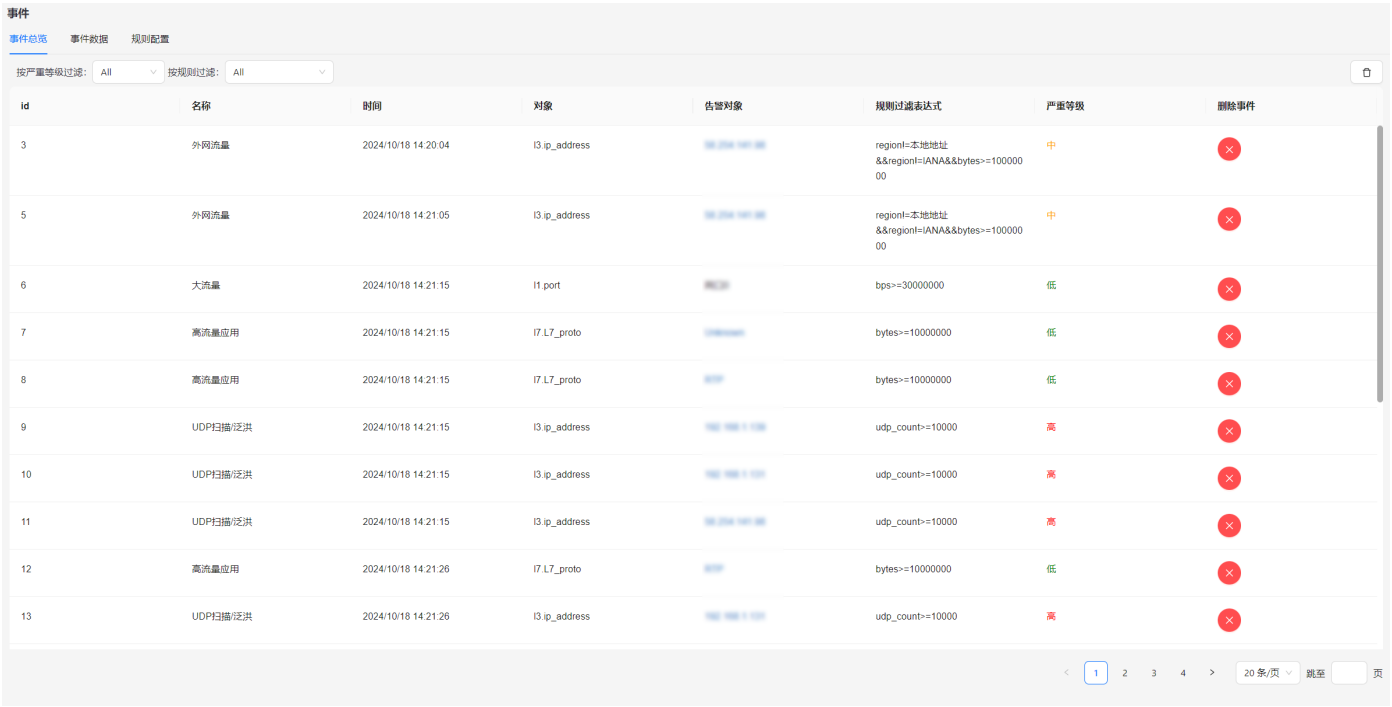
可以输入导出数据的起止范围，导出从特定位置开始的若干条数据。

勾选 **导出所有数据** 选项，可导出所有数据。

7. 通用模块

7.1 事件 / 告警

7.1.1 事件总览



此页面展示所有触发的规则事件，表格中的每一行表示该规则的一次触发。

可以按照规则触发器对事件进行过滤。

> **注意：** 只保留最近触发的 **1000条** 事件。

7.1.2 事件数据

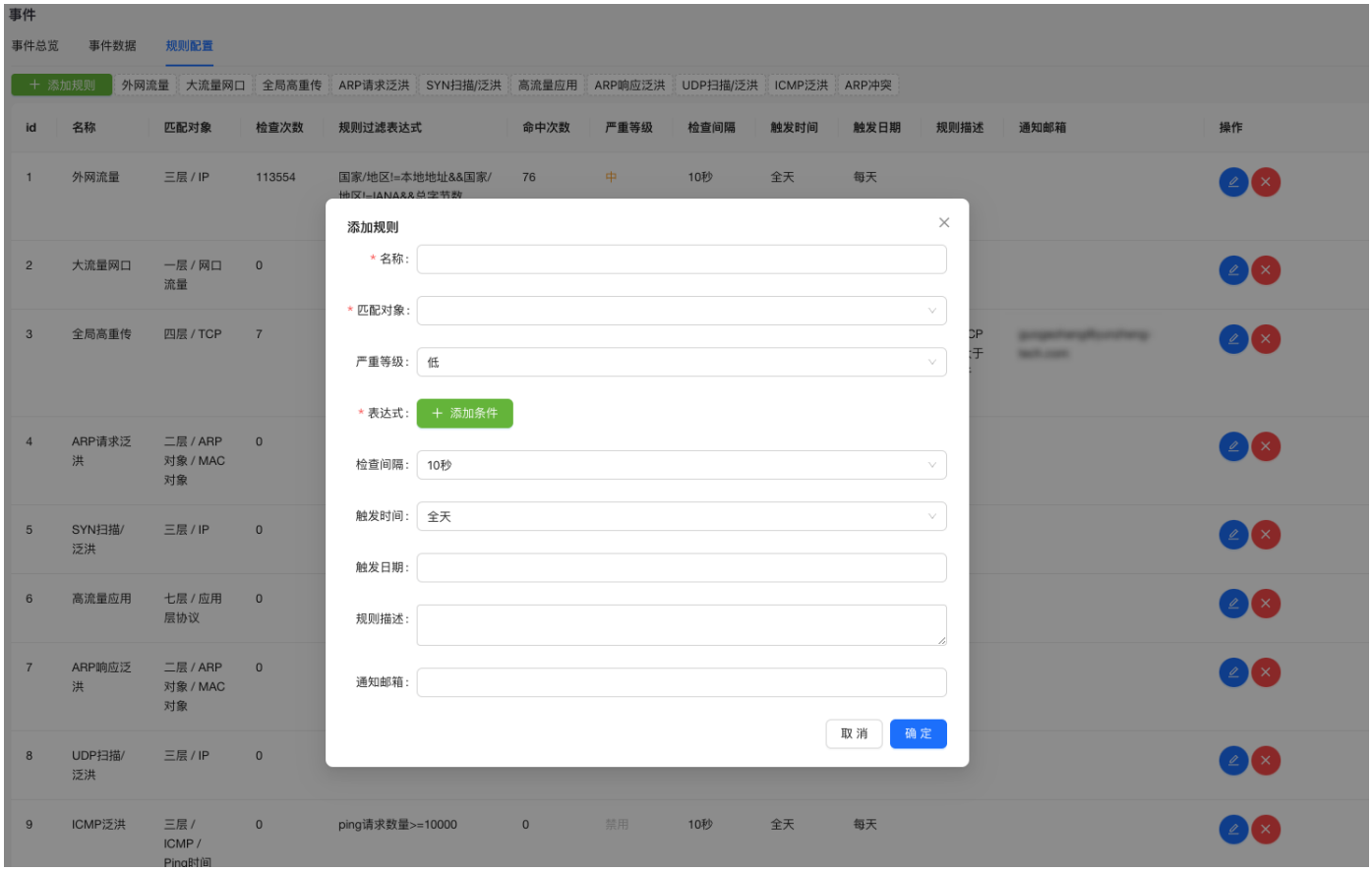
此页面展示了各规则随时间变化的命中次数、检查次数和命中率。

名称	描述
规则 id	唯一地表示一条规则的 ID
规则名称	规则的名称
规则命中次数	即该规则的触发次数
规则检查次数	
规则命中率	规则命中次数 / 规则检查次数

7.1.3 规则配置

规则配置页面显示了所有已添加的规则，在此页面，可以对规则进行管理。

7.1.3.1 添加规则

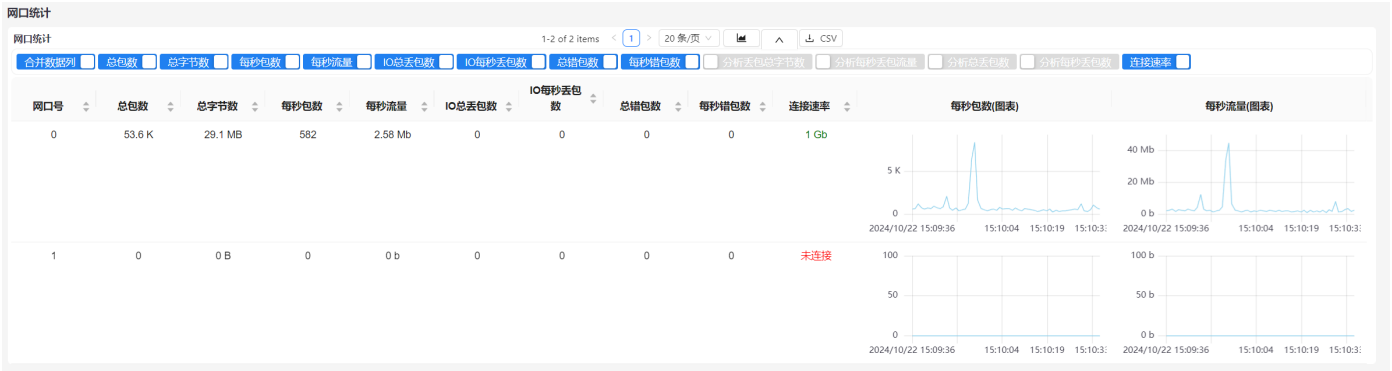


点击 **添加规则** 按钮，可以对多种统计指标进行匹配、监控。

名称	描述
名称	设置该规则的名称
匹配对象	选择需要匹配的分析模块
严重等级	可选：低、中、高，以及禁用。禁用时，规则将不进行检查，也不会触发事件
表达式	网络对象、统计指标具体的匹配规则。每一行是一个条件，同一规则下的所有条件为 **AND(且)** 的关系
检查间隔	可选 1秒、10秒、1分钟、10分钟、1小时
触发时间	设置规则可在一天中的触发的时间段
触发日期	设置规则的触发日期
规则描述	填写对规则的描述
通知邮箱	填写该规则被触发时，通知的邮箱

在 **添加规则** 按钮右侧，提供了一系列的预设规则。预设规则添加后，默认为 **禁用** 状态。可以编辑规则以启用规则，或修改规则参数。

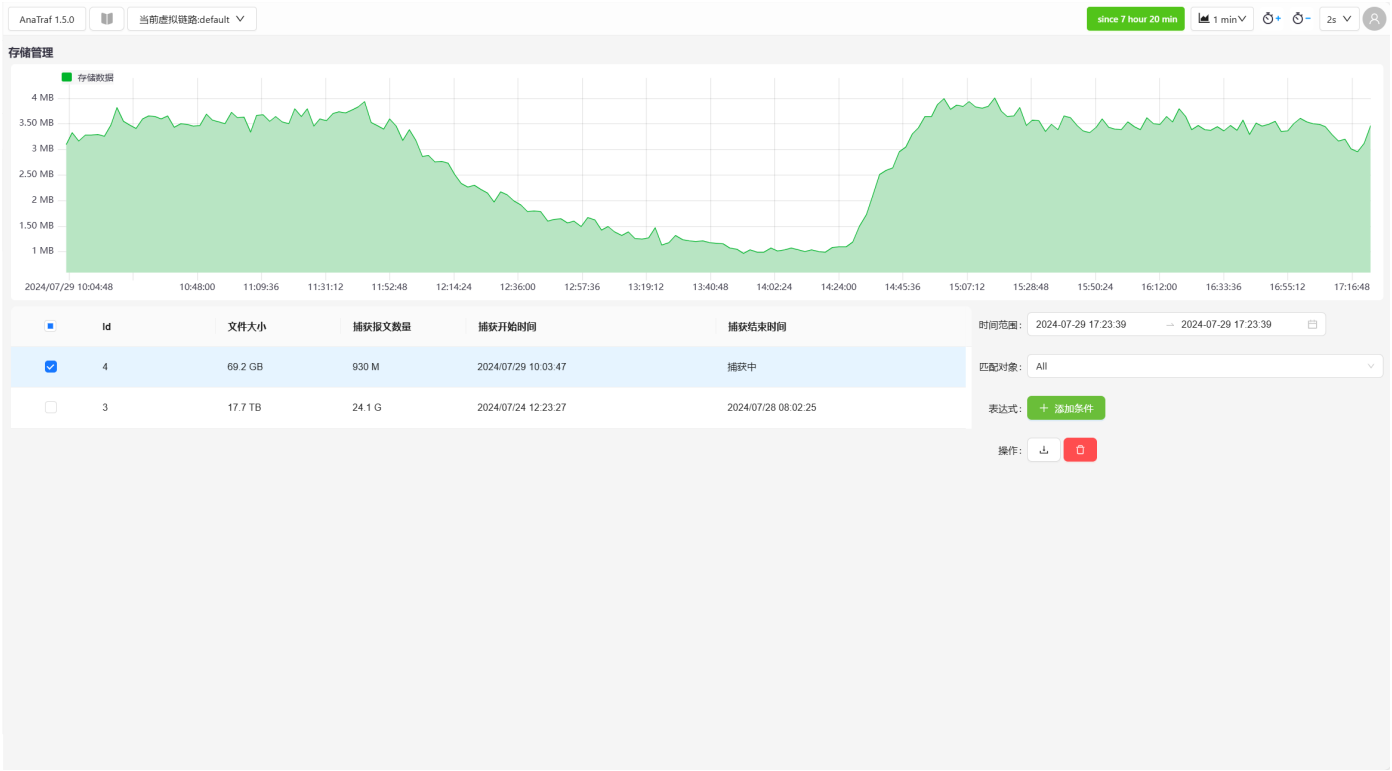
7.2 网口统计



网口统计显示 AnaTraf 网络流量分析仪各网口的实时状态以及流量统计。

名称	描述
网口号	-
总包数	-
总字节数	-
每秒包数	-
每秒流量	-
IO 总丢包数	因收发能力达到瓶颈导致的丢包数量
IO 每秒丢包数	因收发能力达到瓶颈导致的每秒丢包数量
总错包数	-
每秒错包数	-
分析丢包总字节数	因分析能力达到瓶颈导致的丢包字节数
分析每秒丢包流量	因分析能力达到瓶颈导致的每秒丢包流量
分析总丢包数	因分析能力达到瓶颈导致的丢包数量
分析每秒丢包数	因分析能力达到瓶颈导致的每秒丢包数量
连接速率	显示网口的连接速率，如果该网口未连接，则显示为红色的“未连接”提示，并且该网口的流量统计结果为 0

7.3 存储管理



此页面展示了分析仪的流量捕获情况，可以对捕获的流量文件进行下载和删除。

上方的曲线图显示了存储数据随时间的变化。点击列表中的捕获文件，将显示相应捕获文件的存储数据随时间变化的曲线图。

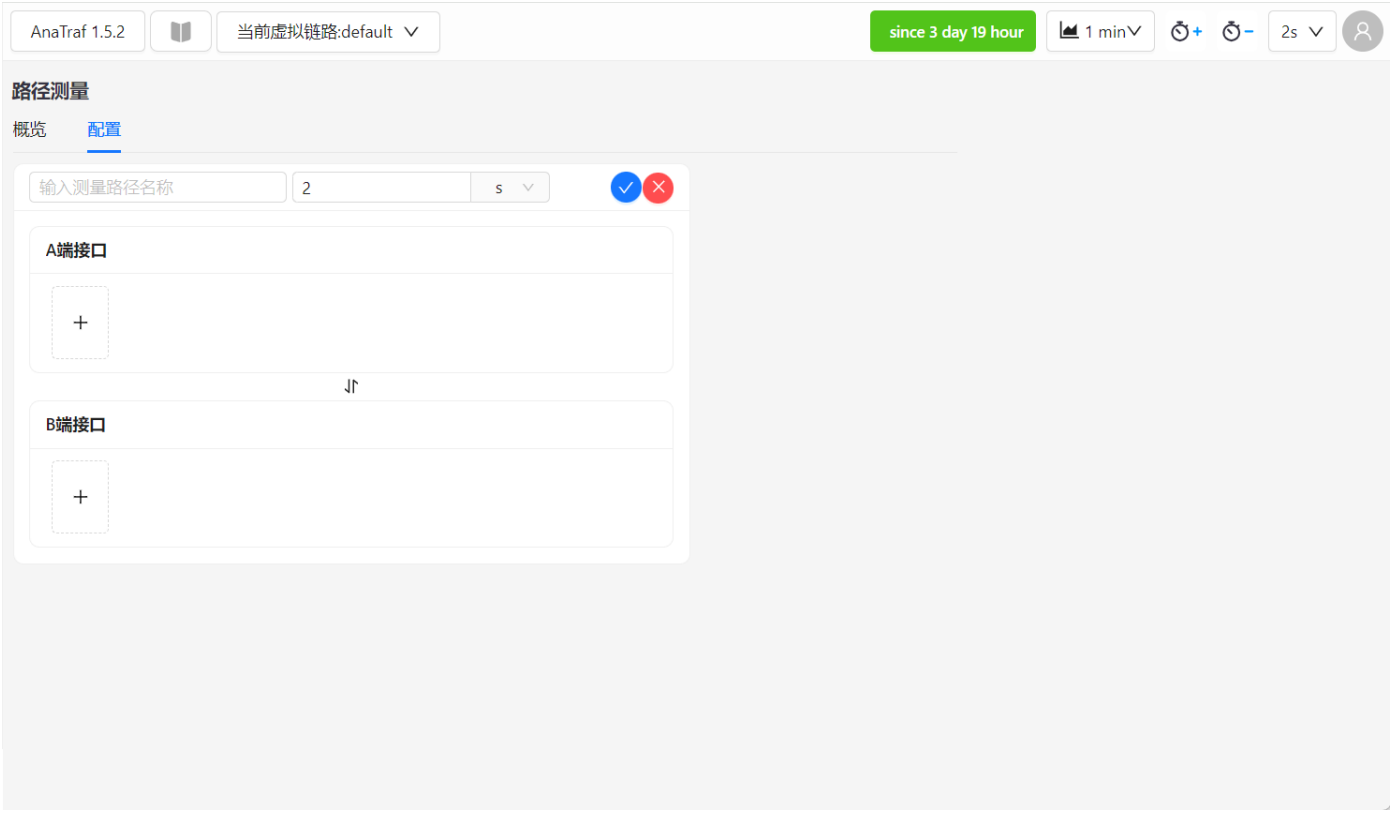
通过鼠标拖拽可以选取时间范围，随后对该时间范围内的流量数据进行下载。

- 循环存储：当硬盘空间已满时，新捕获的流量将从历史捕获文件中时间最早的一个开始覆盖存储。

7.4 路径测量

在部署分析仪时，可以将网络中各节点的流量镜像至分析仪的不同网口。路径测量功能可以测量网络中两个节点之间的延迟和丢包。

例如，需要测量网络流量经过一个网络设备（A - 设备 - B）的延迟和丢包，将网络中两个节点 A 和 B 的流量分别镜像至分析仪的网口 1 和网口 2，那么通过路径测量功能，可以测量 A -> B 和 B -> A 方向的丢包和延迟。



配置时填写路径测量的名称、最大等待延迟以及选择 A 端和 B 端的网口。配置完成后，可以回到路径测量的 **概览** 页面查看延迟和丢包的测量结果。

> **注意：**
>
> 1. 丢包的测量结果是滞后的，滞后的时间为设置的最大等待延迟；延迟的测量结果是实时的。
> 2. 最大等待延迟影响丢包率的统计，例如 A -> B 方向，如果一个报文在 B 点与在 A 点被观测到的时间差超过最大等待延迟，那么这个报文将被判定为丢包。判定为丢包的报文将不计算延迟。

7.5 上传 PCAP 文件进行回溯分析

分析仪支持对 PCAP 文件进行分析，使用 PCAP 分析功能 **不中断** 实时的流量分析。

PCAP 文件支持上传，以及在存储管理页面选取后点击 **回放** 按钮。

PCAP 文件回放的流量将在一条独立的 **replay 虚拟链路** 中分析。replay 虚拟链路的流量统计结果和其他实时分析的虚拟链路完全独立。

通过顶部的 **虚拟链路** 按钮切换至回放链路即可查看 PCAP 的统计分析结果。通过 WEB GUI 查看 PCAP 统计结果的操作与实时分析模式下的操作完全一致。

> **注意：** 分析仪只对上传的 pcap 文件进行分析，而不进行存储，因此 **replay 虚拟链路** 不提供在线预览和 pcap 下载功能。

7.6 AI 智能助手

AI 智能助手 在分析仪 WEB 界面顶部工具栏、时间范围选择区域旁提供入口（AI 图标）。当部署方已接入云端 Agent 服务且当前用户具备相应权限时，该入口可见；界面会从云端加载智能助手前端模块并与 Agent 服务通信。

打开助手后，将以侧栏形式展示对话界面。侧栏支持 **浮层** 与 **停靠** 两种布局：浮层模式下点击侧栏外的遮罩可关闭；停靠模式下主内容区会随侧栏宽度收缩。侧栏宽度可按需调整。

智能助手能够获取与当前分析视图相关的 **页面上下文**，例如：当前所处的功能路由、分析仪全局 **时间范围**（与顶部时间控制器一致）、以及当前仪表板中各面板的查询配置等。用户可在浏览各类统计、钻取详情的同时向助手提问，便于结合当前数据做解读与排障思路梳理。

使用助手前，通常需要在助手界面中完成 **云端 Agent 服务的账号登录**（具体以部署方提供的认证方式为准）。助手依赖与部署环境之间的网络连通性；若无法加载助手模块或连接服务失败，请检查网络与部署配置。

> **说明：** 智能助手与下文 报告（网络分析报告） 中的可选 **AI 深度分析** 均依赖同一类云端 Agent / AI 服务，是否开放、如何认证由部署方决定。助手侧重交互式问答；报告侧重对一段时间内的流量数据做结构化分析与文档输出。

7.7 报告（网络分析报告）

在左侧导航栏的 **通用** 分组下选择 **报告**，可进入 **网络分析报告** 功能（页面标题为「网络分析报告」）。该功能在选定的时间范围内，从分析仪已采集的统计数据中汇总 L2 / L3 / L4 / L7 等多层信息，对网络异常与风险点进行检测，并生成可读的分析结论与报告文档。访问该菜单需要具备与常规数据查询页面相当的 **数据查看** 类权限（以实际角色配置为准）。

分析范围与配置

- **时间范围**：可在报告页内指定起止时间，也可与界面 **全局时间范围** 对齐（例如从全局时间复制到表单，或将表单时间应用回全局），以便与其它统计页面保持一致的分析窗口。
- **目标 IP（可选）**：可填写关注的 IP，将分析焦点集中到与该主机相关的连接与指标；不填则面向整体流量做综合检测。

分析模式

报告支持两种能力，可单独开启或同时开启（**至少启用其一** 方可开始分析）：

1. **规则检测**：基于预置规则对常见网络问题做快速扫描，例如高重传、异常连接行为等，不依赖云端 AI 即可得到结构化问题列表与统计摘要。
2. **AI 深度分析**：在规则检测与数据汇总的基础上，由云端 AI 对结果做校验、补充与深化描述，并生成 **Markdown 格式的网络问题分析报告**正文，便于运维或研发直接阅读与转发。

若开启 AI 分析但 **尚未登录** 云端 AI 服务，或 **AI 服务不可用**，分析仪将 **自动降级**：仍可根据规则检测结果生成报告，并在界面中提示本次未使用或未能完成 AI 部分的原因。AI 不可用或失败时，也可能使用基于规则的摘要作为报告正文的备选。

结果与导出

分析完成后，界面将展示检测到的问题、关键统计指标，以及 **网络问题分析报告**（含 AI 生成的 Markdown 章节，或在降级场景下的规则摘要）。用户可将报告 **导出为 Markdown 文件** 下载保存。

历史分析报告 列表用于快速打开近期生成的报告记录。请注意：历史记录默认保存在 **本机浏览器本地存储** 中，清除站点数据或更换浏览器后可能丢失，重要报告请及时下载备份。

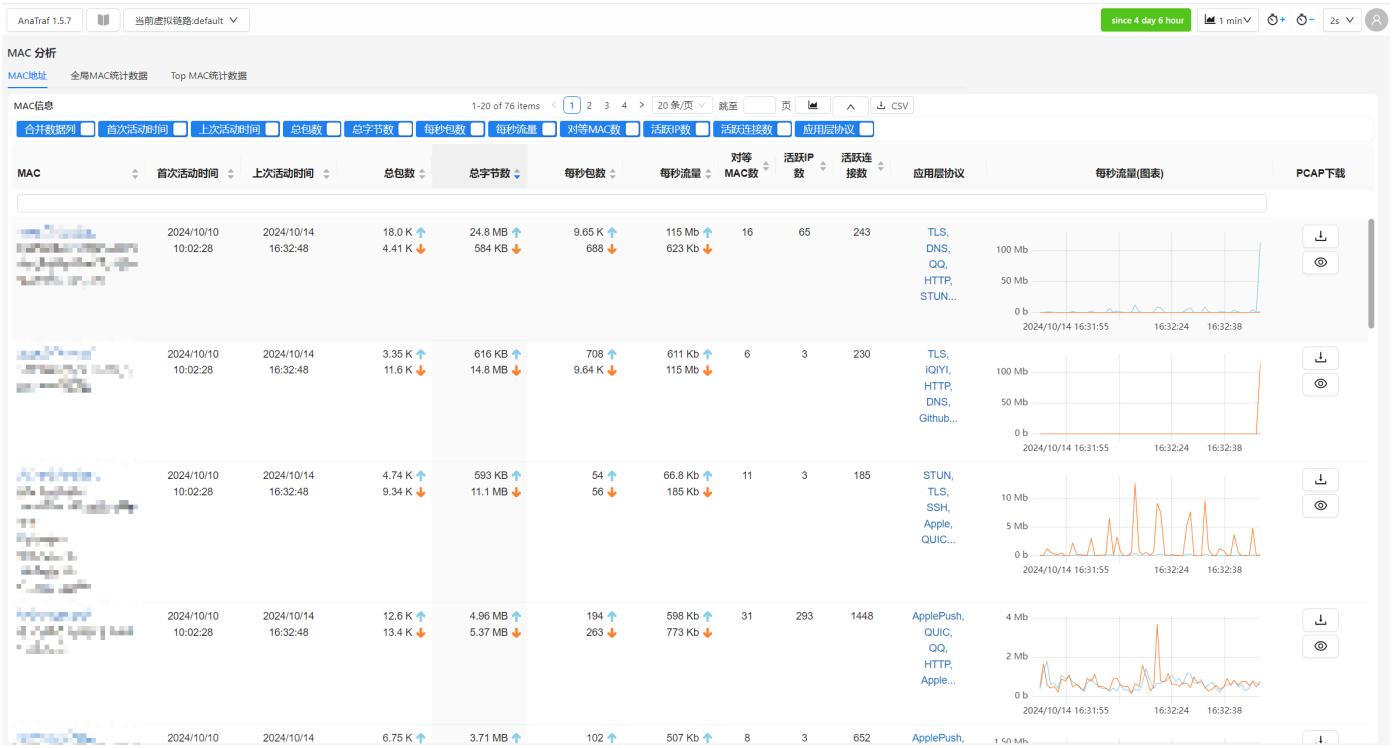
> **注意：**
>
> 1. 报告所依据的数据与统计口径与当前数据源（内存库 / 长期库）及所选时间范围一致，过短的时间窗口可能不足以暴露间歇性问题。
> 2. AI 生成的内容为辅助性解读，关键处置仍应结合现场拓扑、配置与原始统计、必要时配合 PCAP 与在线解码进一步核实。

8. L2 以太网

8.1 MAC

MAC 模块在网络协议栈的第二层上运行。在此模块，您可以查看AnaTraf 网络流量分析仪观测到的所有 MAC 地址的信息，包括：相应的网络流量、所使用的协议类型以及各自的流量、MAC Peer 对等点以及两个通信的 MAC 地址之间的流量。

8.1.1 MAC 信息表



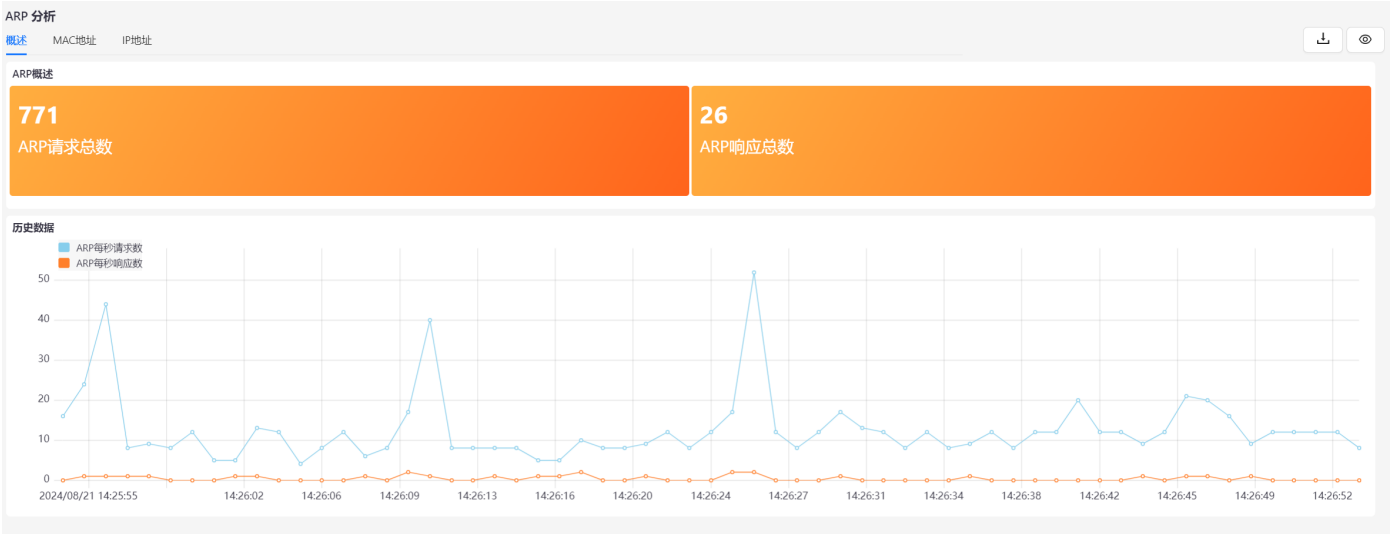
MAC 地址表展了分析仪观测到的所有 MAC 地址的信息。
包含的信息及其含义如下：

名称	描述
MAC 地址	被分析仪捕获到的 MAC 地址。点击该地址可跳转至该设备的详细信息页面
网卡供应商	根据 MAC 地址前缀（OUI）识别出的网卡制造商。例如 Intel、Apple 等。请注意，某些地址（如广播或多播地址）不属于任何特定供应商
DHCP 主机名	DHCP 名称是从 dhcp 请求中被动提取的。它可用于通过 DHCP 名称识别特定系统，例如打印机等
MAC	分析仪观测到的 MAC 地址，点击该地址可以访问该 MAC 地址的详细页面
第一次（最近活动时间）	该 MAC 地址首次出现在网络中的时间，反映该设备首次被监测到的时间点
上次活动时间	该 MAC 地址最近一次发送或接收数据的时间，反映设备当前是否仍活跃
总接收/发送包数	该 MAC 地址接收的总数据包数（红色箭头），发送的总数据包数（绿色箭头）
总接收/发送字节数	该 MAC 地址接收的总字节数（红色箭头），发送的总字节数（绿色箭头）
每秒接收/发送包数	该 MAC 地址每秒接收的数据包数（红色箭头），每秒发送的数据包数（绿色箭头）
每秒接收/发送流量	该 MAC 地址每秒接收的字节数（红色箭头），每秒发送的字节数（绿色箭头）
对等 MAC 数	与该 MAC 地址有过直接通信的其他 MAC 地址数量，用于衡量该设备在局域网中的连接广度
对等 IP 数	与该 MAC 地址关联的唯一 IP 地址数量。若此数值很大，可能代表该设备为 NAT 网关、路由器等
活跃连接数	当前该设备维持的活跃网络连接数量。可用于识别服务器、代理等高连接数设备
应用层协议	该设备所使用的所有 L7（应用层）协议类型，例如 HTTP、DNS、TLS 等，有助于了解设备用途及行为模式

8.2 ARP

ARP 模块在网络协议栈的第二层上运行，以跟踪各个 MAC 地址使用哪个 IP 地址。ARP 模块检测 ARP 请求和 ARP 响应，并建立所有已知的 MAC 地址和 IP 地址之间关联性的数据库。

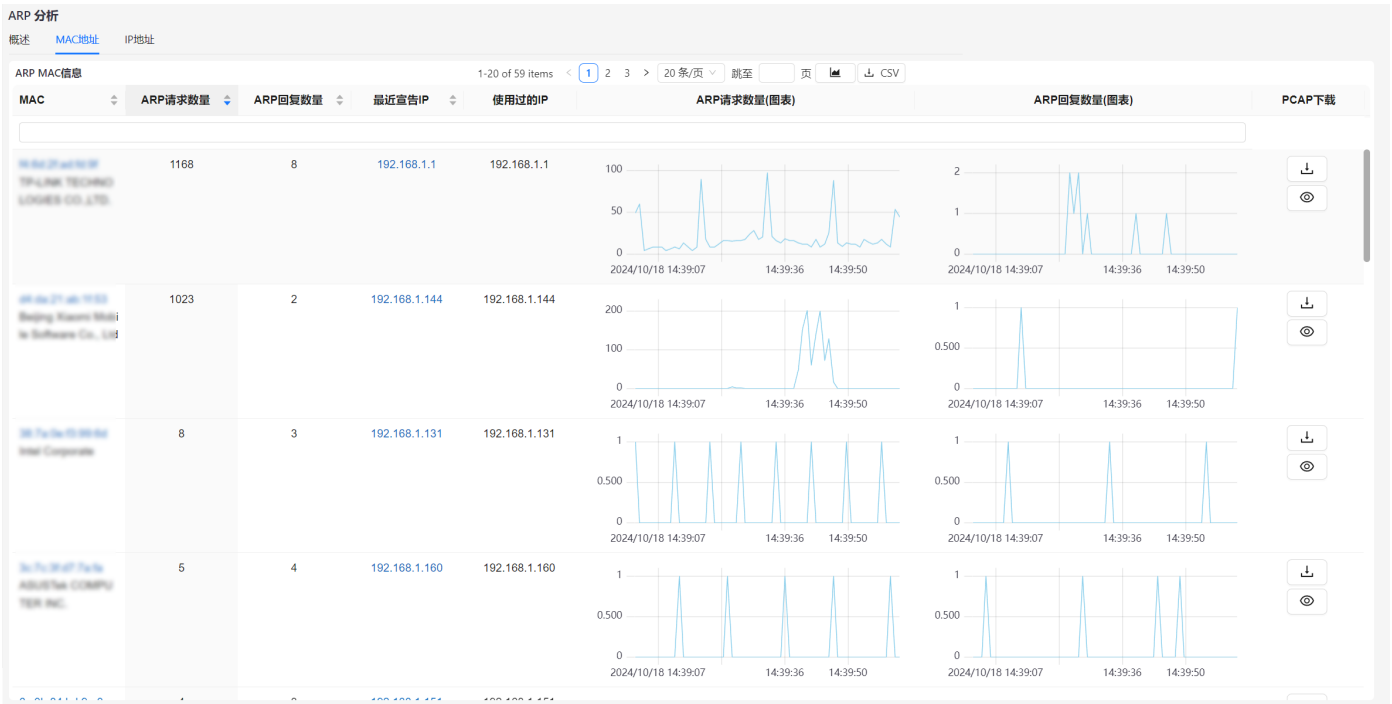
8.2.1 ARP 概述



ARP 概述部分显示了所有观测到的 ARP 请求的示数量以及响应的数量。

历史数据显示了 ARP 请求和响应数量的历史曲线图。

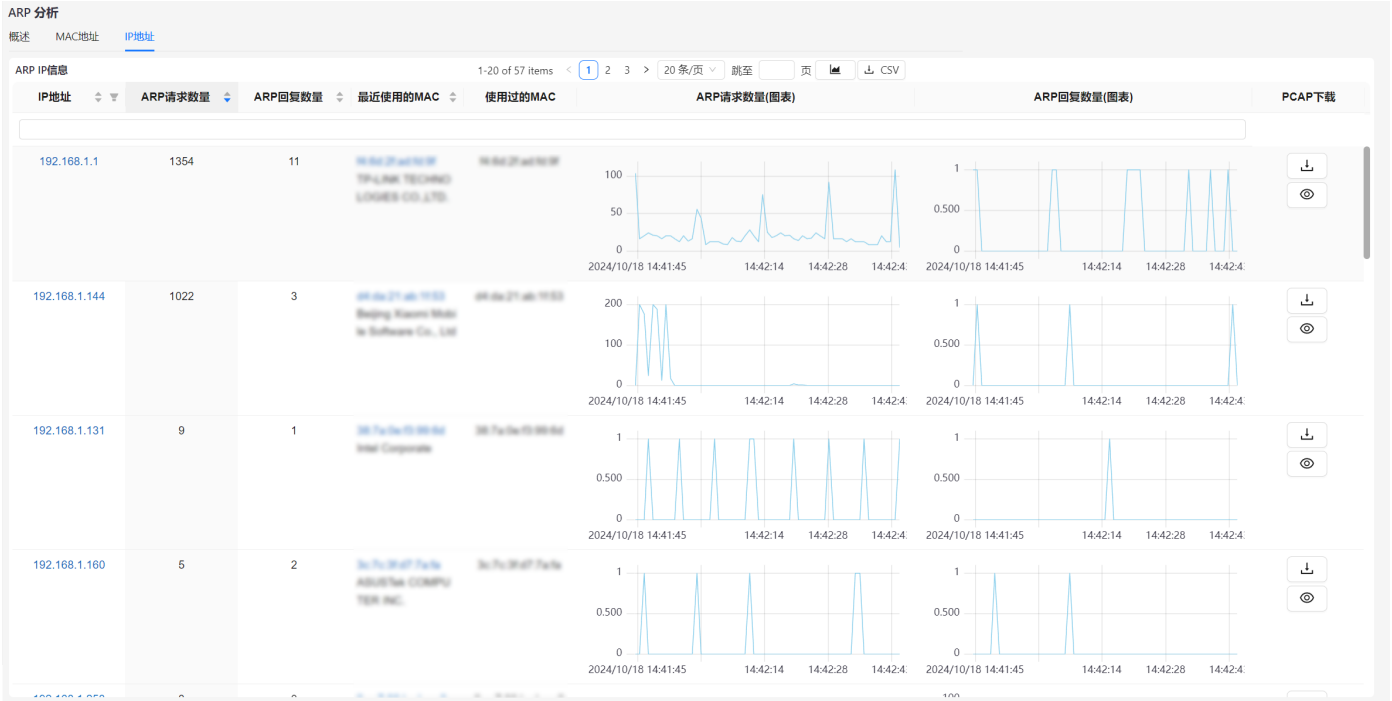
8.2.2 ARP - MAC 地址页



MAC 地址表显示了 MAC 地址最近宣告的 IP 地址、使用过的 IP 地址，以及 ARP 回复的数量。

名称	描述	参考意义
MAC 地址	点击该 MAC 地址可以访问该 MAC 地址的详细页面	-
ARP 回复数量	该 MAC 地址的 ARP 回复数量	-
最近宣告 IP	该 MAC 地址最近宣告的 IP 地址	-
使用过的 IP 地址	该 MAC 地址使用过的所有 IP 地址。当使用过多个 IP 地址时，按时间由近到远的顺序排列	如果出现多个 IP 地址，可能存在 IP 冲突的情况

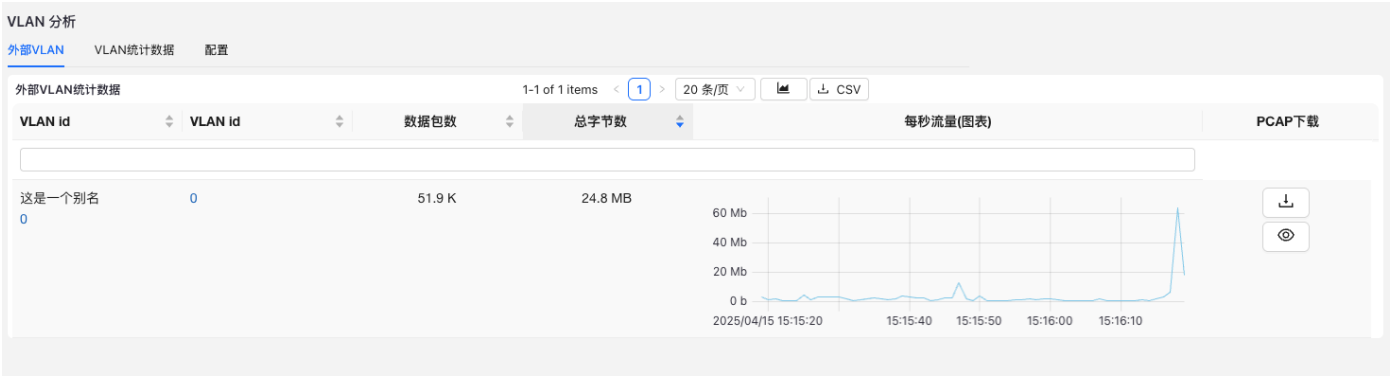
8.2.3 ARP - IP 地址页



IP 地址表展示的是 MAC 地址选项卡的相反方向，显示了 IP 地址最近使用的 MAC 地址、使用过的 MAC 地址，以及 ARP 回复的数量。

名称	描述	参考意义
IP 地址	点击该 IP 地址可以访问该 IP 地址的详细页面	-
ARP 回复数量	该 IP 地址的 ARP 回复数量	-
最近使用的 MAC 地址	该 IP 地址最近使用的 MAC 地址	-
使用过的 MAC 地址	该 IP 地址使用过的所有 MAC 地址。当使用过多个 MAC 地址时，按时间由近到远的顺序排列	如果出现多个 MAC 地址，可能存在 IP 冲突的情况

8.3 VLAN



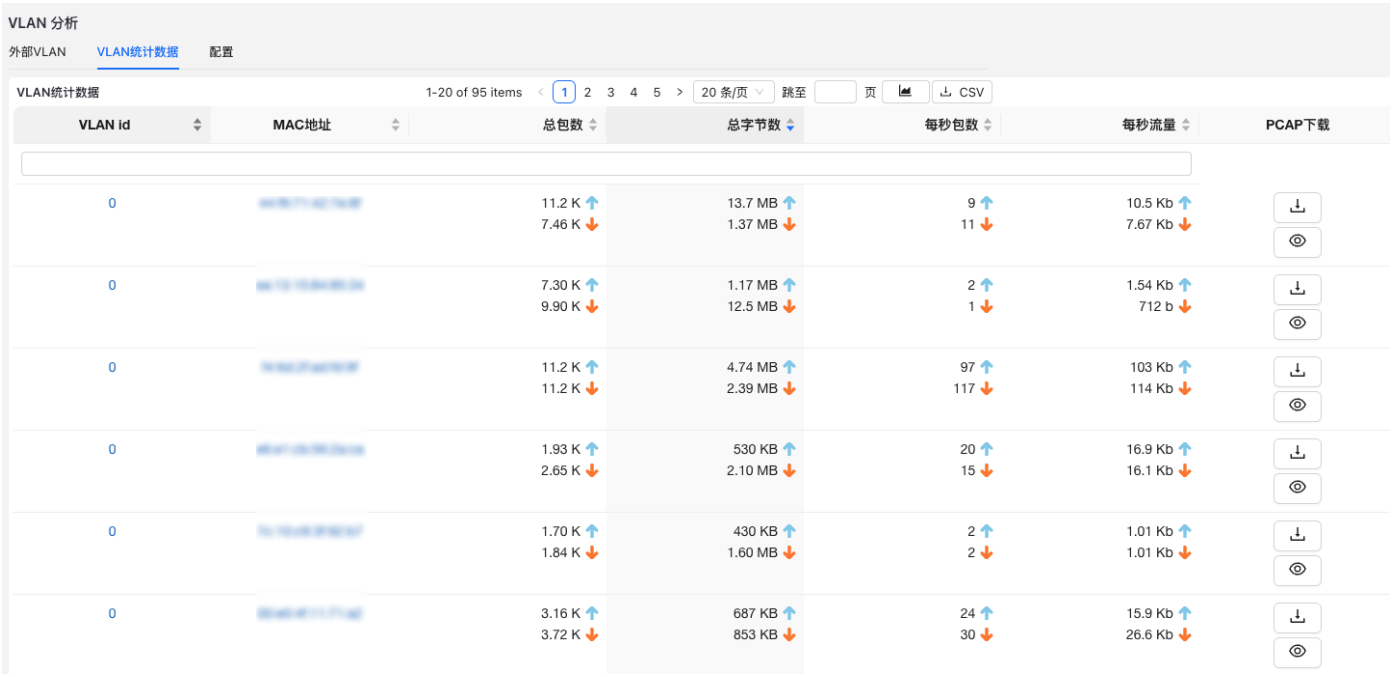
VLAN 模块显示了分析仪所有观测到的 VLAN 信息。该模块显示了观测到的每个 VLAN 的流量统计。

8.3.1 外部 VLAN 选项卡

该选项卡显示了每个 VLAN ID 的流量统计。

名称	描述
VLAN ID	分析仪观测到的 VLAN ID。点击该 VLAN ID 可访问该 VLAN ID 的详细信息页面
数据包数量	具有该 VLAN ID 的数据包总数
总字节数	具有该 VLAN ID 的流量的总字节数

8.3.2 VLAN 统计数据选项卡



该选项卡显示了每个 VLAN ID 以及 MAC 地址的流量统计。

名称	描述
VLAN ID	分析仪观测到的 VLAN ID。点击该 VLAN ID 可访问该 VLAN ID 的详细信息页面
MAC 地址	-
流量统计	-

8.3.2 VLAN 别名

此页面可以为 VLAN ID 设置自定义的备注名称。

可以通过**导出 CSV**按钮将当前 VLAN 别名配置导出。也可以通过**上传CSV**批量为 VLAN ID 设置别名。

CSV 文件的格式为：

```
VLAN ID 1、别名
VLAN ID 2、别名
VLAN ID 3、别名
```

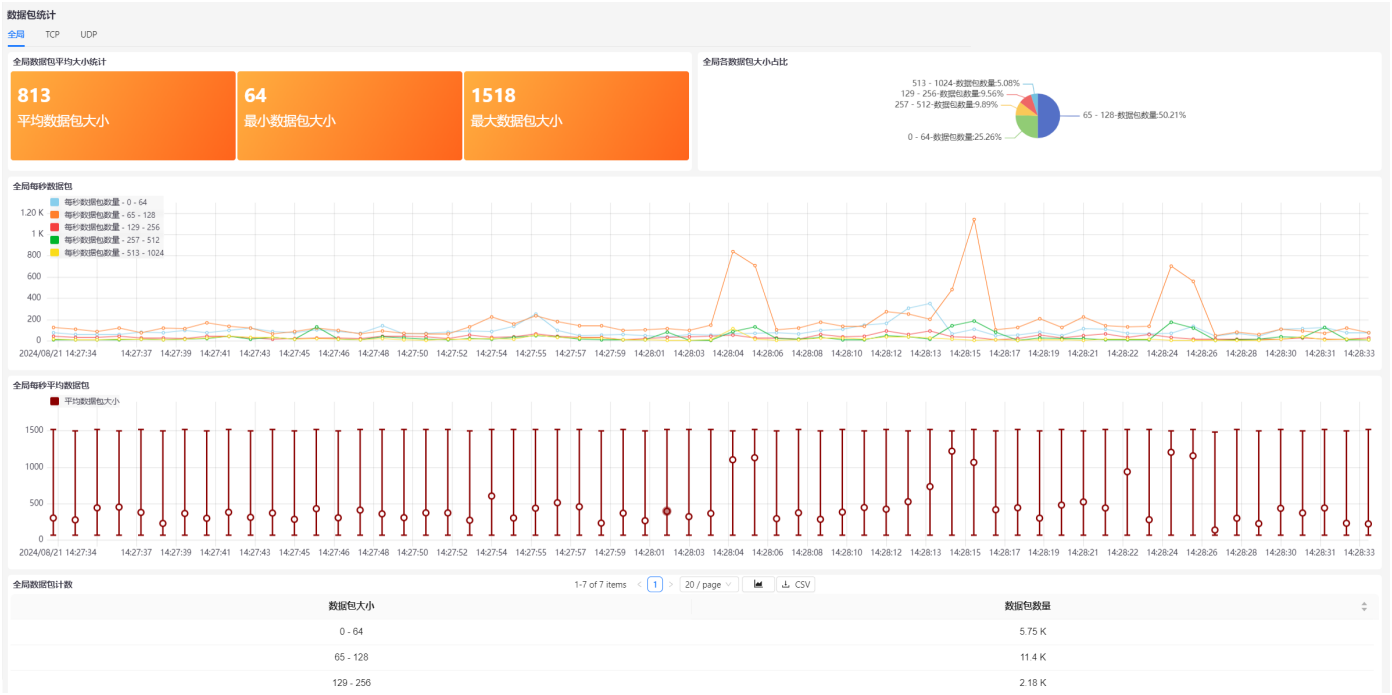
8.4 L2 QoS

二层 QoS提供 VLAN 各优先级的流量统计。

PCP	优先级	简称	描述
1	0（最低）	BK	背景流量
0	1（默认）	BE	尽力而为
2	2	EE	极大努力
3	3	CA	关键应用程序
4	4	VI	视频，< 100ms 延迟和抖动
5	5	VO	音频，<10 ms 延迟和抖动
6	6	IC	网间控制
7	7（最高）	NC	网络控制

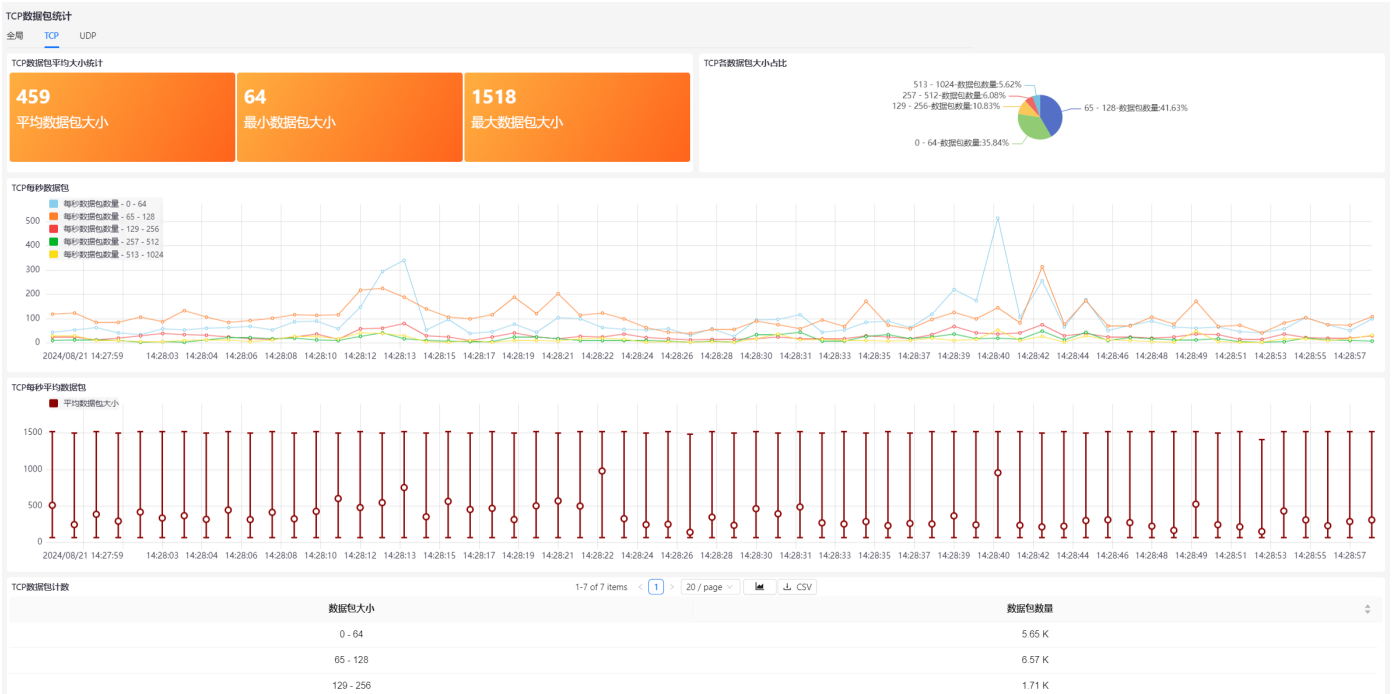
8.5 数据包大小统计

8.5.1 全局数据包统计



此页面显示了分析仪接收到的所有流量的数据包大小统计。提供最大 / 最小 / 平均数据包大小，以及不同大小的数据包的分布情况。

8.5.2 TCP 数据包大小统计

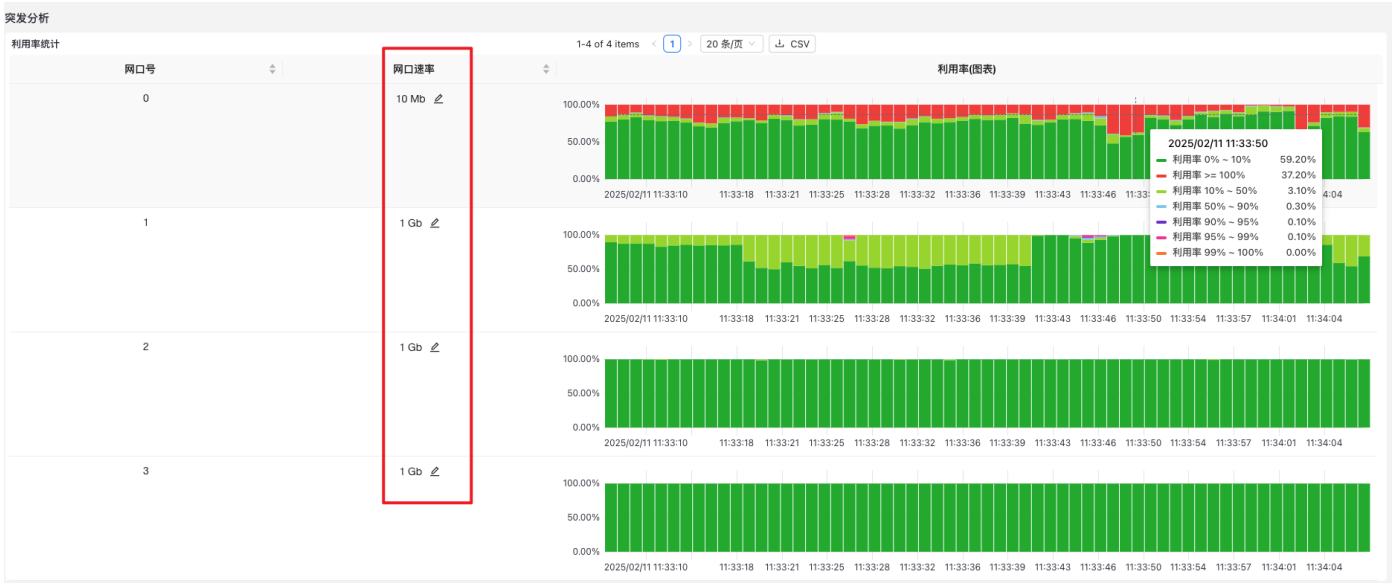


此页面显示了分析仪接收到的所有流量中，TCP 流量的数据包大小统计。提供最大 / 最小 / 平均数据包大小，以及不同大小的数据包的分布情况。

8.5.3 UDP 数据包大小统计

此页面显示了分析仪接收到的所有流量中，UDP 流量的数据包大小统计。提供最大 / 最小 / 平均数据包大小，以及不同大小的数据包的分布情况。

8.6 突发分析



突发分析模块以 1 ms 的时间间隔测量每个网口的利用率，并显示利用率的图表。

利用率的图表上显示：**“利用率 0% ~ 10%”**、**“利用率 10% ~ 50%”**、**“利用率 50% ~ 90%”**、**“利用率 90% ~ 95%”**、**“利用率 99% ~ 100%”**、**“利用率 >= 100%”**。

各利用率区间的值累加为 100%。如果 **“利用率 0% ~ 10%”** 的值为 95%，表示在一秒内，该网口在 95% 的测量间隔内的利用率为 0 ~ 10%。

点击 **网口速率列** 中的 **编辑** 按钮，可以设置网口的带宽，默认值为网口的连接速率。

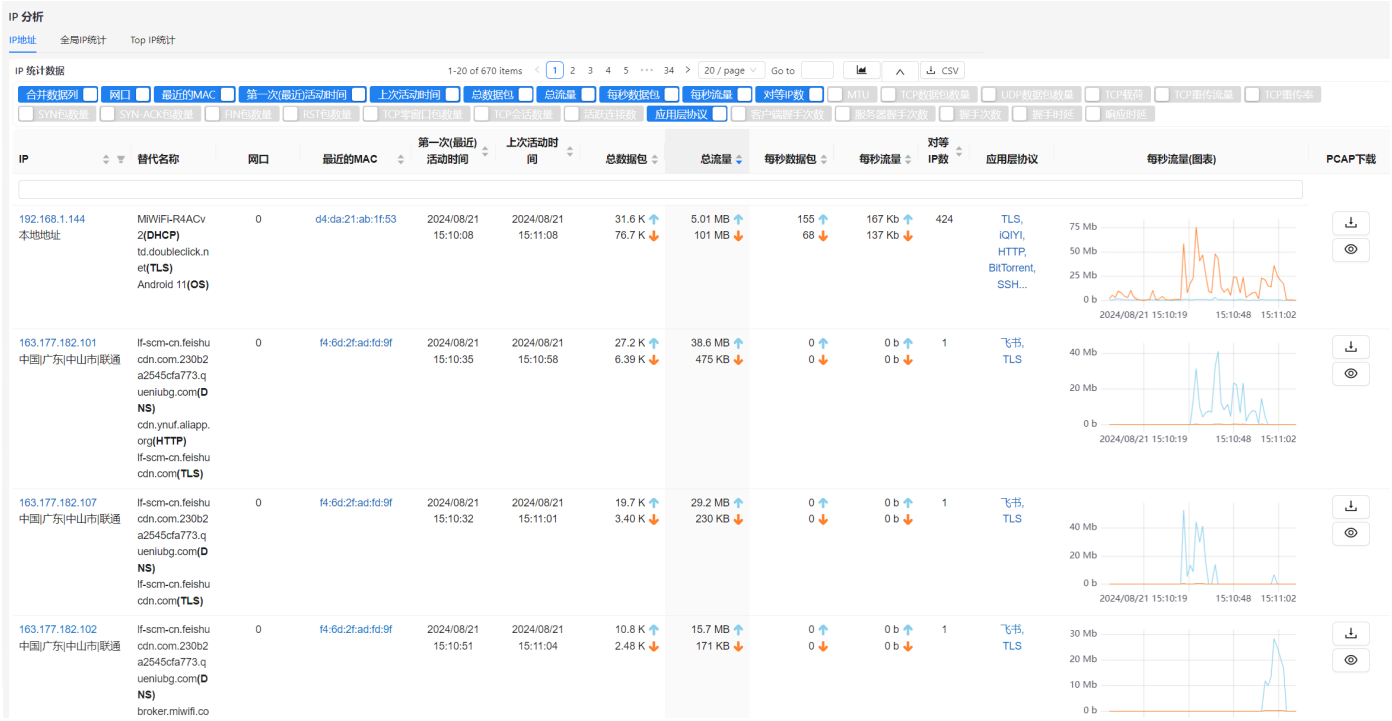
> **注意：** 设置的网口带宽只用于计算网口利用率，不改变网口的连接速率。例如，网口连接速率为 1Gbps，但实际链路的带宽为 100Mbps，可以在此设置网口的带宽，使网口利用率的计算更准确，反应真实的网络状况。

9. L3 IP

9.1 IP

IP 模块在网络协议栈的第三层上运行。它存储所有有关 IPv4 和 IPv6 地址的信息。对于每一个 IP 地址，都会计算相应的网络流量、所使用的协议类型及流量。互相通信的两个 IP 地址之间的流量都会存储，也可以每个连接的流量及其协议的详细信息。

9.1.1 IP 地址选项卡



IP 地址选项卡显示分析仪观测到的所有 IP 地址的信息表。该表包含以下信息：

名称	描述
IP 地址	分析仪观测到的 IP 地址，点击该地址可以访问该 IP 地址的详细页面
国家/地区	该 IP 地址所属的国家或地区
最近的MAC	该 IP 地址最近使用的 MAC 地址
首次活动时间	该 IP 地址第一次活动的时间
上次活动时间	该 IP 地址最后一次接收或发送数据包的时间
总接收 / 发送包数	该 IP 地址接收的总数据包数（红色箭头），发送的总数据包数（绿色箭头）
总接收 / 发送字节数	该 IP 地址接收的总字节数（红色箭头），发送的总字节数（绿色箭头）
每秒接收 / 发送包数	该 IP 地址接收的总字节数（红色箭头），发送的总字节数（绿色箭头）
	该 IP 地址每秒接收的字节数（红色箭头），每秒发送的字节数（绿色箭

每秒接收 / 发送字节数	头）
对等 IP 数	与该 IP 地址进行过通信的 IP 地址数量
上行 / 下行 MTU	上行 / 下行 MTU 大小
TCP 数据包数量	该 IP 地址传输的 TCP 数据包数量（如果是 TCP 通信）
UDP 数据包数量	该 IP 地址传输的 UDP 数据包数量（如果是 UDP 通信）
接收 / 发送 TCP 载荷	该 IP 地址接收 / 发送的 TCP 载荷（如果是 TCP 通信）
接收 / 发送 TCP 重传流量	该 IP 地址接收 / 发送的 TCP 重传流量（如果是 TCP 通信）
接收 / 发送 SYN 包数量	该 IP 地址接收 / 发送的 TCP SYN 包数量（如果是 TCP 通信）
接收 / 发送 SYN-ACK 包数量	该 IP 地址接收 / 发送的 TCP SYN-ACK 包数量（如果是 TCP 通信）
接收 / 发送 FIN 包数量	该 IP 地址接收 / 发送的 TCP FIN 包数量（如果是 TCP 通信）
接收 / 发送 RST 包数量	该 IP 地址接收 / 发送的 TCP RST 包数量（如果是 TCP 通信）
接收 / 发送 TCP 零窗口包数量	该 IP 地址接收 / 发送的 TCP 零窗口包数量（如果是 TCP 通信）
TCP 会话数量	该 IP 地址建立的 TCP 会话数量
活跃连接数	该 IP 地址活跃的连接数量
应用层协议	该 IP 地址观测到的应用层协议
客户端握手次数	表示有第二次握手（SYN-ACK）和第三次握手（ACK）的次数
服务器握手次数	表示有第一次握手（SYN）和第二次握手（SYN-ACK）的次数
握手次数	该 IP 的客户端握手次数和服务器握手次数之和
客户端握手平均时延	该 IP 的客户端握手平均时延
服务器握手平均时延	该 IP 的服务器握手平均时延
握手平均时延	该 IP 的握手平均时延
响应次数	该 IP 的 TCP 响应次数
平均响应时延	该 IP 的 TCP 平均响应时延
网口	观测到该 IP 地址的网口

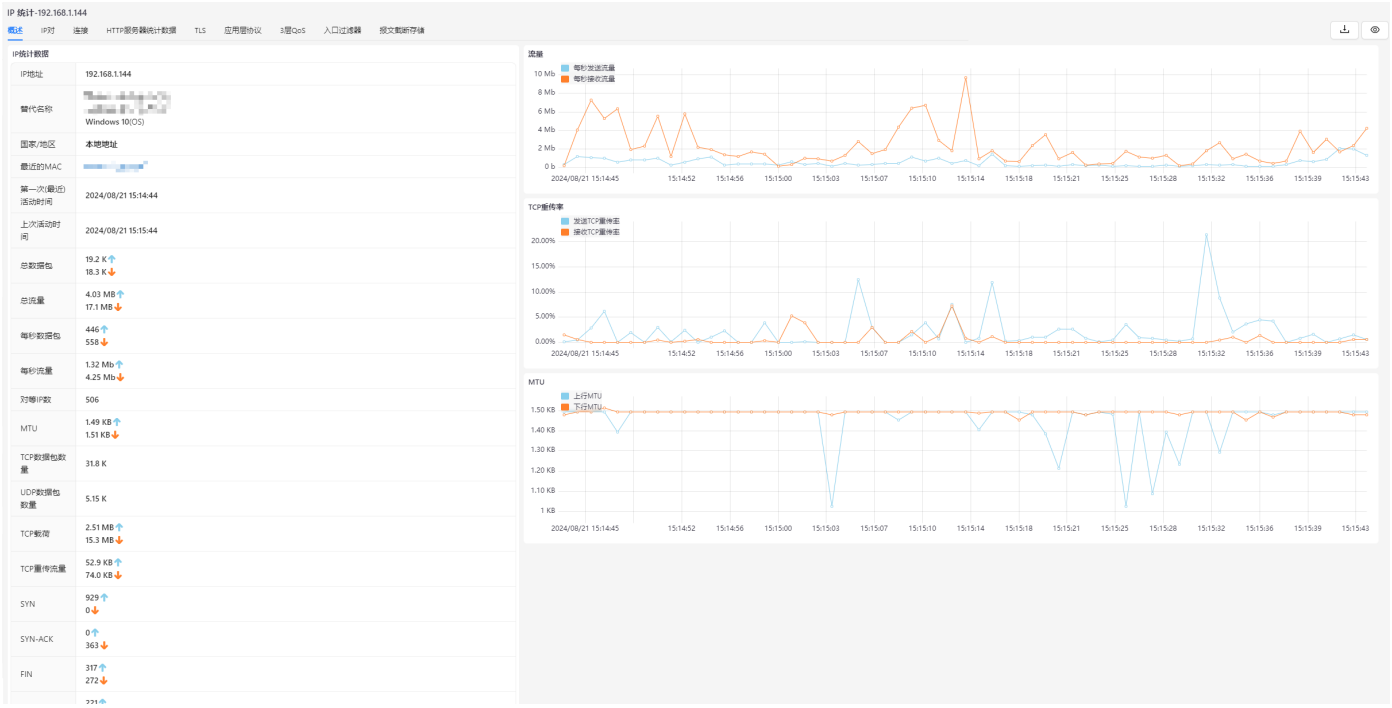
9.1.2 TOP IP 统计

此页面上的饼图显示了接收 / 发送流量最多的 10 个 IP 地址。

9.2 IP 详细页面

IP 详细页面显示了特定一个 IP 地址的流量分析结果。

9.2.1 概述选项卡



概述选项卡总结了 IP 的统计数据，包括：

名称	描述
MAC地址	点击该 MAC 地址可以访问该 MAC 地址的详细页面
活跃时间	首次活动时间，上次活动时间
流量统计	基本的流量统计，数据包数，字节数，每秒数据包和每秒流量
传输层统计	TCP 数据包数量、UDP 数据包数量、TCP 标志位统计等
应用层协议	该 IP 使用过的应用层协议

9.2.3 Peers 选项卡

显示了与当前 IP 地址通信的所有对等 IP 地址，并提供二者的流量统计。

9.2.4 Connections 选项卡

在连接选项卡，显示了涉及当前 IP 的所有连接及流量统计。

包含的统计项及描述可参考 L4 连接模块

9.2.5 HTTP server statistics 选项卡

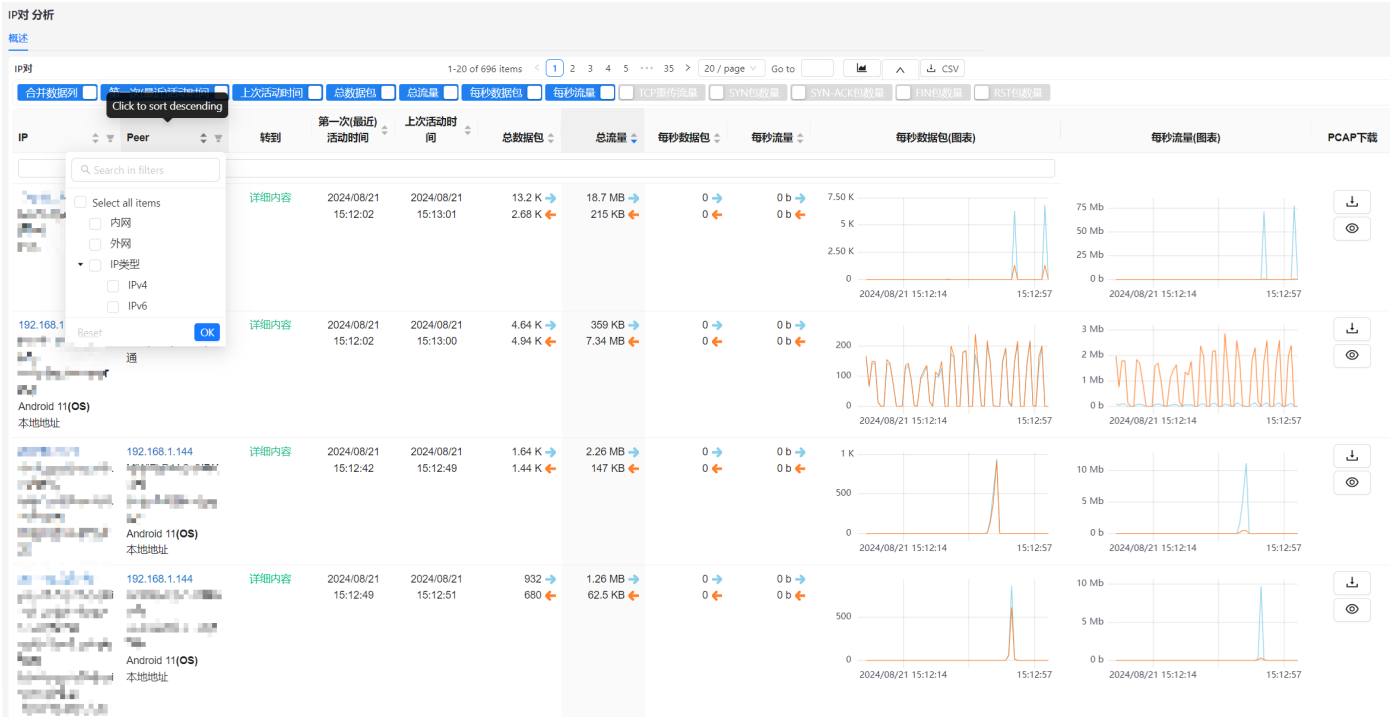
此选项卡显示了当前 IP 地址作为 HTTP 服务器处理的 HTTP 请求信息。

名称	描述	参考意义
IP 地址	IP 地址	-
主机名	主机名	-
请求数量	该 HTTP 服务器处理的请求数量	-
国家 / 地区	IP 地址所在的国家或地区	-
最小 / 平均 / 最大响应耗时	根据观测到的该 HTTP 服务器所有 HTTP 响应计算的最小 / 平均 / 最大响应时间	高响应时间可能表明服务器端处理请求速度慢，可能由于服务器负载高、程序设计问题、数据库查询时间过长等原因造成
1xx(信息)响应数量	该 HTTP 服务器 1xx(信息)响应数量	通常被视为正常情况的一部分，因为它们并不表示故障或错误
2xx(成功)响应数量	该 HTTP 服务器 2xx(成功)响应数量	-
3xx(重定向)响应数量	该 HTTP 服务器 3xx(重定向)响应数量	请求的资源已被移动到不同的位置或者临时不可用，需要客户端采取额外的步骤来完成请求
4xx(客户端错误)响应数量	该 HTTP 服务器 4xx(客户端错误)响应数量	表示客户端错误，提供了关于请求失败的详细信息
5xx(服务器错误)响应数量	该 HTTP 服务器 5xx(服务器错误)响应数量	表示服务器在尝试处理客户端请求时发生了问题

9.2.6 应用层协议选项卡

名称	描述
协议（应用）名	识别到的 L7 应用层协议名
首次活动时间	该协议第一次活动时间
上次活动时间	该协议最近一次活动时间
总数据包	分析仪观测到的该协议的总数据包个数
总流量	分析仪观测到的该协议的总字节数
每秒数据包	该协议每秒数据包数
每秒流量	该协议每秒字节数

9.3 IP Pairs



IP Pairs 模块显示了所有 IP 对之间的流量统计信息。

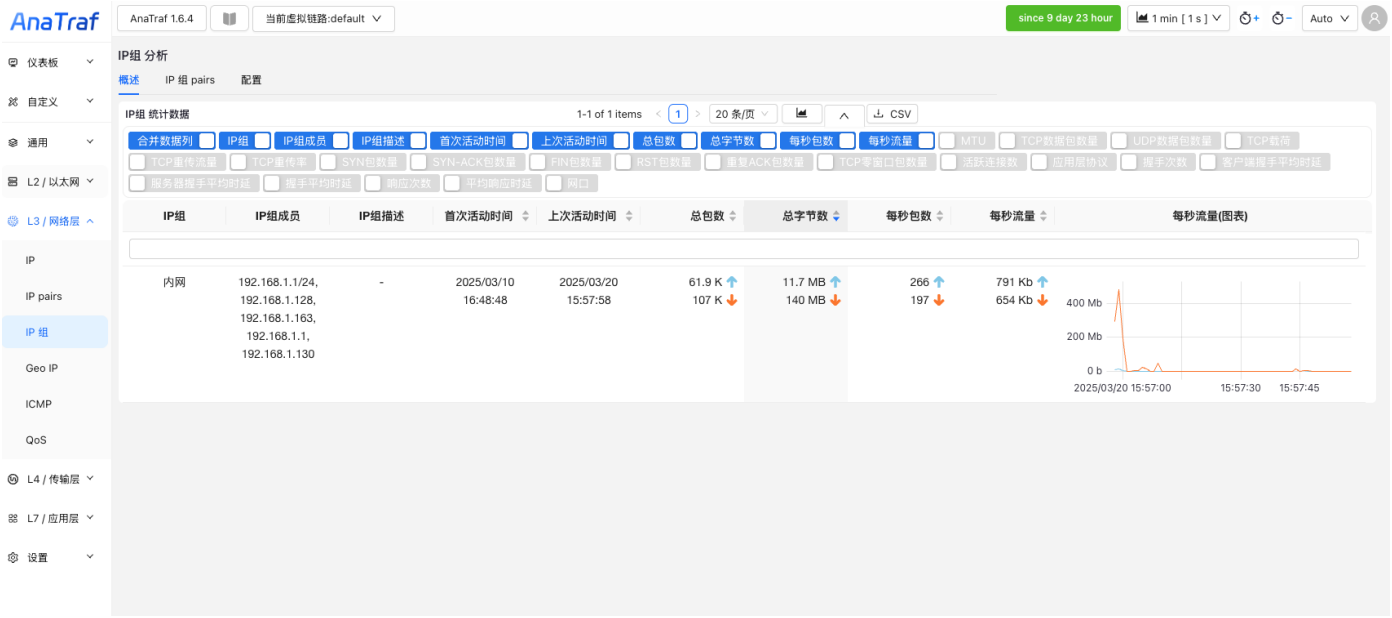
IP Pairs 表包含如下内容：

名称	描述
IP 地址	分析仪观测到的该 IP Pair的第一个报文的源 IP 地址，其目的 IP 地址为对等 IP 地址
对等 IP	参照 IP 地址解释
首次活动时间	该 IP Pair 第一次活动的时间
上次活动时间	该 IP Pair 最后一次接收或发送数据包的时间
上行总包数	该 IP Pair 上行（IP 地址向对等 IP）方向的总数据包数量
下行总包数	该 IP Pair 下行（对等 IP 向 IP 地址）方向的总数据包数量
上行总字节数	该 IP Pair 上行（IP 地址向对等 IP）方向的总字节数量
下行总字节数	该 IP Pair 下行（对等 IP 向 IP 地址）方向的总字节数量
TCP 重传流量	该 IP Pair 的 TCP 重传的总字节数（如果是 TCP 通信）
SYN 包数量	该 IP Pair 的 TCP SYN 标志的数据包数量（如果是 TCP 通信）
SYN-ACK 包数量	该 IP Pair 的 TCP SYN-ACK 标志的数据包数量（如果是 TCP 通信）
FIN 包数量	该 IP Pair 的 TCP FIN 标志的数据包数量（如果是 TCP 通信）
RST 包数量	该 IP Pair 的 TCP RST 标志的数据包数量（如果是 TCP 通信）

9.4 IP Group

IP Group 功能可以将任何 IP、IP 网段配置成一个 IP 组，对 IP 组的流量进行统计分析。多个 IP 组可以重叠，一个 IP 地址可以在多个 IP 组内。

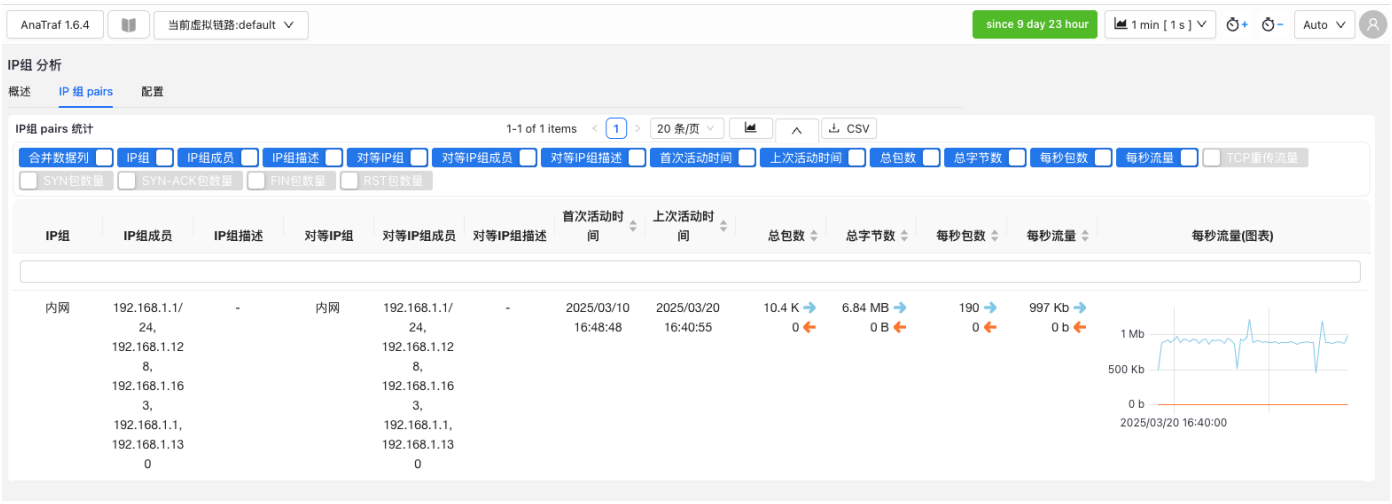
9.4 IP Group 概述



名称	描述
IP 组	-
IP 组成员	-
IP 组描述	-
首次活动时间	-
上次活动时间	-
接收 / 发送包数	-
接收 / 发送字节数	-
每秒接收 / 发送包数	-
接收 / 发送速率	-
上行 / 下行 MTU	上行 / 下行 MTU 大小
TCP 数据包数量	该 IP 组传输的 TCP 数据包数量（如果是 TCP 通信）
UDP 数据包数量	该 IP 组传输的 UDP 数据包数量（如果是 UDP 通信）
接收 / 发送 TCP 载荷	该 IP 组接收 / 发送的 TCP 载荷（如果是 TCP 通信）
接收 / 发送 TCP 重传流量	该 IP 组接收 / 发送的 TCP 重传流量（如果是 TCP 通信）

接收 / 发送 SYN 包数量	该 IP 组接收 / 发送的 TCP SYN 包数量（如果是 TCP 通信）
接收 / 发送 SYN-ACK 包数量	该 IP 组接收 / 发送的 TCP SYN-ACK 包数量（如果是 TCP 通信）
接收 / 发送 FIN 包数量	该 IP 组接收 / 发送的 TCP FIN 包数量（如果是 TCP 通信）
接收 / 发送 RST 包数量	该 IP 组接收 / 发送的 TCP RST 包数量（如果是 TCP 通信）
接收 / 发送 TCP 零窗口包数量	该 IP 组接收 / 发送的 TCP 零窗口包数量（如果是 TCP 通信）
TCP 会话数量	该 IP 组建立的 TCP 会话数量
活跃连接数	该 IP 组活跃的连接数量
应用层协议	该 IP 组观测到的应用层协议
客户端握手次数	表示有第二次握手（SYN-ACK）和第三次握手（ACK）的次数
服务器握手次数	表示有第一次握手（SYN）和第二次握手（SYN-ACK）的次数
握手次数	该 IP 组内的 IP 客户端握手次数和服务器握手次数之和
客户端握手平均时延	该 IP 组内的 IP 的客户端握手平均时延
服务器握手平均时延	该 IP 组内的 IP 的服务器握手平均时延
握手平均时延	该 IP 组内的 IP 的握手平均时延
响应次数	该 IP 组内的 IP 的 TCP 响应次数
平均响应时延	该 IP 组内的 IP 的 TCP 平均响应时延
网口	观测到该 IP 组的网口

9.4 IP Group Pairs

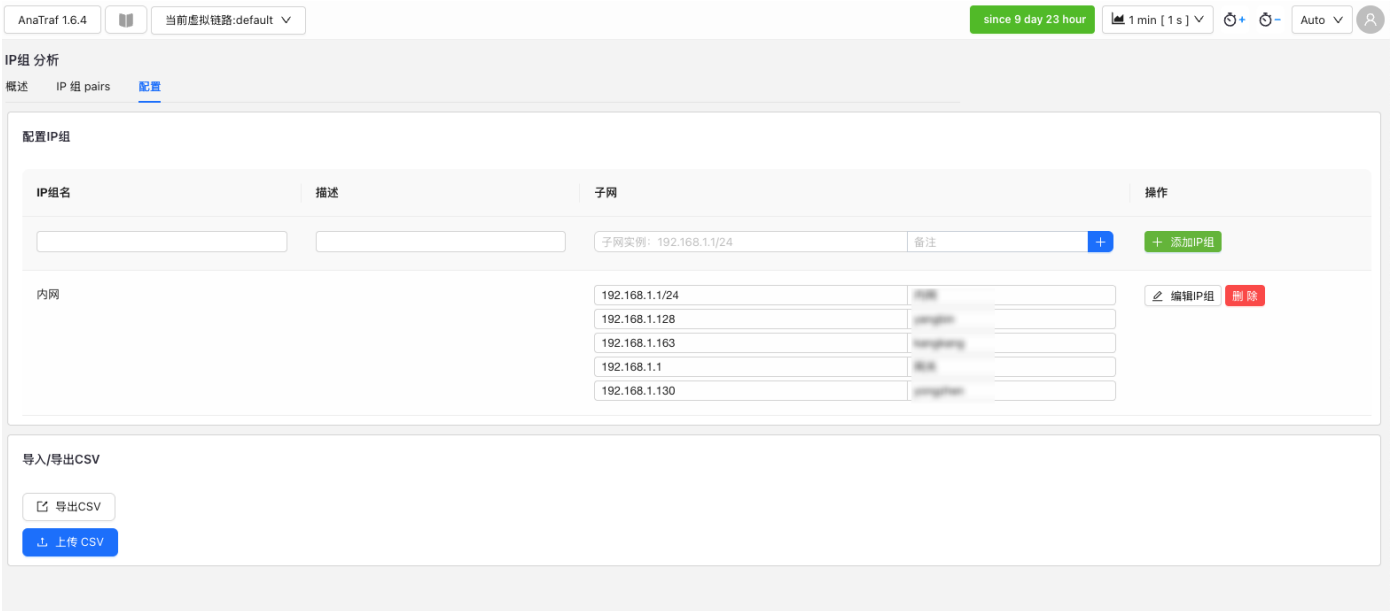


此选项卡显示 IP 组之间的流量统计。

IP Group Pairs 表包含如下内容：

名称	描述
IP 组	-
IP 组描述	-
对等 IP 组	-
对等 IP 组描述	-
首次活动时间	该 IP Group Pair 第一次活动的时间
上次活动时间	该 IP Group Pair 最后一次接收或发送数据包的时间
上行总包数	该 IP Group Pair 上行（IP 地址向对等 IP）方向的总数据包数量
下行总包数	该 IP Group Pair 下行（对等 IP 向 IP 地址）方向的总数据包数量
上行总字节数	该 IP Group Pair 上行（IP 地址向对等 IP）方向的总字节数量
下行总字节数	该 IP Group Pair 下行（对等 IP 向 IP 地址）方向的总字节数量
TCP 重传流量	该 IP Group Pair 的 TCP 重传的总字节数（如果是 TCP 通信）
SYN 包数量	该 IP Group Pair 的 TCP SYN 标志的数据包数量（如果是 TCP 通信）
SYN-ACK 包数量	该 IP Group Pair 的 TCP SYN-ACK 标志的数据包数量（如果是 TCP 通信）
FIN 包数量	该 IP Group Pair 的 TCP FIN 标志的数据包数量（如果是 TCP 通信）
RST 包数量	该 IP Group Pair 的 TCP RST 标志的数据包数量（如果是 TCP 通信）

9.4 IP Group 配置



可以在此选项卡配置 IP 组。

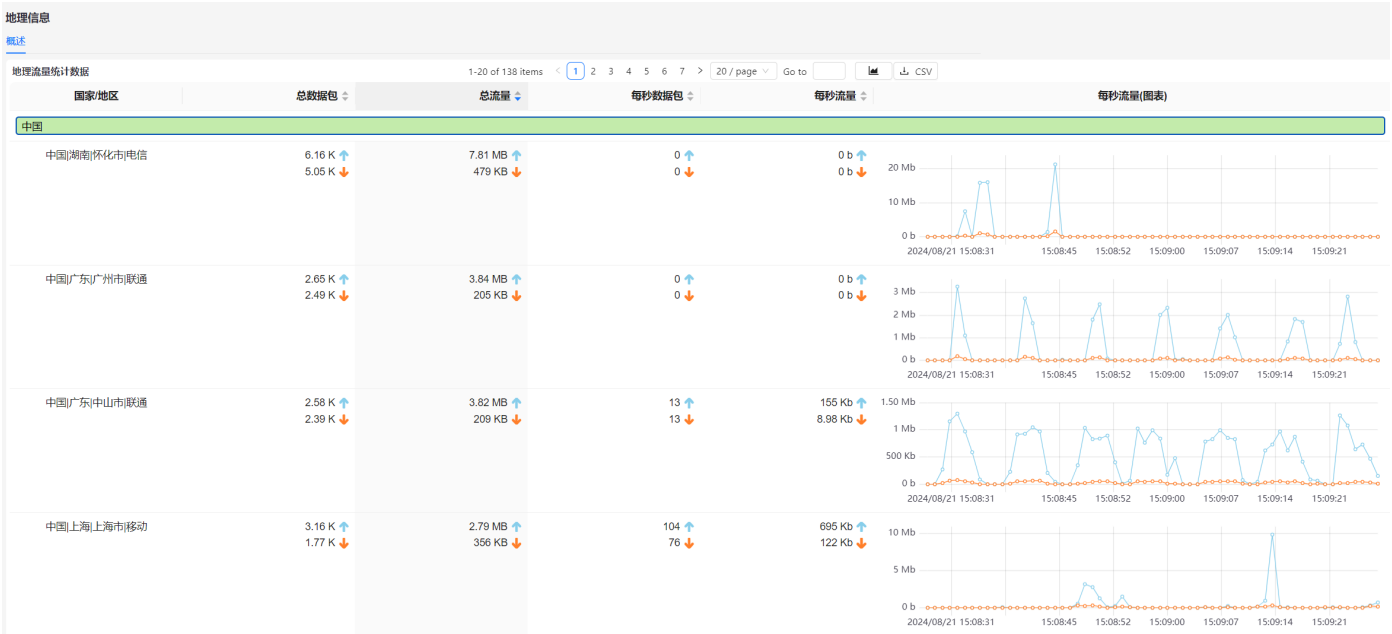
导出 CSV 可以将分析仪当前的 IP 组配置以及 IP 别名配置导出 CSV 表格，可用于梳理网络资产。

导入 CSV 可以上传一个 CSV 文件来配置 IP 组。

CSV 文件的格式为：

```
IP1、组1、IP 别名
IP2、组1、IP 别名
IP3、组2、IP 别名
```

9.5 GEO IP

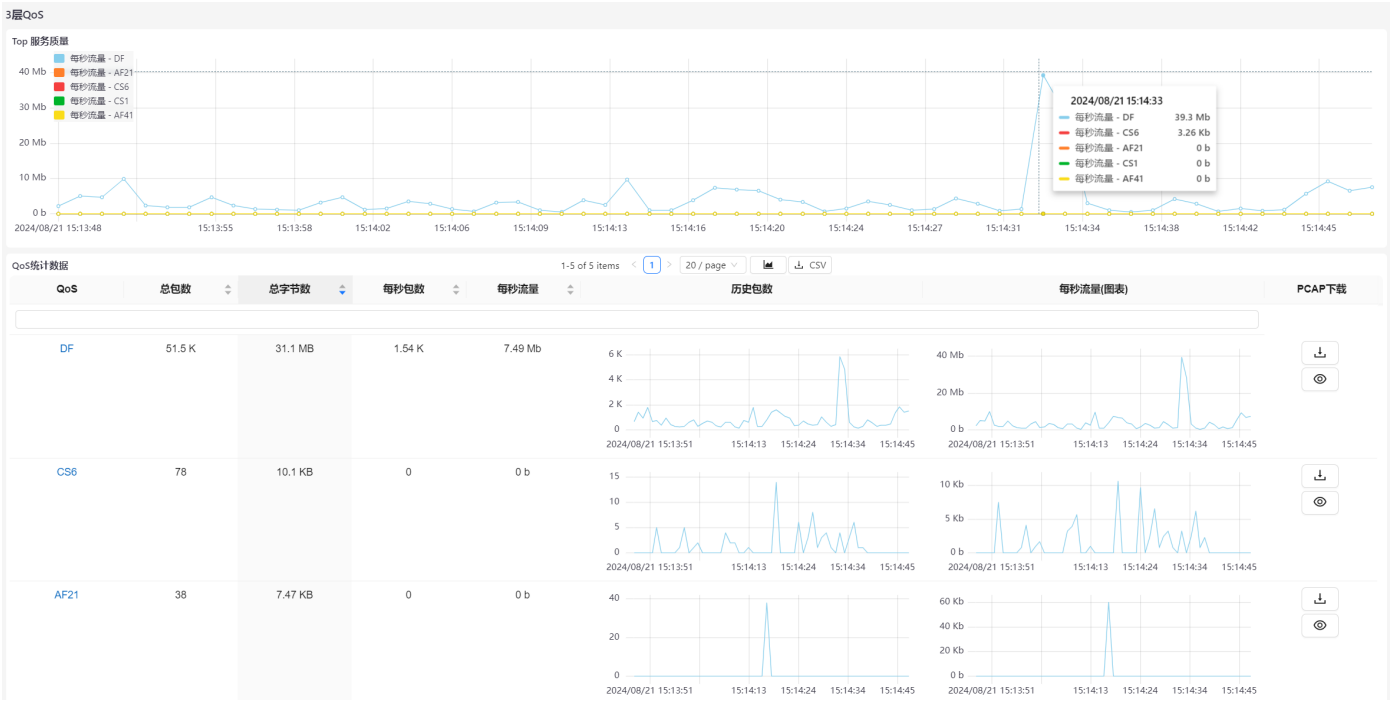


IP Geolcation 模块使用 GeoIP 库来识别 IP 地址所在的国家或地区。

IP 地理位置统计表显示了不同国家或地区的流量统计。

名称	描述
国家 / 地区	IP 地址所在的国家或地区
总收/发包数	该国家 / 地区接收的总数据包数（红色箭头），发送的总数据包数（绿色箭头）
总接收/发送字节数	该国家 / 地区接收的总字节数（红色箭头），发送的总字节数（绿色箭头）
每秒收/发包数	该国家 / 地区每秒接收的数据包数（红色箭头），每秒发送的数据包数（绿色箭头）
每秒接收/发送流量	该国家 / 地区每秒接收的字节数（红色箭头），每秒发送的字节数（绿色箭头）
每秒上下行流量	显示该国家 / 地区每秒上下行流量随时间变化的历史曲线

9.6 L3 QoS



L3 QoS 提供各差分服务编码点（Differentiated Services Codepoint）的流量统计。

典型的业务类型定义如下表：

业务类型	DSCP 名	DSCP 值
Network Control	CS6	48
Telephony	EF	46
Voice Admit	VOICE-ADMIT	44
Signaling	CS5	40
Multimedia Conferencing	AF41, AF42, AF43	34, 36, 38
Real-Time Interactive	CS4	32
Multimedia Streaming	AF31, AF32, AF33	26, 28, 30
Broadcast Video	CS3	24
Low-Latency Data	AF21, AF22, AF23	18, 20, 22
OAM	CS2	16
High-Throughput Data	AF11, AF12, AF13	10, 12, 14
Standard	DF (CS0)	0
Low-Priority Data	CS1	8

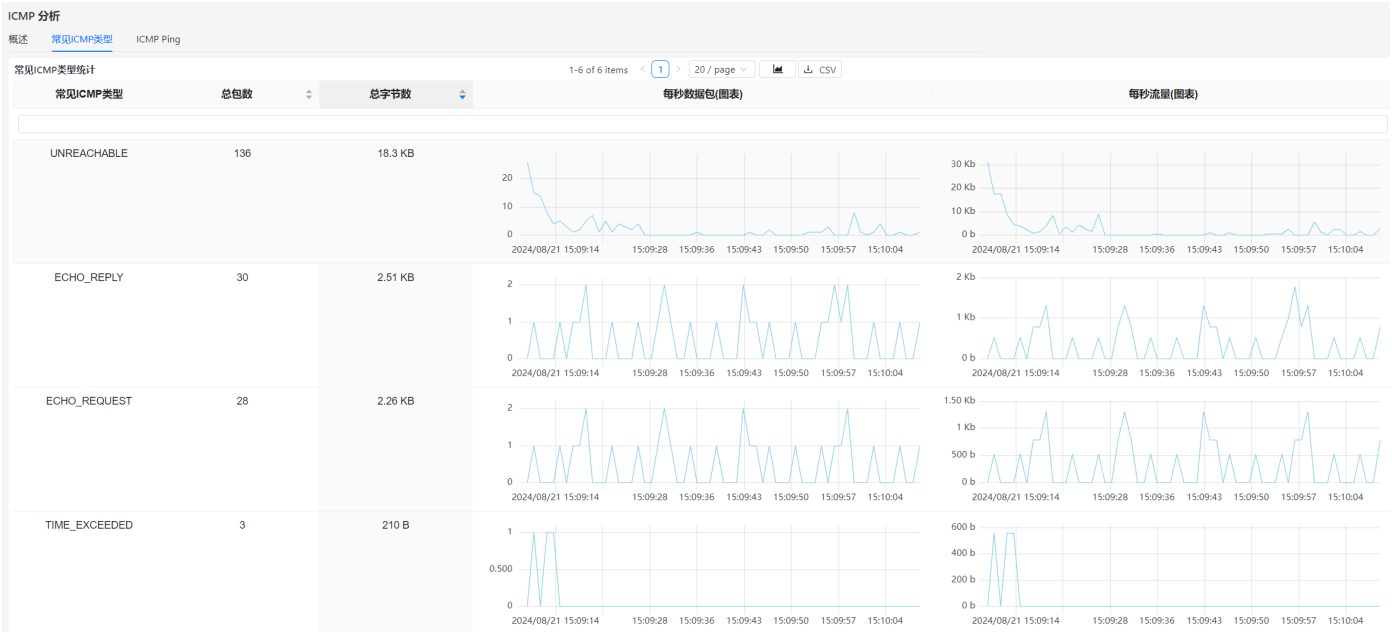
9.7 ICMP

ICMP 模块处理分析仪观测到的 ICMP 流量。

9.7.1 概述

概述选项卡显示了一段时间内分析仪观测到的 ICMP 报文数量及总字节大小，并提供每秒流量和每秒数据包的历史曲线图。

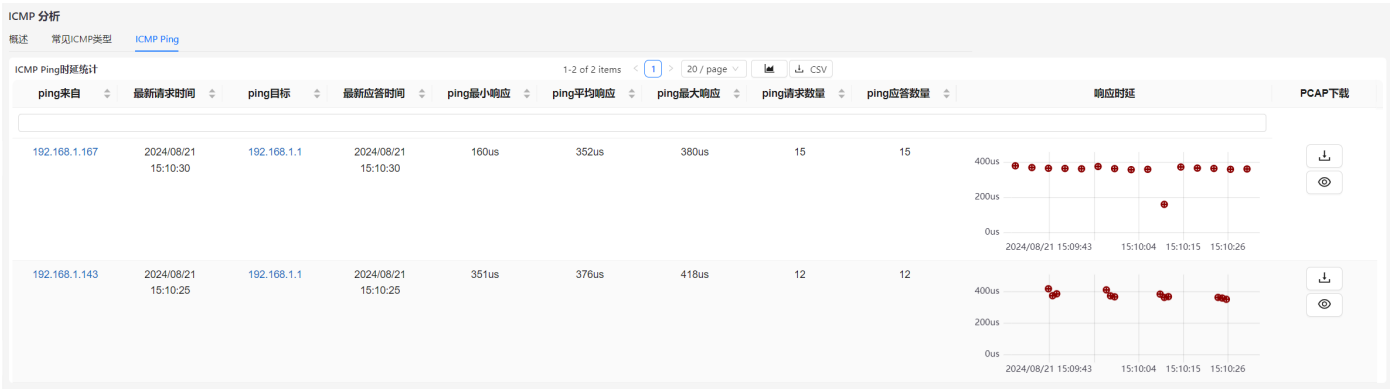
9.7.2 常见 ICMP 类型



常见 ICMP 类型选项卡显示了分析仪观测到的所有 ICMP 类型的流量统计。

名称	描述
TIME_EXCEEDED	数据包在传输过程中因为存活时间（TTL）耗尽或者片段重新组装失败而被丢弃
ECHO_REPLY	目标设备收到Echo Request后返回的响应，包含有关延迟和可达性的信息
ECHO_REQUEST	用于Ping命令，发送给目标设备以测试网络连接是否可达
TIMESTAMP_REPLY	目标设备返回的时间戳响应
TIMESTAMP_REQUEST	请求目标设备返回当前时间戳
UNREACHABLE	数据包未能到达目标，通常由于网络路径问题、目标端口未打开或者防火墙阻止等原因引起

9.7.3 ICMP Ping



ICMP Ping 选项卡显示分析仪观测到的所有 ping 信息。

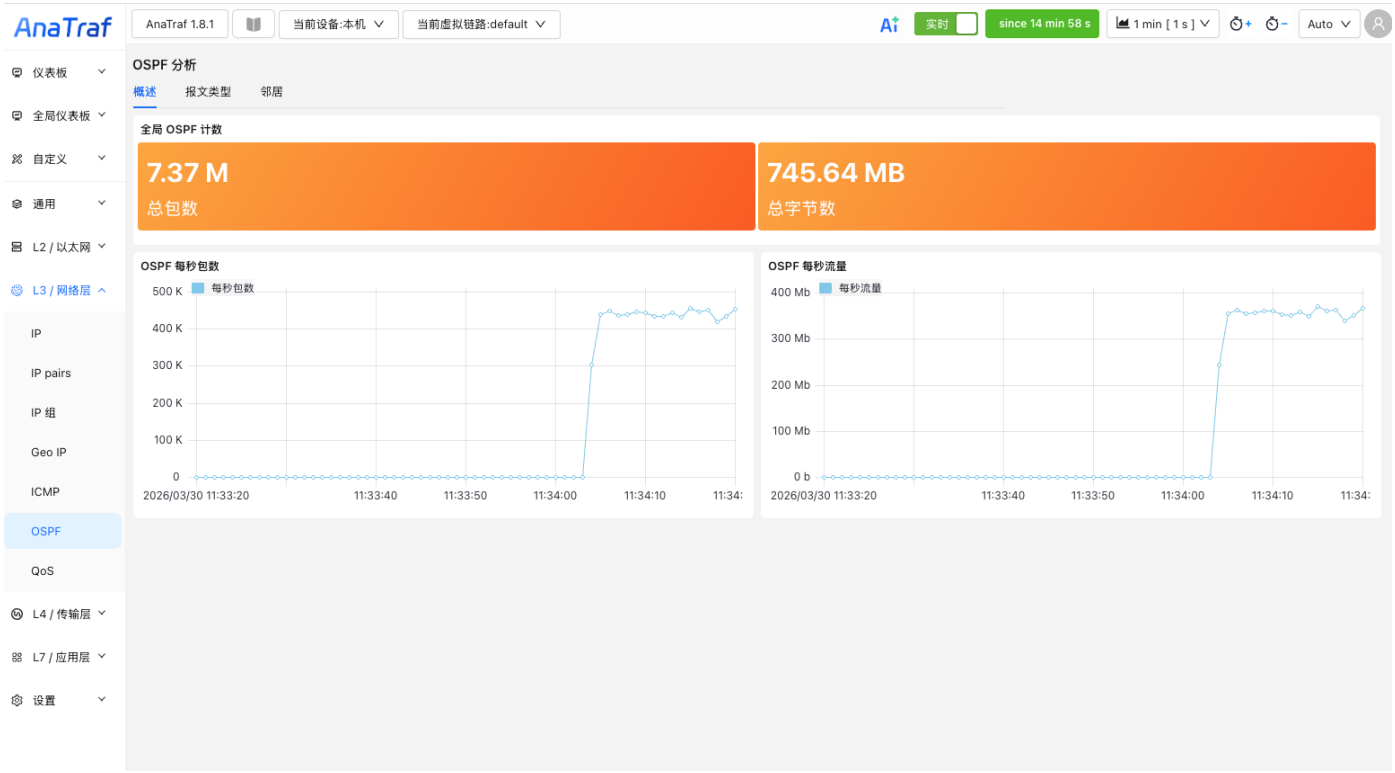
名称	描述
ping 来自	源 IP 地址
最新请求时间	ping 请求时间
ping 目标	目的 IP 地址
最新应答时间	最新应答时间
最小 / 平均 / 最大响应	ping 的最小 / 平均 / 最大响应时间
请求 / 应答数量	ping 请求和应答数量

9.8 OSPF

OSPF（Open Shortest Path First）分析模块对镜像或串联链路上的 OSPF 报文进行解析与统计，用于观察路由协议流量规模、报文构成以及邻居关系与健康度。左侧导航 **L3** 下进入 **OSPF**，包含 **概述**、**报文类型**、**邻居** 三个选项卡；从邻居表可下钻至 **OSPF 邻居详情** 页面。

> **注意：** 若不需要 OSPF 分析，可在分析功能开关中关闭对应模块以降低分析负载。镜像口需能观测到 OSPF 报文（通常为组播 `224.0.0.5` / `224.0.0.6` 或点对点链路上的单播）。

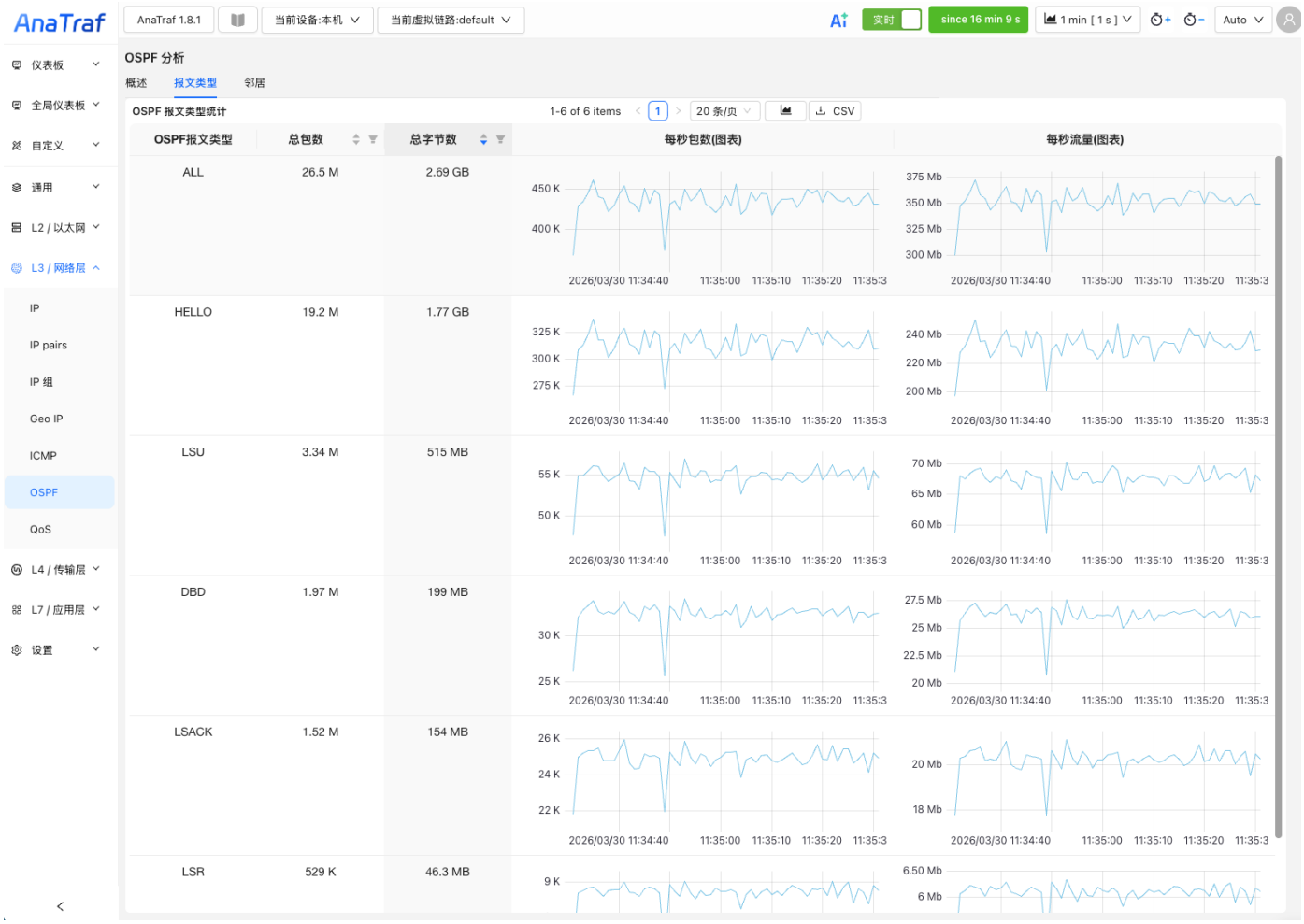
9.8.1 概述



概述 选项卡提供全网 OSPF 流量的汇总视图：

名称	描述	含义与用法
全局 OSPF 计数	观测到的 OSPF 总包数、总字节数	反映整网 OSPF 控制面负载。突发升高常与拓扑变化、大量 LSU/LSA 泛洪或邻居震荡有关；长期极低可能表示镜像未抓到 OSPF 或该区域几乎无路由活动。
OSPF 每秒包数（pps）	各网口 OSPF 报文速率随时间变化	用于观察控制面是否出现瞬时洪峰。与「报文类型」页对照，可判断是 Hello 异常增多还是 LSU/LSAck 等同步报文抬升。
OSPF 每秒流量（bps）	各网口 OSPF 字节速率随时间变化	与 pps 结合：pps 不高但 bps 高，可能多为较大 LSU；两者同时升高需关注链路与设备 CPU。

9.8.2 报文类型



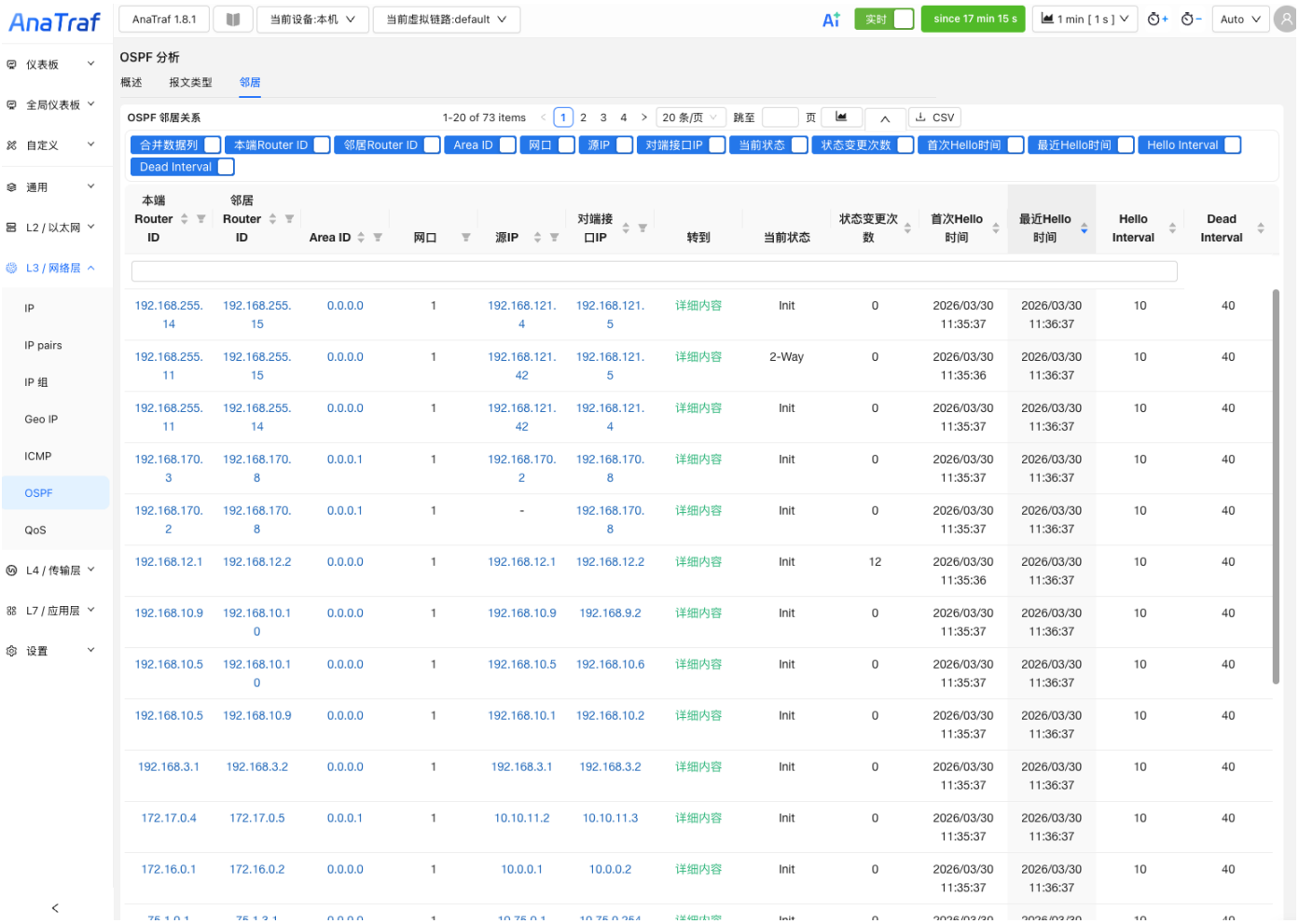
报文类型 选项卡按 OSPF 报文类型汇总统计，表中可查看各类型的包数、字节数，并可通过图开关查看 **每秒包数**、**每秒流量** 的历史曲线。汇总行还可能包含 **all**、**count** 等聚合项（以界面显示为准）。

各类型在协议中的作用如下（与界面中的类型名称对应）：

类型（示例）	协议含义	关注要点
hello	维持邻居发现与保活，携带 Router ID、Area、定时器、邻居列表等	应周期性出现；若仅见 LSU 而长期无 Hello，需检查是否镜像不全或网段不一致。
dbd	数据库描述，交换 LSA 摘要，用于主从协商与加载拓扑摘要	邻居建立初期增多属正常；稳定后仍持续大量 DBD 可能表示邻接反复重建。
lsr	链路状态请求，向邻居索取缺失的 LSA	多见于同步阶段；与 LSU 交替出现可对照是否卡在请求—应答环节。
lsu	链路状态更新，承载具体 LSA，是泛洪的主要载体	网络震荡或大面积拓扑变化时 LSU 会明显增多。
lsack	链路状态确认，对 LSU 的可靠传递做确认	与 LSU 成对观察；确认异常可能导致重传与进一步泛洪。

表中的 **总包数 / 总字节数** 表示该类型在统计窗口内的累计量；**每秒包数 / 每秒流量** 表示强度随时间的变化，便于与故障时刻对齐。

9.8.3 邻居



邻居 选项卡以「本端 Router ID + 邻居 Router ID + Area ID + 网口」等维度展示 OSPF 邻居关系，主要列说明如下：

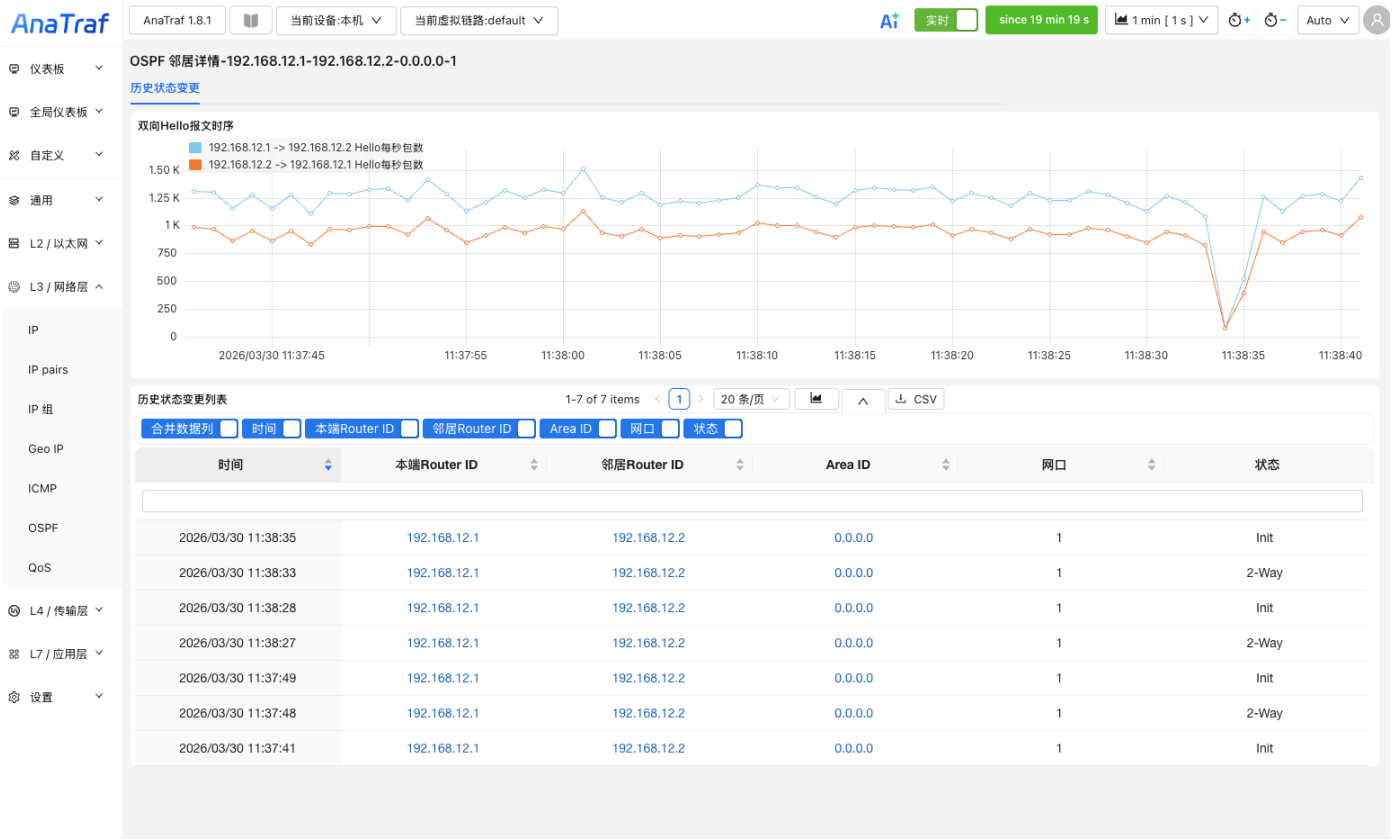
名称	描述	含义与用法
本端 Router ID	本地 OSPF 路由器标识（通常为 32 位点分十进制形式）	在区域内唯一标识一台 OSPF 路由器，与接口 IP 无关；排障时用于在拓扑中定位「哪一台设备」参与邻接。
邻居 Router ID	对端邻居的路由器标识	与本端成对出现，标识链路上对端的 OSPF 身份；与 **源 IP / 对端接口 IP** 一起可对照物理连接与逻辑邻居是否一致。
Area ID	所属 OSPF 区域	同一链路上邻居双方 Area 必须一致，否则无法形成正常邻接；骨干区域为 Area 0（常显示为 `0.0.0.0`）。
网口	观测到该邻居关系的分析仪网口	多网口设备上用于区分流量来自哪条镜像链路；跨网口出现同一对 Router ID 时需结合布线判断是否为合法多路径或重复镜像。
源 IP	本端在链路上的接口 IP（报文源地址）	即本端发出的 OSPF 报文源地址，应与该链路子网规划一致；与 Router ID 不同属于正常现象。
对端接口 IP	邻居在链路上的接口 IP	对端在报文中的源地址视角下的邻居接口；用于确认二层邻接所对应的实际 IP。
当前状态	分析仪根据 Hello 等推断的状态	见下表 **邻居状态说明**。分析仪侧为被动观测，状态可能与设备 CLI 完全一致或略粗粒度，以趋势与是否稳定为主。
状态变更次数	上述状态发生变化的累计次数	数值持续快速增长表示邻居关系不稳定（闪断、参数不一致、链路抖动等），适合作为告警或巡检指标。
首次 Hello 时间 / 最近 Hello 时间	首次与最近一次观测到 Hello 的时间	**最近 Hello** 若长期不更新且接近或超过 Dead Interval，可能表示邻居已失效或镜像中断；与详情页 Hello 曲线互证。
Hello Interval	Hello 报文发送间隔（秒，来自报文）	链路上双方应一致；不一致会导致邻接无法建立或频繁抖动。
Dead Interval	邻居失效判定时间（秒，来自报文）	通常为 Hello Interval 的数倍；在此时间内未收到 Hello 会认为邻居 Down。分析仪上若 Hello 曲线断续，可与该值对照判断是否超时。

邻居状态说明（界面常见取值）：

状态	含义（协议侧）	在阅读分析仪数据时的提示
Unknown	尚未从报文中可靠推断出更高状态	可能为刚出现流量、报文不全或仅抓到单向包；建议结合 **邻居详情** 双向 Hello 曲线判断。
Init	已从对端 Hello 中看到本端 Router ID，但尚未双向确认	常见于邻接建立初期；若长时间停留需检查 Hello/Area/认证等参数。
2-Way	双方已在 Hello 中互相列出对方，广播型网络中稳定邻居常停留于此	在广播/NBMA 上为正常状态；在点对点链路上若长期仅 2-Way 而无进一步同步，需结合设备类型与网络类型理解（分析仪仅反映可见报文推断结果）。

表格支持列筛选与列显示开关。点击行内 **转到** 链接（若已配置）可打开 **OSPF 邻居详情**，仅针对该邻居对展示更细的数据。

9.8.4 邻居详情



OSPF 邻居详情 页面在选定本端 Router ID、邻居 Router ID、Area ID 与网口后展示：

区域	名称	描述	含义与用法
图表	双向 Hello 报文时序	**本端到邻居** 与 **邻居到本端** 两个方向的 Hello 每秒包数（pps）曲线	正常时两条曲线应大致同频（与 Hello Interval 一致）。仅一侧有包多为单通、ACL/镜像方向错误或链路问题；两侧同时掉零可能为链路或设备 OSPF 进程异常。
表格	历史状态变更列表	按时间记录该邻居的状态变化	用于还原「何时开始不稳」；与全网 **概述** 中 pps 峰值、**报文类型** 中 LSU 突增时间对齐，可缩小根因范围（链路 vs 泛洪 vs 配置变更）。

10. L4 传输层

10.1 连接

连接模块显示了分析仪观测到的所有 IP 地址的连接。

10.1.1 连接详细

连接统计数据包括：

名称	描述
客户端 IP	客户端 IP 地址
客户端详情	包括端口号、DHCP名、操作系统、IP 地理位置信息等
服务器 IP	服务器 IP 地址
服务器详情	包括端口号、DHCP名、操作系统、IP 地理位置信息等
客户端端口	客户端端口号
服务器端口	服务器端口号
首次活动时间	该连接第一次开始活动的时间
上次活动时间	该连接最后一次接收或发送数据包的时间
应用层协议	识别到的应用层协议
MTU	最大传输单元
L4 字节	传输层传输字节数

> **注意：** 应用层协议显示为一段时间内最新识别出的协议。

TCP 统计数据包括：

名称	描述	参考意义
客户端 IP	客户端 IP 地址	
客户端详情	包括端口号、DHCP名、操作系统、IP 地理位置信息等	
服务器 IP	服务器 IP 地址	
服务器详情	包括端口号、DHCP名、操作系统、IP 地理位置信息等	

客户端端口	客户端端口号	
服务器端口	服务器端口号	
首次活动时间	该连接第一次开始活动的时间	
上次活动时间	该连接最后一次接收或发送数据包的时间	
应用层协议	识别到的应用层协议	
MTU	最大传输单元	
L4 字节	传输层传输字节数	
重传字节	TCP 连接中，重新传输的字节数量	1. 网络延迟和抖动。网络延迟较大或者抖动严重，使得确认包无法及时返回，导致发送方认为数据包丢失并进行重传。 2. 丢包。由于物理链路问题、过载的路由器或交换机等原因，数据包在传输过程中被丢弃。 3. 配置问题。如 TCP 窗口大小配置不当，也会影响重传率
重传率	TCP 重传字节数 / TCP 总字节数	-
重传包	TCP 连接中，重新传输的数据包数量	-
乱序包	在 TCP 连接中，接收的数据包顺序与发送时的顺序不一致的数量	网络路径变化。数据包在传输过程中可能经过不同的路径，不同路径的链路延迟不同，导致数据包到达顺序发生变化
Flag	TCP SYN、SYN-ACK、FIN、RST 数据包数	1. 大量的SYN包而没有相应的SYN-ACK包，可能说明有SYN洪水攻击（SYN Flooding Attack），这是DDoS攻击的一种形式。 2. 大量 RST 包，可能存在应用程序错误（应用程序没有正确处理连接请求，导致连接被重置）、网络路径问题（某些中间设备（如防火墙或IDS）重置连接）
握手次数	TCP 客户端 / 服务器握手次数	-
握手最小 / 平均 / 最大时延	TCP 客户端/服务器握手时延	-
流关闭时间	连接关闭时间	-

重复ACK的TCP包	TCP DUP ACK包是指TCP接收端在接收到一个重复的数据包时，向发送端发送的重复确认包	网络中存在数据包丢失或乱序现象
会话状态	该连接的状态	-
MSS	最大报文段大小	1. MSS过小影响性能。导致更多的报文段和确认包，增加网络开销，降低传输效率。 2. MSS过大导致分片。设置的MSS过大，超过路径上某些链路的MTU，数据包会被分片传输，增加了开销和延迟
窗口缩放	客户端 / 服务器窗口缩放值	-
零窗口	TCP零窗口数据包是由接收方发送的通知包，表明其接收缓冲区已满，当前无法接收更多数据	接收方的处理能力不足或缓冲区过小，导致频繁出现缓冲区已满的情况
最大窗口	客户端 / 服务器最大窗口大小	-
最大未确认传输	已经发送但未被接收方确认的数据字节数量	1. 网络延迟。高的可能表明网络延迟较大，数据包在网络中传输的时间较长。延迟可能由物理距离、网络拥堵或路由复杂性引起。 2. 丢包。丢包使得发送方重传数据，从而增加未确认字节数。 3. 接收端处理能力。接收端处理速度较慢，不能及时发送ACK，会导致发送端的未确认字节数增加
流信息	-	-
响应次数	客户端 / 服务器响应次数	-
响应时延	TCP连接中从发送方发送一个数据包到接收方收到并确认该数据包之间所经历的时间	-
应用时延	该连接的应用时延	-
TLS Hello 握手时延	TLS 握手过程时所花费的时间	1. 服务器资源不足。如果服务器负载高，处理TLS握手请求的能力受到限制，会导致握手时延增加。 2. 网络延迟或拥塞。在高网络负载或不稳定网络条件下，握手请求和响应的传输时间会增加。 3. 证书链验证问题。握手时延可能是由于证书链验证出现问题，例如证书吊销检查、证书过期或未正确配置
		1. 服务器负载或性能问题。服务器处理请求和响应的能力

TLS 第一次数据响应时延	在建立 TLS 连接后，客户端首次向服务器发送数据并且服务器响应第一个数据包所花费的时间	不足，导致响应时间延长。 2. 网络延迟或拥塞。数据传输过程中网络中的延迟或拥塞，使得响应时间增加。 3. 数据包丢失和重传。数据包在传输过程中丢失或需要重传，延长了数据的到达时间。 4. 应用层优化不足。未进行有效的性能优化措施，如缓存、压缩和减少请求次数等
TLS 协商的加密算法	-	-
TLS 版本	-	-
有效性	无效连接（invalid）：握手失败，或者握手成功但没有传输数据，或者仅在单方向传输数据	频繁出现无效连接的情况，意味着网络资源可能存在浪费

> **注意：**
>
> 1. 在未观测到一条 TCP 连接的握手过程时，通过端口号的范围区分客户端（端口号大于10000）与服务器（端口号小于1000），以及通过内、外网 IP 区分客户端、服务器。
> 2. 当通过端口号范围和内、外网 IP 无法进行区分时，则将观测到的该连接的第一个数据包的发送方认定为客户端，接收方认定为服务器。

10.2 TCP

TCP 模块提供分析 TCP 连接的质量，包括 TCP 握手情况，响应时间，TCP 标志位，TCP 重传和 TCP 零窗口等。

10.2.1 TCP 握手

TCP 握手选项卡显示有关所有 TCP 连接的握手时间统计。

全局 TCP 握手时间的信息包括：

名称	描述
握手次数	TCP 握手次数，计算的值为成功建立连接的次数
客户端最小 / 平均 / 最大握手时延	SYN-ACK 和 ACK 包之间的时延
服务器最小 / 平均 / 最大握手时延	SYN 和 SYN-ACK 包之间的时延

表格信息包括：

名称	描述
IP 地址	-
客户端握手次数	该 IP 地址作为客户端时的握手次数
服务器握手次数	该 IP 地址作为服务器时的握手次数
握手最小 / 平均 / 最大时延	该 IP 地址的最小 / 平均 / 最大握手时延

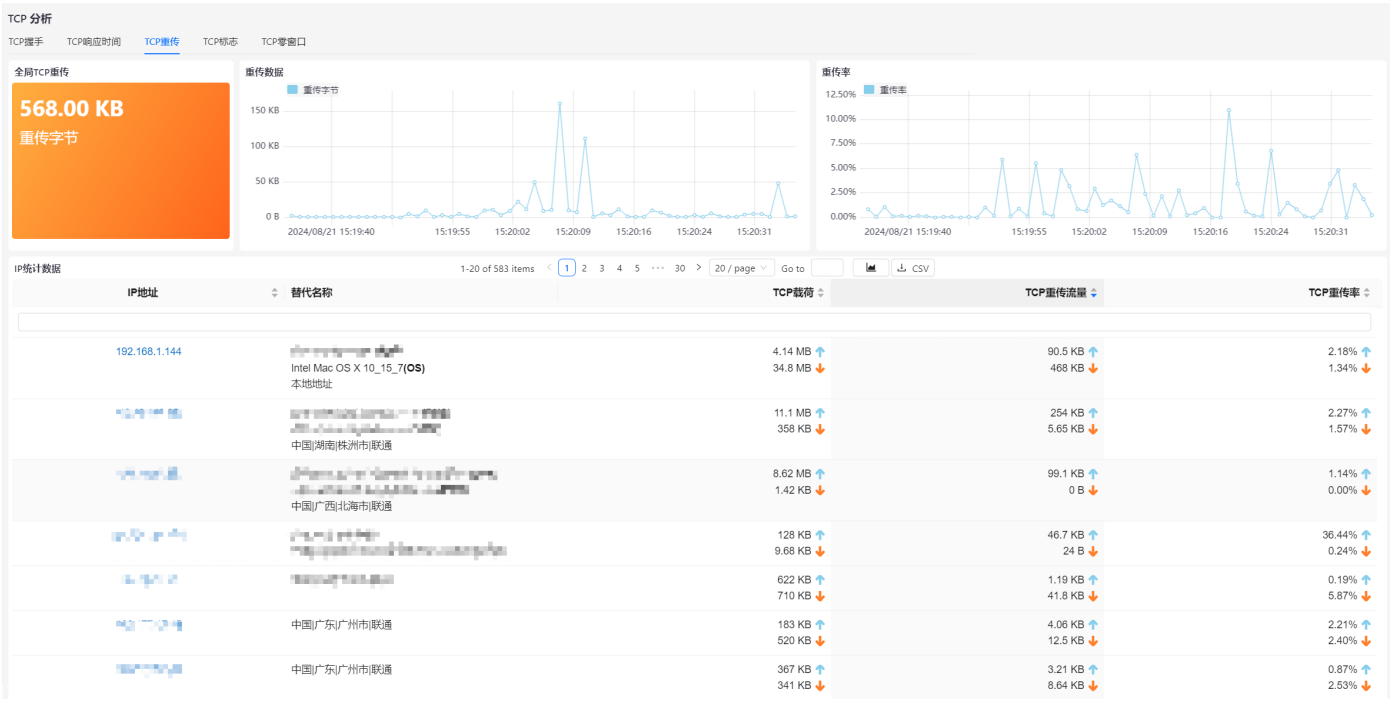
10.2.2 TCP 响应时延

计算的时间是数据传输和相应的确认之间的时延。

响应时延表格：

名称	描述
IP 地址	服务器 IP 地址
最小 / 平均 / 最大时延	该 IP 地址的最小 / 平均 / 最大时延

10.2.3 TCP 重传



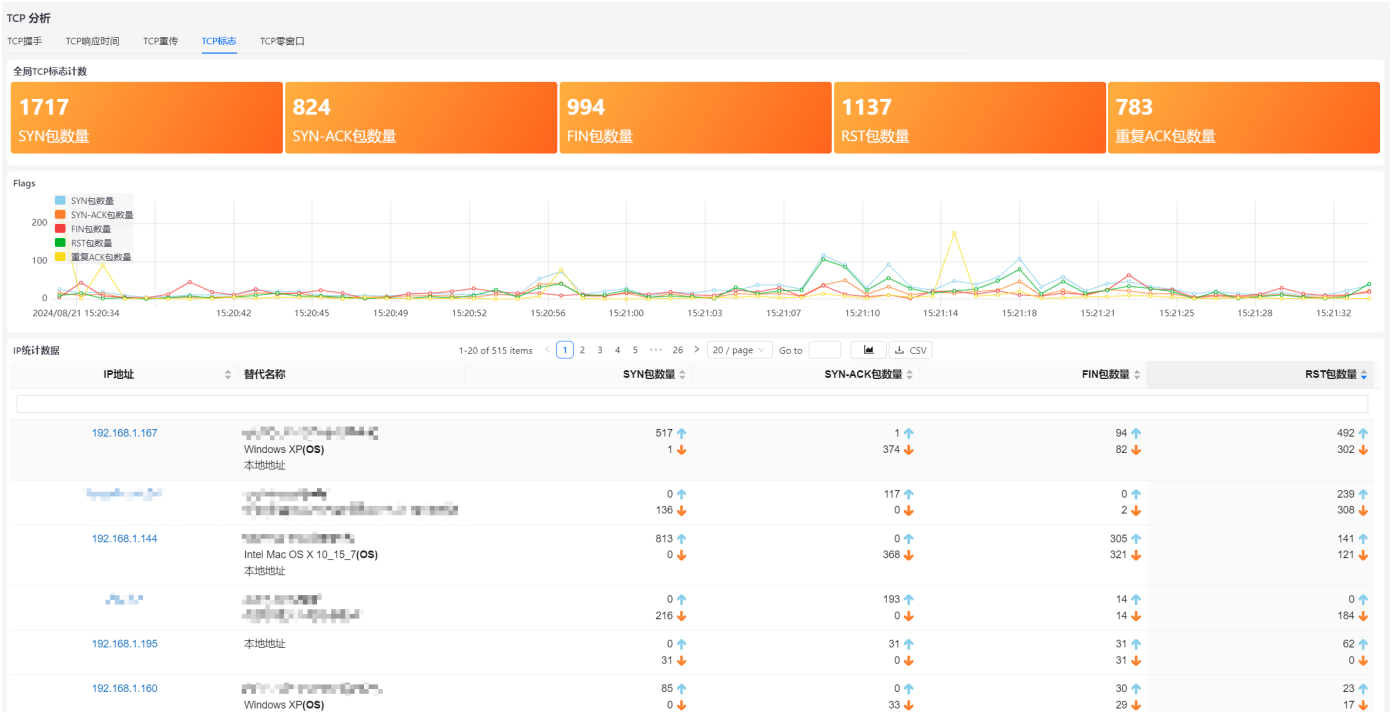
全局 TCP 重传部分展示了分析仪观测到的总 TCP 重传字节数。

名称	描述
重传数据	重传字节随时间变化的图表
重传率	重传率随时间变化的图表

表格信息包括：

名称	描述
IP 地址	IP 地址
发送 TCP 载荷	该 IP 地址发送的 TCP payload 字节数
接收 TCP 载荷	该 IP 地址接收的 TCP payload 字节数
发送 TCP 重传流量	该 IP 地址发送的 TCP 重传字节数
接收 TCP 重传流量	该 IP 地址接收的 TCP 重传字节数

10.2.4 TCP 标志位

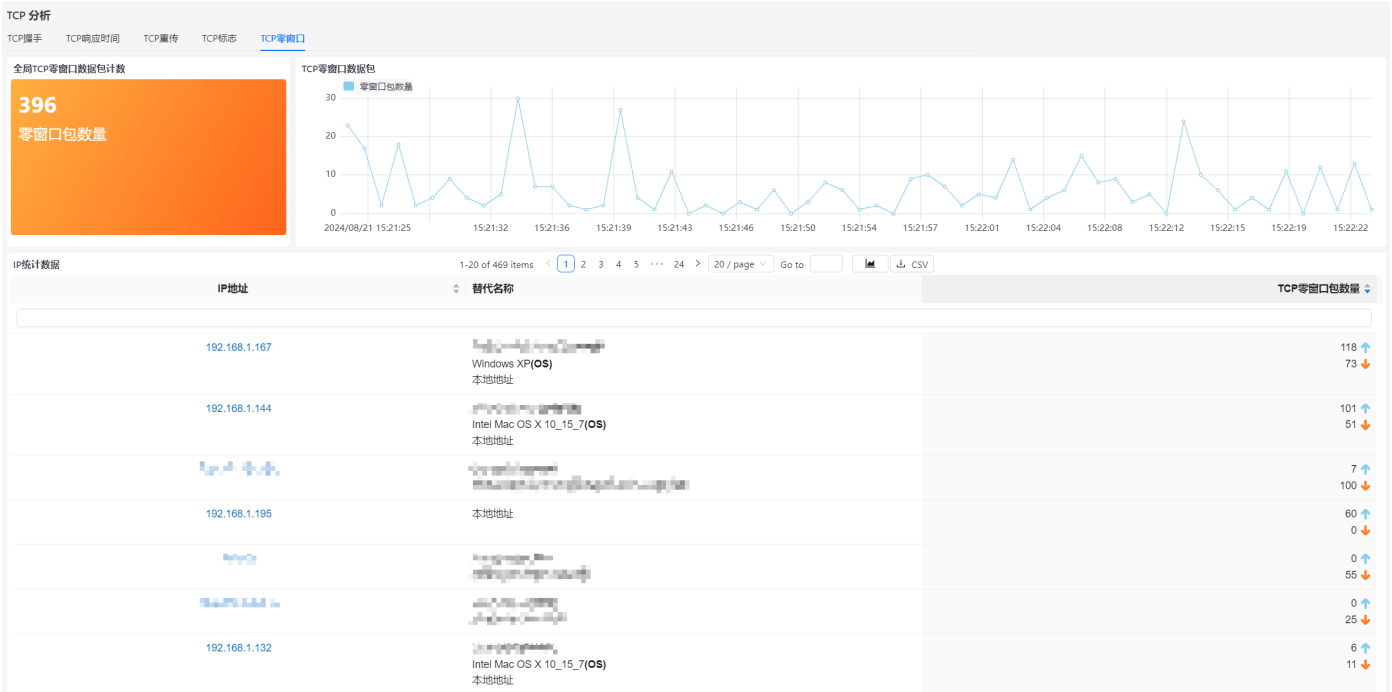


全局 TCP 标志计数显示了分析仪观测到的 SYN、SYN-ACK、FIN、RST、DUP ACK 包数量，并提供各种标志位包数量随时间变化的曲线图。

表格内容包括：

名称	描述	参考意义
IP 地址	-	-
发送 / 接收 SYN 包数量	该 IP 地址发送 / 接收的 SYN 包数量	大量的SYN包而没有相应的SYN-ACK包，可能说明有SYN洪水攻击（SYN Flooding Attack），这是DDoS攻击的一种形式
发送 / 接收 SYN-ACK 包数量	该 IP 地址发送 / 接收的 SYN-ACK 包数量	如果客户端发出SYN包后未收到SYN-ACK包，可能是服务器配置错误或网络路径上的设备（如防火墙）阻止了通信
发送 / 接收 FIN 包数量	该 IP 地址发送 / 接收的 FIN 包数量	过高的FIN包数量可能意味着应用程序频繁启动和关闭连接，需要检查应用程序的连接管理逻辑
发送 / 接收 RST 包数量	该 IP 地址发送 / 接收的 RST 包数量	大量 RST 包，可能存在应用程序错误（应用程序没有正确处理连接请求，导致连接被重置）、网络路径问题（某些中间设备（如防火墙或 IDS）重置连接）

10.2.5 TCP 零窗口



全局 TCP 零窗口数据包计数展示了分析仪观测到的 TCP zero windows 数据包数量及其随时间变化的曲线图。

表格内容包括：

名称	描述
IP 地址	IP 地址
发送 / 接收 TCP 零窗口数据包	该 IP 地址发送 / 接收的 TCP 零窗口数据包

11. L7 应用层

11.1 L7 应用层协议

L7 应用层协议对识别出的应用层协议（包括自定义协议）进行流量统计。

TOP 5 Protocols 显示了一段时间内流量最大的五种应用层协议的流量随时间变化的曲线图。

表格内容包括识别出的应用层协议及其流量统计。

11.1.1 自定义协议

进入**自定义协议**标签页，点击**添加自定义协议**按钮，可以根据规则添加自定义协议。

规则	描述	示例
IP	可设置 IP 地址或 IP 段	192.168.1.1/24
L4 协议	可设置 TCP、UDP 或 ANY	-
端口	可设置端口号或端口范围	123-456
Payload 正则匹配	可以设置正则表达式对 Payload 进行匹配	baidu
HEX 特征值匹配	可以设置十六进制特征值对 Payload 进行精确匹配	详见下文
域名	可设置域名，支持设置多个域名	baidu.com
匹配模式	可设置流审计模式或内容审计模式	详见下文

11.1.1.1 HEX 特征值匹配

HEX 特征值匹配功能允许您通过指定数据包 Payload 中的特定字节位置和值来精确识别协议。该功能适用于需要基于二进制特征进行协议识别的场景，例如识别特定格式的工业协议、自定义应用协议等。

HEX 特征值配置项：

- **偏移量（Offset）**：必填，指定要匹配的字节在 Payload 中的起始位置（相对于 Payload 起始位置的字节偏移量）。偏移量从 0 开始计数，不能为负数。
- **字节数（Length）**：必填，指定要匹配的字节长度。必须大于 0。
- **匹配值（Value）**：必填，指定要匹配的十六进制字节值。格式为十六进制字符串，多个字节之间用空格分隔，例如：`0x01 0x02 0x03` 或 `01 02 03`。匹配值的长度必须等于字节数。
- **掩码（Mask）**：可选，用于部分匹配。当需要只匹配某些位时，可以使用掩码。掩码格式与匹配值相同，为十六进制字符串。掩码中的每个字节用于指定对应位置需要匹配的位：
  - 掩码位为 `0xFF`（或 `0xff`）表示该位必须完全匹配
  - 掩码位为 `0x00` 表示该位不参与匹配
  - 掩码位为其他值（如 `0xF0`）表示只匹配高 4 位，低 4 位忽略

匹配逻辑：

- **多个 HEX 特征值**：如果配置了多个 HEX 特征值，所有特征值都必须匹配（AND 逻辑）。只有当所有特征值都匹配成功时，协议识别才会成功。
- **HEX 特征值与正则表达式**：如果同时配置了 HEX 特征值和正则表达式，两者都必须匹配（AND 关系）。只有当 HEX 特征值匹配成功且正则表达式也匹配成功时，协议识别才会成功。
- **与其他规则的关系**：HEX 特征值匹配可以与其他匹配规则（IP/端口、域名等）组合使用。所有规则之间是 AND 关系，必须全部满足才能识别为自定义协议。

使用示例：

- **示例 1：匹配固定魔数**
  - 偏移量：`0`
  - 字节数：`4`
  - 匹配值：`0x4D 0x5A 0x90 0x00`（Windows PE 文件魔数）
  - 掩码：不设置（完全匹配）
- **示例 2：使用掩码进行部分匹配**
  - 偏移量：`0`
  - 字节数：`2`
  - 匹配值：`0x12 0x34`
  - 掩码：`0xF0 0xFF`（只匹配第一个字节的高 4 位，第二个字节完全匹配）
  - 说明：该配置会匹配 `0x10-0x1F` 范围内的任意值作为第一个字节，`0x34` 作为第二个字节
- **示例 3：多个特征值组合**
  - 特征值 1：
    - 偏移量：`0`
    - 字节数：`2`
    - 匹配值：`0x01 0x02`
  - 特征值 2：
    - 偏移量：`10`

        - 字节数：`4`
        - 匹配值：`0xAA 0xBB 0xCC 0xDD`
    - 说明：只有当 Payload 的第 0-1 字节为 `0x01 0x02`，且第 10-13 字节为 `0xAA 0xBB 0xCC 0xDD` 时，才会匹配成功

注意事项：

- HEX 特征值的偏移量和字节数必须确保不会超出 Payload 的实际长度，否则匹配会失败。
- 如果配置了多个 HEX 特征值，建议按照偏移量从小到大的顺序配置，便于管理和理解。
- 掩码功能适用于需要匹配协议版本号、可变字段等场景，可以增加匹配的灵活性。
- HEX 特征值匹配与正则表达式匹配可以同时使用，但建议根据实际需求选择最合适的匹配方式。对于二进制协议，HEX 特征值匹配通常更精确和高效。

11.1.1.2 匹配模式

自定义协议支持两种匹配模式，用于控制协议识别的行为：

- **基于流（Flow Audit）**：流审计模式，匹配一次后整条流标记。当数据流中的第一个数据包匹配成功后，整条数据流都会被标记为该自定义协议，后续数据包不再进行匹配检查。该模式适用于协议特征在连接建立时就能识别的场景，可以提高识别效率。
- **基于包（Content Audit）**：内容审计模式，每个包都进行匹配。对数据流中的每个数据包都进行匹配检查，只有匹配成功的数据包才会被标记为该自定义协议。该模式适用于协议特征可能出现在数据流中任意位置的场景，或者需要精确统计匹配数据包数量的场景。

> **注意：**
>
> 1. 匹配模式的选择会影响协议识别的准确性和性能。对于特征明显的协议，建议使用"基于流"模式以提高性能；对于特征可能分散在多个数据包中的协议，建议使用"基于包"模式。
> 2. 匹配模式在创建自定义协议时设置，后续可以修改。

11.2 HTTP

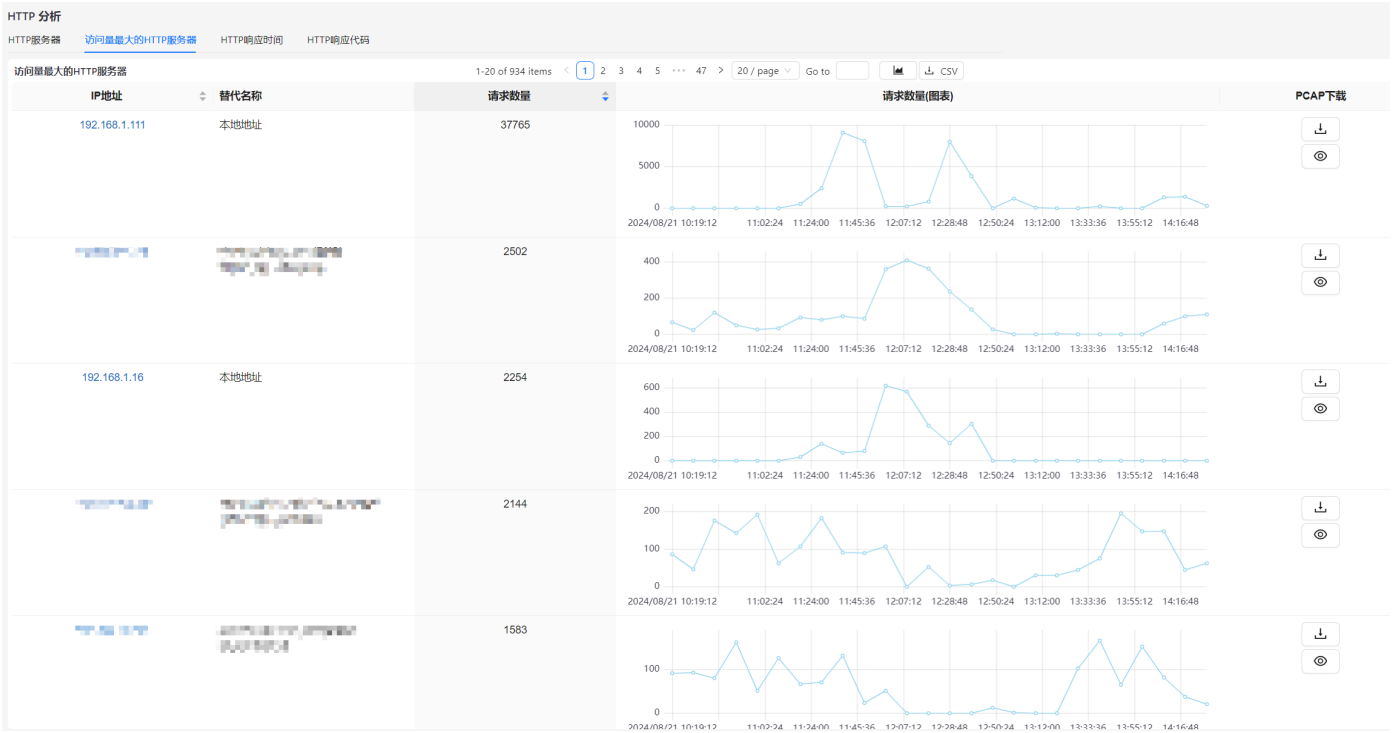
HTTP 模块处理分析仪观测到的 HTTP 流量。

11.2.1 HTTP 服务器

HTTP 服务器选项卡显示可以检索 HTTP 信息的所有 IP 地址。表格包含的信息如下：

名称	描述
IP 地址	HTTP 服务器的 IP 地址。点击此地址可访问该 IP 地址的详细信息页面
主机名	客户端请求的名称

11.2.2 访问量最大的 HTTP 服务器



该选项卡显示所有访问的 HTTP 服务器。表格包含信息如下：

名称	描述
IP 地址	HTTP 服务器的 IP 地址。点击此地址可访问该 IP 地址的详细信息页面
请求数量	HTTP 服务器接收到的请求数量
国家 / 地区	该 IP 地址所在的国家 / 地区

11.2.3 HTTP 响应时间

该选项卡显示了所有 HTTP 请求的全局统计信息和 HTTP 服务器的响应时间表。
全局响应时延数据包括：

名称	描述
请求数量	分析仪观测到的 HTTP 请求数量
最小响应耗时	根据观测到的所有 HTTP 响应计算的最小响应时间
平均响应耗时	根据观测到的所有 HTTP 响应计算的平均响应时间
最大响应耗时	根据观测到的所有 HTTP 响应计算的最大响应时间

不同时期的平均响应时延（包括最大/最小时延）图展示了最大 / 最小 / 平均时延随时间变化的箱线图。

HTTP 服务器的表格包含如下信息：

名称	描述
IP 地址	HTTP 服务器的 IP 地址。点击此地址可访问该 IP 地址的详细信息页面
请求数量	该 HTTP 服务器的响应数量
最小响应耗时	根据观测到的该 HTTP 服务器所有 HTTP 响应计算的最小响应时间
平均响应耗时	根据观测到的该 HTTP 服务器所有 HTTP 响应计算的平均响应时间
最大响应耗时	根据观测到的该 HTTP 服务器所有 HTTP 响应计算的最大响应时间

11.2.4 HTTP 响应代码

该选项卡显示了 HTTP 响应代码的全局统计信息，包括各种响应代码的数量和分布饼图，以及每个 HTTP 服务器的响应代码信息。

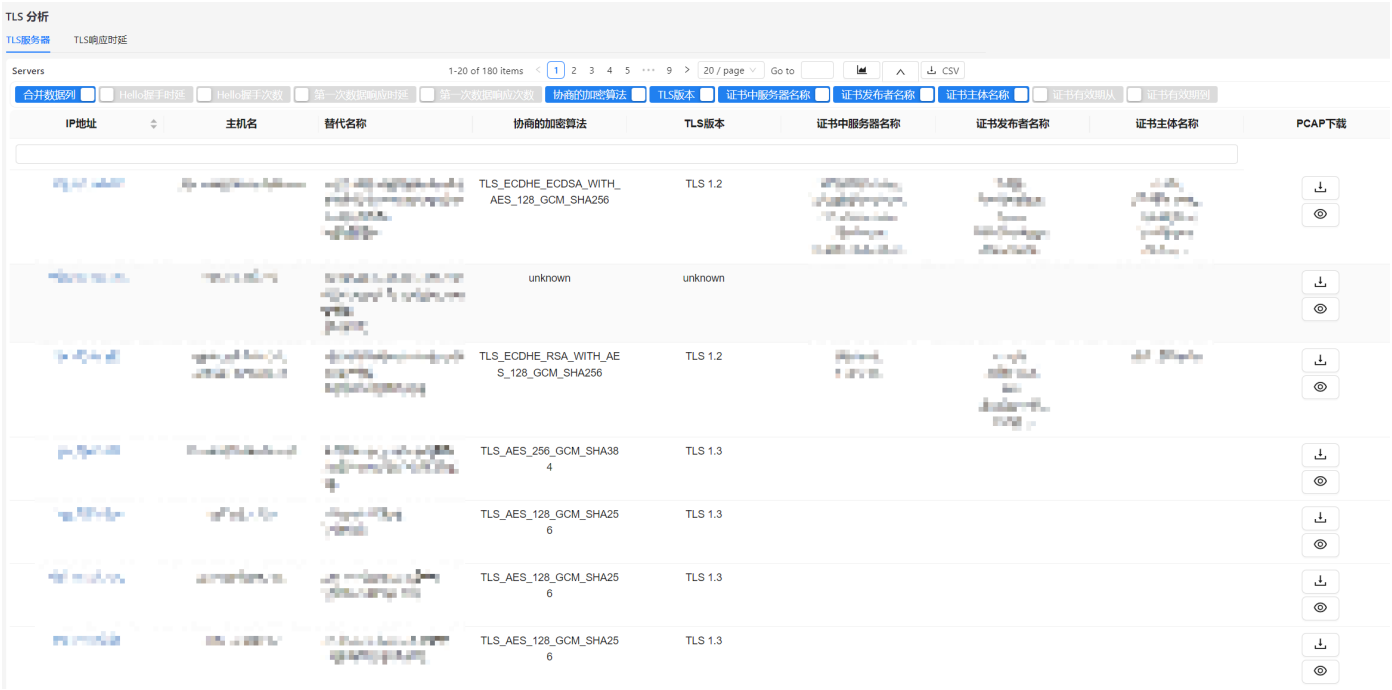
响应代码表格包含以下信息：

名称	描述	参考意义
IP 地址	HTTP 服务器的 IP 地址。点击此地址可访问该 IP 地址的详细信息页面	-
请求数量	该 HTTP 服务器的响应数量	-
1xx(信息)响应数量	该 HTTP 服务器 1xx(信息)响应数量	通常被视为正常情况的一部分，因为它们并不表示故障或错误
2xx(成功)响应数量	该 HTTP 服务器 2xx(成功)响应数量	-
3xx(重定向)响应数量	该 HTTP 服务器 3xx(重定向)响应数量	请求的资源已被移动到不同的位置或者临时不可用，需要客户端采取额外的步骤来完成请求
4xx(客户端错误)响应数量	该 HTTP 服务器 4xx(客户端错误)响应数量	表示客户端错误，提供了关于请求失败的详细信息
5xx(服务器错误)响应数量	该 HTTP 服务器 5xx(服务器错误)响应数量	表示服务器在尝试处理客户端请求时发生了问题
(其他)响应数量	除去上述 5 类响应的其他种类响应数量	-

11.3 TLS

TLS 模块处理分析仪观测到的 TLS 流量。

11.3.1 TLS 服务器

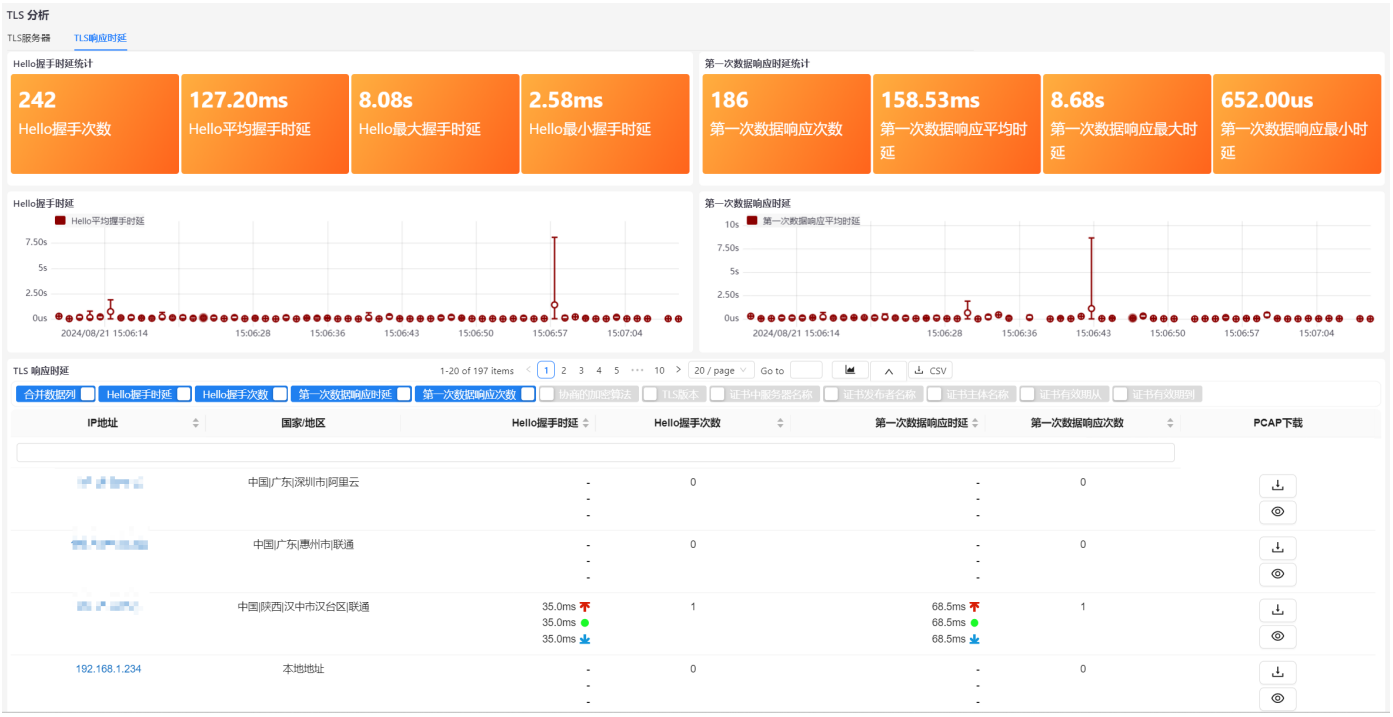


该选项卡显示所有访问的 TLS 服务器。由于一个 IP 可能托管多个服务，因此一个 IP 地址可以看到多个名称。

表格包含信息如下：

名称	描述
IP 地址	TLS 服务器的 IP 地址。点击此地址可访问该 IP 地址的详细信息页面
主机名	TLS 服务器名称。客户端请求的名称，由于一个 IP 可能托管多个服务，因此一个 IP 地址可以看到多个名称
替代名称	该 IP 地址的别名。包括 DNS 名称和 DHCP 名称（如果有）
证书中服务器名称	和主机名类似，这里列出所有看到的证书中的服务器名称
证书发布者名称	代表证书颁布机构(CA)的身份信息。通常包含国家(C)、州或省(ST)、城市(L)、组织(O)、组织单位(OU)、公共名称(CN)
证书主体名称	代表证书所签署的对象的身份信息。通常包含国家(C)、州或省(ST)、城市(L)、组织(O)、组织单位(OU)、公共名称(CN)
协商的加密算法	协商的密码套件
TLS 版本	使用的 TLS 版本
证书有效期从	证书有效期的开始时间
证书有效期到	证书到期时间

11.3.2 TLS 响应时延



该选项卡显示了所有 SSL/TLS 请求的全局统计信息和可计算响应时间的所有 SSL/TLS 服务器的响应时间表。

全局统计数据包括：

名称	描述
Hello 握手次数	分析仪观测到的 TLS Hello 握手次数
Hello 最小 / 平均 / 最大握手时延	所有服务器的最小 / 平均 / 最大握手时延
第一次数据响应次数	所有服务器的第一次数据响应次数
第一次数据响应最小 / 平均 / 最大时延	所有服务器的第一次数据响应的最小 / 平均 / 最大时延

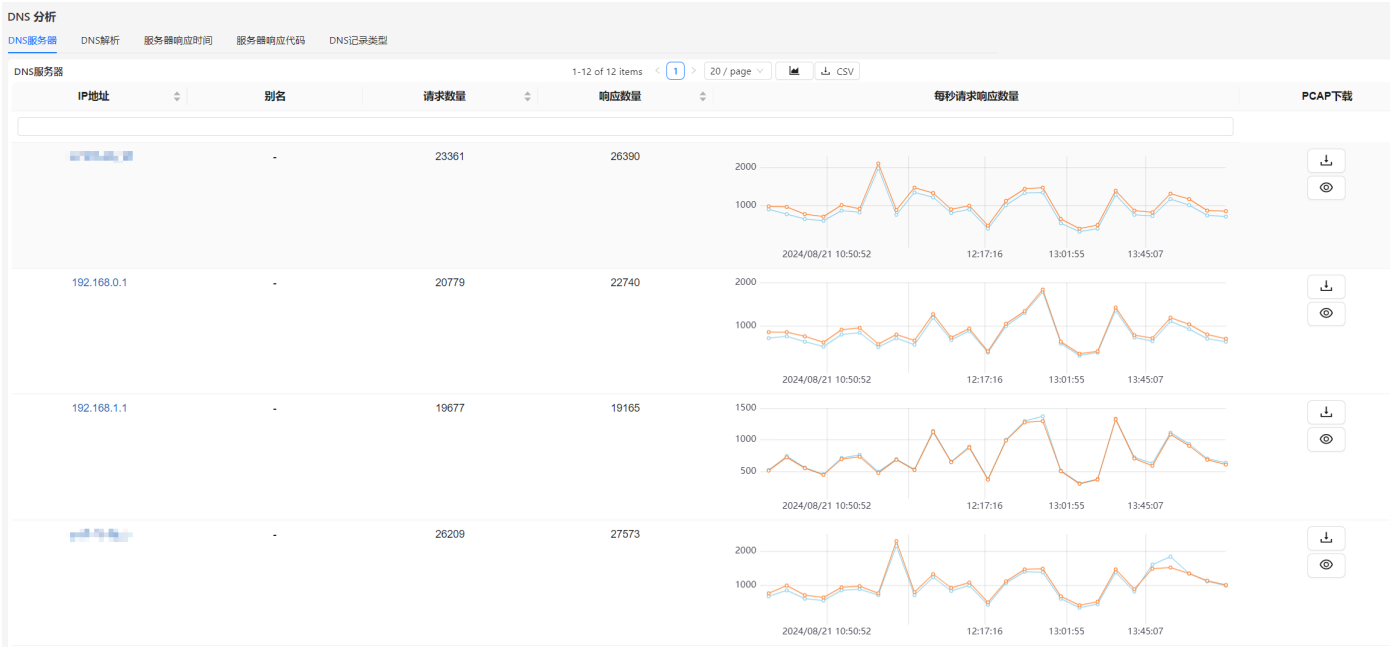
TLS 响应时延表格包含信息：

名称	描述	参考意义
IP 地址	TLS 服务器的 IP 地址	-
国家 / 地区	TLS 服务器所处的国家 / 地区	-
Hello 最小 / 平均 / 最大握手时延	TLS 握手过程时所花费的时间	1. 服务器资源不足。如果服务器负载高，处理TLS握手请求的能力受到限制，会导致握手时延增加。 2. 网络延迟或拥塞。在高网络负载或不稳定网络条件下，握手请求和响应的传输时间会增加。 3. 证书链验证问题。握手时延可能是由于证书链验证出现问题，例如证书吊销检查、证书过期或未正确配置
第一次数据响应最小 / 平均 / 最大时延	在建立 TLS 连接后，客户端首次向服务器发送数据并且服务器响应第一个数据包所花费的时间	1. 服务器负载或性能问题。服务器处理请求和响应的能力不足，导致响应时间延长。 2. 网络延迟或拥塞。数据传输过程中网络中的延迟或拥塞，使得响应时间增加。 3. 数据包丢失和重传。数据包在传输过程中丢失或需要重传，延长了数据的到达时间。 4. 应用层优化不足。未进行有效的性能优化措施，如缓存、压缩和减少请求次数等

11.4 DNS

DNS 模块跟踪域名解析请求和响应。

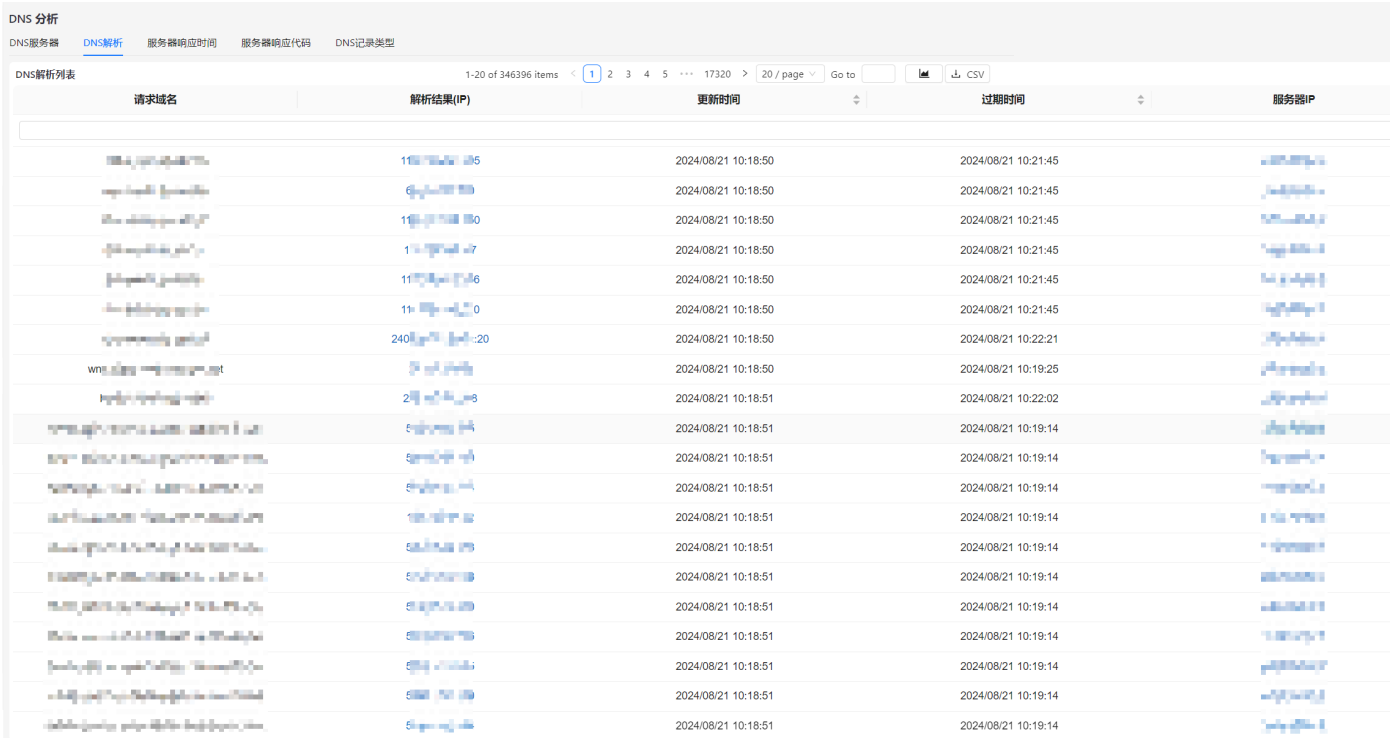
11.4.1 DNS 服务器



DNS 服务器表展示了分析仪观测到 DNS 流量的所有 DNS 服务器。

名称	描述
IP 地址	DNS 服务器的 IP 地址
别名	该 IP 地址的别名
请求数量	该 DNS 服务器收到的 DNS 请求数量
响应数量	该 DNS 服务器 DNS 响应数量

11.4.2 DNS 解析



DNS 解析表展示了分析仪观测到的 DNS 解析信息。

名称	描述
请求域名	DNS 请求解析的域名
解析结果	域名对应的 IP 地址
更新时间	该域名成功解析的时间
过期时间	该域名解析结果的过期时间
服务器 IP	解析该域名的 DNS 服务器的 IP 地址

11.4.3 服务器响应时间

服务器响应时间选项卡显示有关 DNS 请求和响应之间的响应时间信息，分为全局统计信息和每个 DNS 服务器统计信息。

全局响应时延部分展示了最大 / 最小 / 平均响应耗时。

名称	描述
最小 / 平均 / 最大响应耗时	从DNS查询发起到收到DNS响应之间的时间延迟

不同时期的平均响应时延（包括最大/最小时延）图展示了最大 / 最小 / 平均时延随时间变化的箱线图。

DNS 服务器表展示了每个 DNS 服务器的响应时延统计信息。

名称	描述
IP 地址	DNS 服务器的 IP 地址
别名	该 IP 地址的别名
请求数量	该 DNS 服务器收到的 DNS 请求数量
响应数量	该 DNS 服务器 DNS 响应数量
最小响应耗时	根据该 DNS 服务器所有响应耗时计算的最小响应耗时
平均响应耗时	根据该 DNS 服务器所有响应耗时计算的平均响应耗时
最大响应耗时	根据该 DNS 服务器所有响应耗时计算的最大响应耗时
每秒请求响应数量	显示了每秒 DNS 请求数量的历史图

11.4.4 服务器响应代码

服务器响应代码显示了全局和每个 DNS 服务器的响应代码信息。

全局响应代码部分展示了自分析仪开机开始，DNS 响应代码的计数。

名称	描述	参考意义
请求数量	分析仪观测到的所有 DNS 请求数量	-
响应数量	分析仪观测到的所有 DNS 响应数量	-
成功响应数量（NOERROR）	查询成功，没有错误	-
格式错误请求数量（FORMERR）	通常指示了一些与 DNS 报文格式不符或其他格式错误相关的问题	1. DNS报文格式错误。DNS FORMERR 表示服务器无法理解或处理客户端发送的 DNS 请求，因为请求的报文格式不正确。这可能是由于数据包损坏、错误的协议版本或其他通信问题引起的。 2. DNS服务器配置问题。有时 DNS FORMERR 可能是由于 DNS 服务器配置错误引起的，例如不正确的参数设置或不支持的功能请求
服务器错误请求数量（SERVFAIL）	通常指示了 DNS 服务器在处理请求时遇到了问题，无法为客户端提供有效的响应	1. DNS 服务器故障。这可能包括服务器软件崩溃、硬件故障、网络连接问题等。 2. DNS查询负载过重。DNS 服务器可能因为查询负载过重而导致某些请求超时或失败，特别是在高流量或攻击情况下
查询不存在错误数量（NXDOMAIN）	表示所请求的域名不存在，即 DNS 服务器无法解析客户端查询的域名	1. 域名拼写错误或不存在。客户端可能请求了一个不存在的域名，或者域名拼写错误。 2. DNS服务器配置。DNS 服务器可能未正确配置某些域名区域，或者缓存中不包含请求的域名记录
其他错误数量	除了 FORMERR、SERVFAIL、NXDOMAIN 外的其他错误代码的数量	-
错误请求数量	所有的响应中除去成功响应（NOERROR）的数量	-

历史错误数据显示了错误请求储量、格式错误请求数量、服务器错误请求数量、查询不存在错误数量，以及其他错误数量随时间变化的曲线图。

DNS 服务器表显示了每个 DNS 服务器的响应代码信息。

名称	描述
IP 地址	DNS 服务器的 IP 地址
别名	该 IP 地址的别名
请求数量	分析仪观测到的该 DNS 服务器所有 DNS 请求数量
响应数量	分析仪观测到的该 DNS 服务器所有 DNS 响应数量
成功响应数量（NOERROR）	查询成功，没有错误。限定为该 DNS 服务器
格式错误请求数量（FORMERR）	表示格式错误。限定为该 DNS 服务器
服务器错误请求数量（SERVFAIL）	表示服务器故障。限定为该 DNS 服务器
查询不存在错误数量（NXDOMAIN）	表示目标域名不存在。限定为该 DNS 服务器
其他错误数量	除了 FORMERR、SERVFAIL、NXDOMAIN 外的其他错误代码的数量。限定为该 DNS 服务器
错误请求数量	所有的响应中除去成功响应（NOERROR）的数量。限定为该 DNS 服务器
错误历史数据	显示了该 DNS 服务器的错误历史数据随时间变化的曲线图

11.4.5 DNS 记录类型

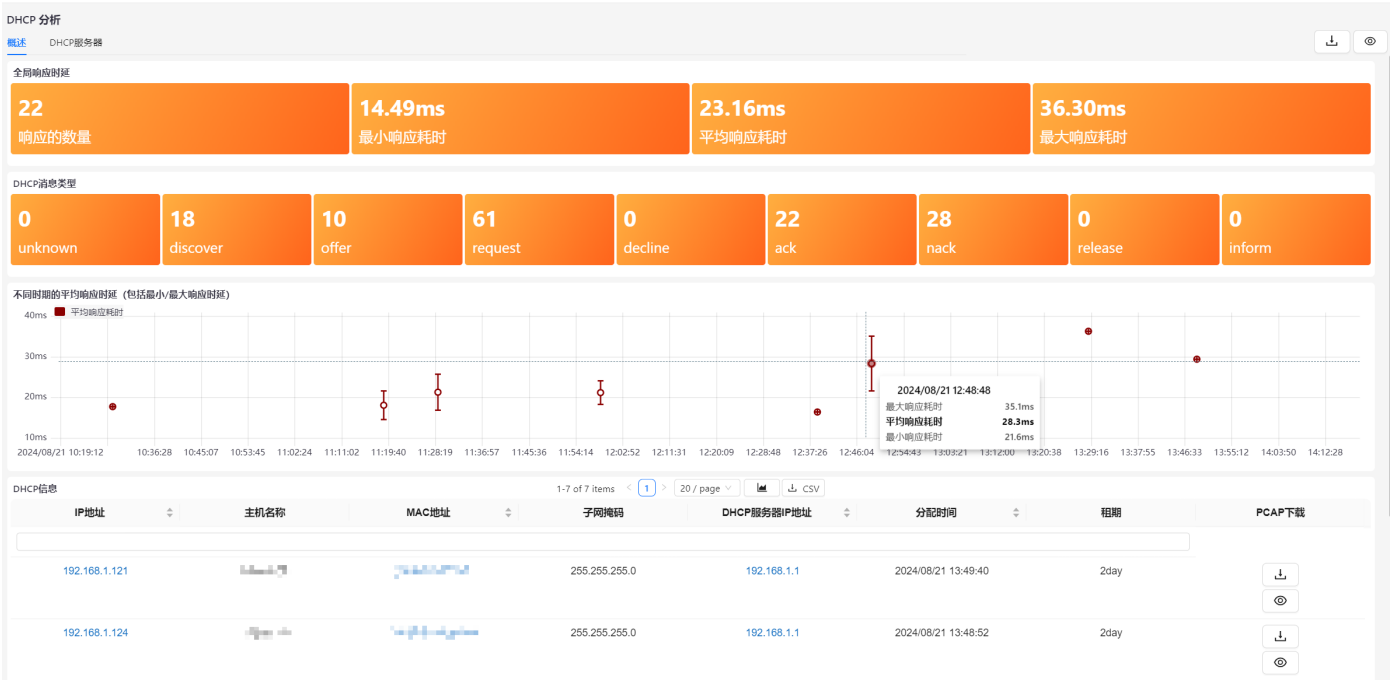
DNS 记录类型选项卡显示了所有 DNS 服务器全局的 DNS 记录类型的数量以及随时间变化的曲线。

名称	描述
A	用于将域名映射到 IPv4 地址
AAAA	用于将域名映射到 IPv6 地址
CNAME	用于创建别名或指向其他域名的链接
MX	用于指定邮件服务器的优先级和地址
SRV	用于指定服务的位置和优先级
OTHER	除去上述的 A、AAAA、CNAME、MX、SRV外的其他记录类型

11.5 DHCP

DHCP 模块跟踪网络中动态 IP 分配的请求和响应。

11.5.1 概述



全局响应时延部分展示了观测到的所有 DHCP 响应的数量，以及根据所有响应耗时计算的最大 / 最小 / 平均响应时延。

名称	描述
响应的数量	AnaTraf 网络流量分析仪自开机开始，观测到的所有 DHCP 响应数量
最小响应耗时	根据所有响应耗时计算的最小响应耗时
平均响应耗时	根据所有响应耗时计算的平均响应耗时
最大响应耗时	根据所有响应耗时计算的最大响应耗时

DHCP 消息类型部分展示了 DHCP 消息类型的计数。

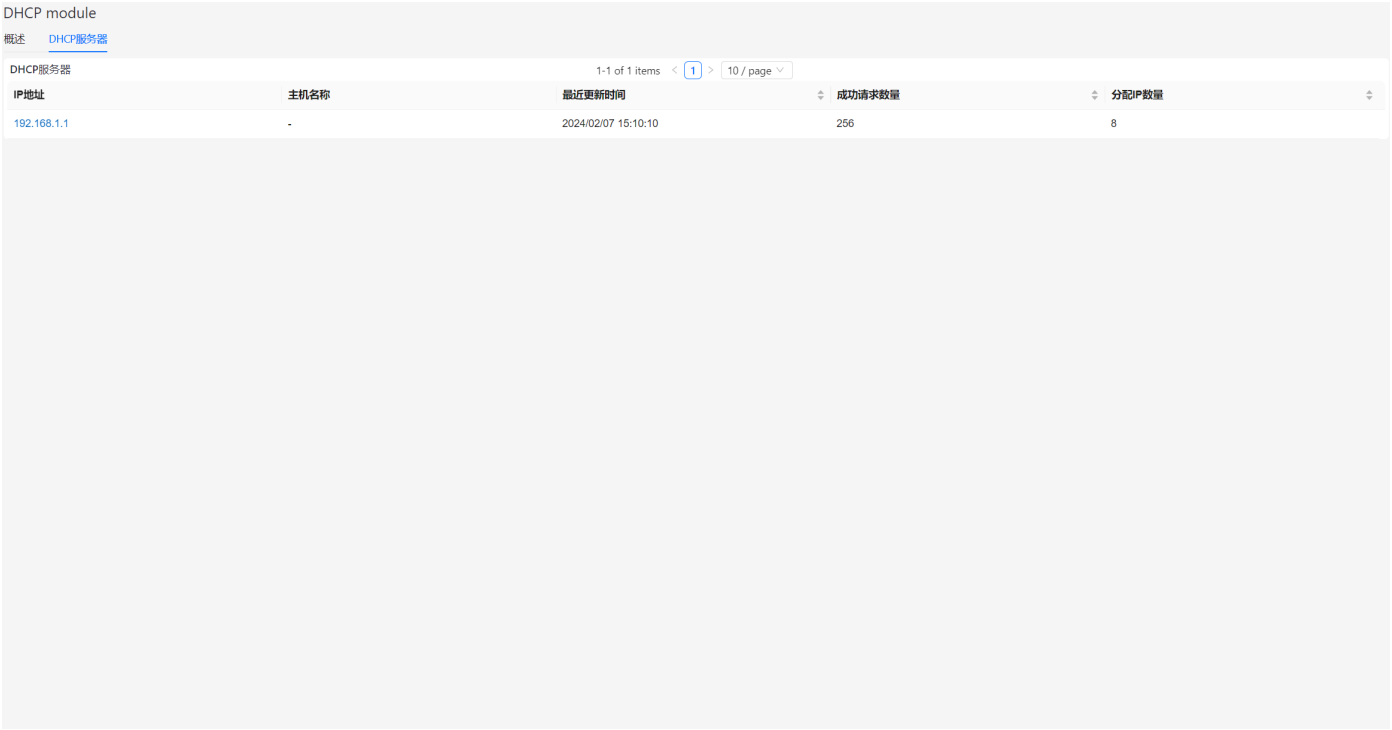
名称	描述
unknown	在某些情况下，DHCP 服务器可能会收到无法识别或无法处理的报文
discover	客户端发送的广播报文，用于寻找可用的 DHCP 服务器
offer	DHCP 服务器响应 DHCP discover 报文的广播，向客户端发送的广播报文
request	客户端发送给 DHCP 服务器的报文，用于确认并请求特定的 DHCP 服务器提供的 IP 地址和配置信息
decline	客户端发送给 DHCP 服务器的报文，表示拒绝接收 DHCP 服务器提供的 IP 地址和配置信息
ack	DHCP 服务器发送给客户端的报文，确认并授予客户端请求的 IP 地址和配置信息
nack	DHCP 服务器发送给客户端的报文，表示拒绝或无法提供请求的 IP 地址和配置信息
release	客户端发送给 DHCP 服务器的报文，用于释放之前分配的 IP 地址和配置信息
inform	客户端发送的报文，用于通知 DHCP 服务器其当前的 IP 地址和配置信息

不同时期的平均响应时延（包括最大/最小时延）图展示了最大 / 最小 / 平均时延随时间变化的箱线图。

DHCP 表展示了网络上所有 DHCP 服务器动态分配的所有 IP 地址。

名称	描述
IP 地址	这是分配给客户端计算机的 IP 地址。点击该地址可以访问该 IP 地址的详细页面
主机名称	在 DHCP 请求时，客户端可以告知自己的主机名称
MAC 地址	客户端计算机的网络设备的地址。点击该地址可以访问该 MAC 地址的详细页面
子网掩码	与分配的 IP 地址对应的网络掩码
DHCP 服务器 IP 地址	为客户端动态分配 IP 地址的 DHCP 服务器的 IP 地址
分配时间	DHCP 服务器将该 IP 地址分配给客户端时的时间
租期	该 IP 地址有效的时间长度

11.5.2 DHCP 服务器



DHCP 服务器表展示了分析仪观测到的所有 DHCP 服务器的概览信息。

名称	描述
IP 地址	DHCP 服务器的 IP 地址
主机名称	DHCP 服务器宣告自己的主机名称
最近更新时间	该 DHCP 服务器最近一次更新的时间
成功请求数量	该 DHCP 服务器成功处理的 DHCP 请求数量
分配 IP 数量	该 DHCP 服务器成功分配的 IP 地址数量

12. 系统设置

12.1 系统信息

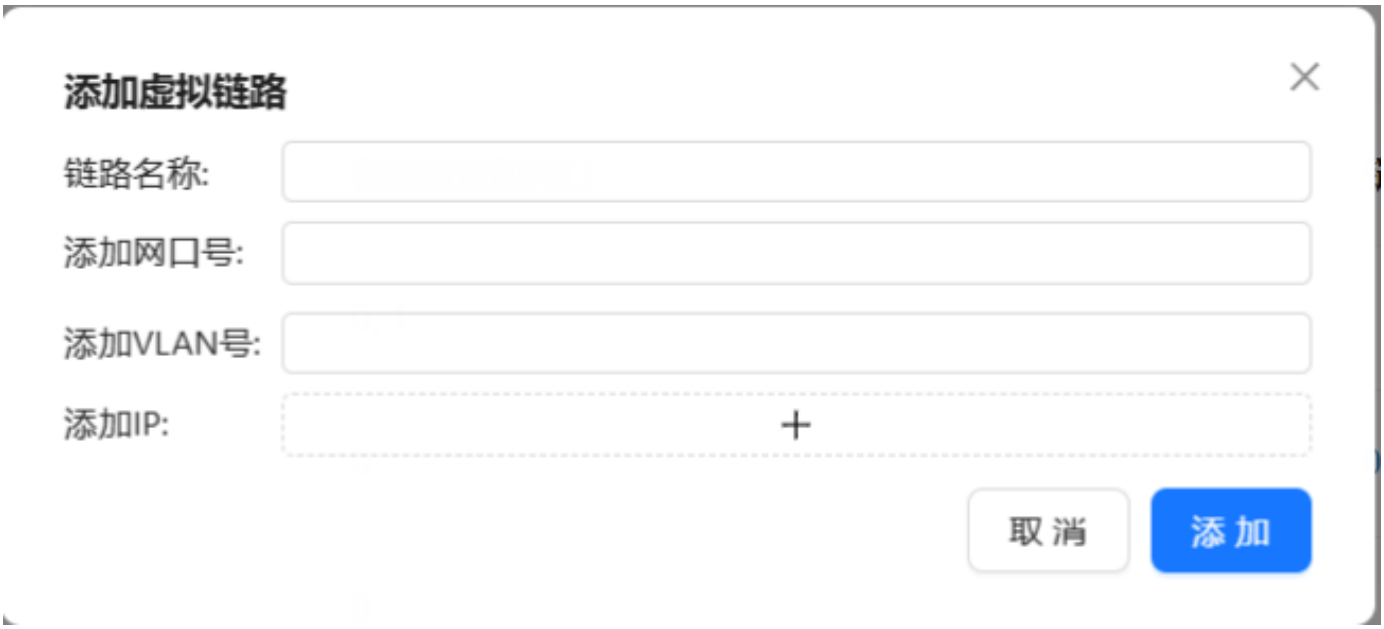
名称	描述	备注
系统描述		
版本	版本号	全局信息
开机时间	（程序总运行时长）程序开始运行的时间	全局信息
系统利用率		
统计信息时间跨度	（分析仪可用的统计信息的时长）最早的统计信息起始时间	全局信息
内存利用率	设备内存利用率	全局信息
系统总负载率	系统整体的负载率	全局信息
IO 模块占用率	系统 IO 模块（接收流量）的占用率	全局信息
分析模块占用率	系统分析模块（分析流量）的占用率	全局信息
主内存分配		
总内存	设备的总内存	全局信息
系统使用内存大小	流量分析程序所使用的内存大小	全局信息
硬盘分配		
硬盘总容量	硬盘总容量	全局信息
系统使用硬盘大小	系统使用的硬盘大小	全局信息
硬盘使用率	硬盘使用率，系统使用硬盘大小 / 硬盘总容量	全局信息
全局统计计数		
存储的 MAC 数量	分析仪当前存储的 MAC 地址数量	当前虚拟链路信息
存储的 IP 数量	分析仪当前存储的 IP 数量	当前虚拟链路信息
最大连接数量	分析仪观测到的最大连接计数	当前虚拟链路信息
活跃连接数量	当前活跃的连接计数	当前虚拟链路信息

12.2 数据过滤

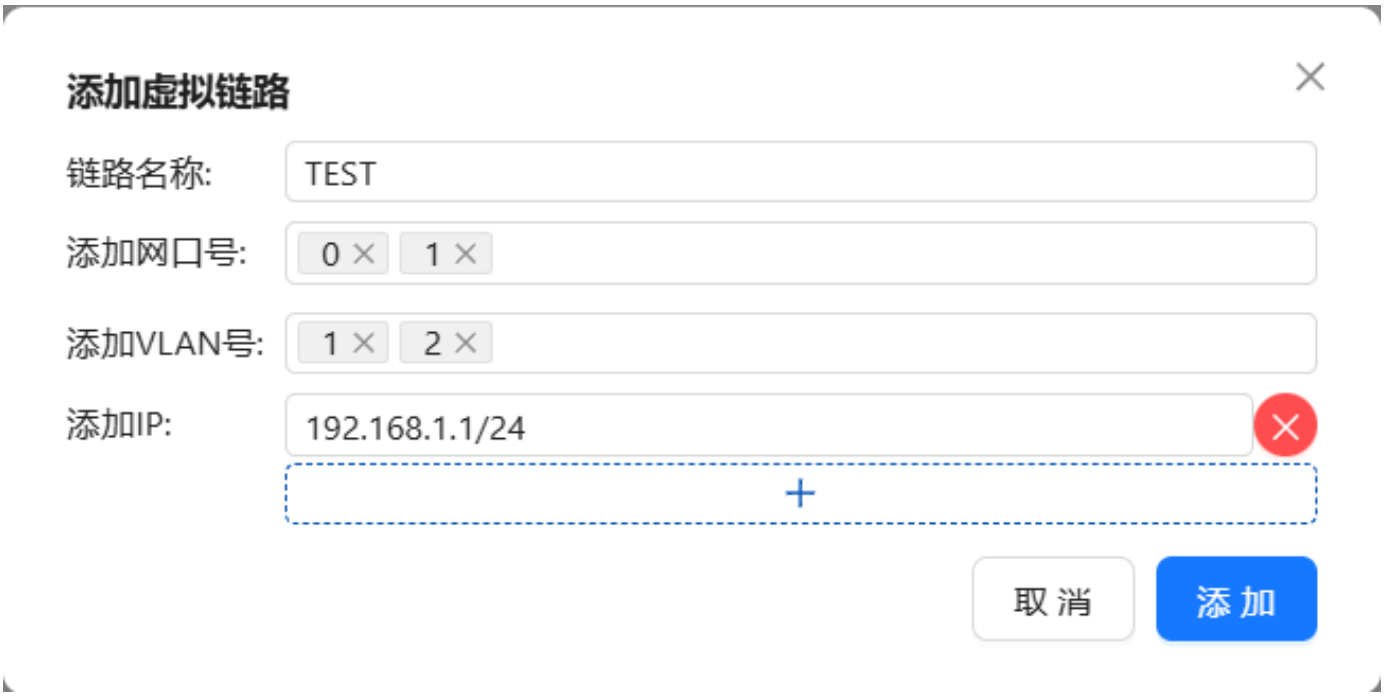
12.2.1 虚拟链路

当设备多个网口接收镜像不同来源的流量，为了区分每个网口或不同类型的流量，可根据链路实现区分。
界面在呈现流量分析结果时也可以分链路进行显示，通过点击界面顶部的虚拟链路按钮切换不同的虚拟链路。每条虚拟链路的统计数据是严格区分的。

此页面可根据网口、VLAN配置虚拟链路。



点击**添加虚拟链路**按钮，再点击**添加链路配置**按钮，填写链路名称，勾选需配置的规则(网口或VLAN)，配置规则，最后点击 **添加** 按钮即可添加虚拟链路。

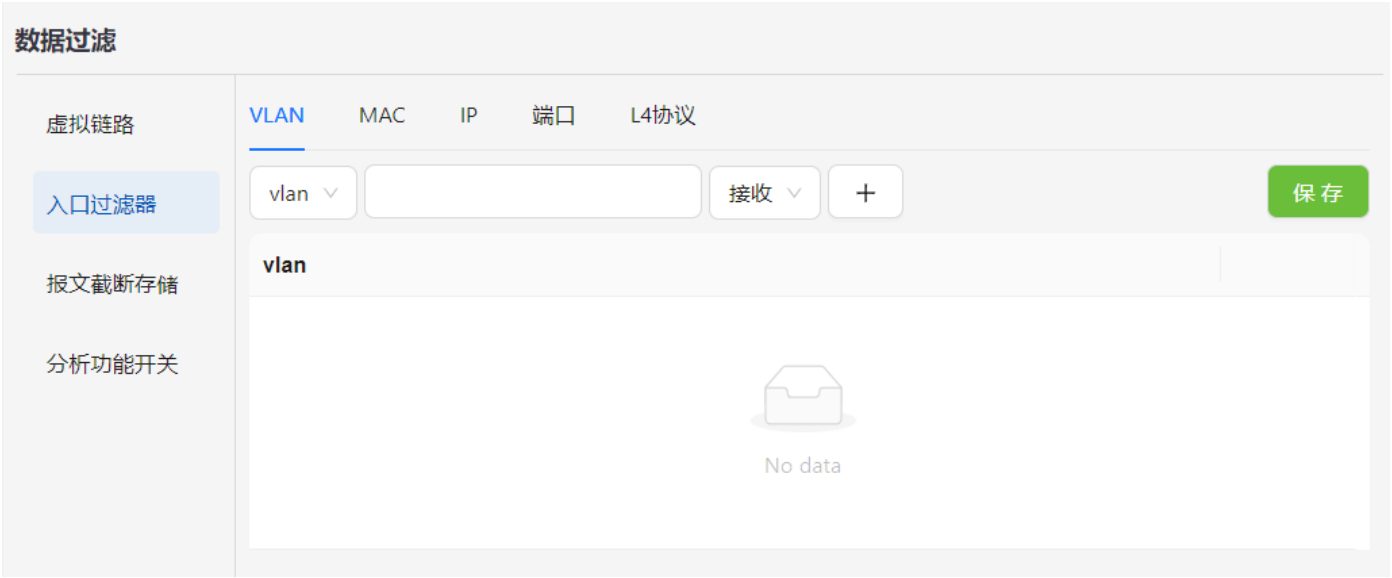


每条规则内的值为 **或（OR）** 的关系，如图中网口号规则中的 1 和 2，表示网口 1 或 网口 2 的流量。

不同规则之间为 **且（AND）** 的关系，如图中的网口号规则和 VLAN 规则，表示将网口 1 或网口 2 接收到的，VLAN ID 为 0 或 3999 的，IP 地址范围为 192.168.1.1/24 的流量划分至一条虚拟链路。

> 注意：
>
> 1. 每条链路的数据顺序代表链路优先级,拖动数据列可以对其进行调整,默认链路无法修改链路优先级也无法删除。
> 2. 除默认链路外，一个数据被只会被纳入一条虚拟链路并进行统计。每个数据包都会被纳入默认链路并进行统计。默认链路 **无法删除**。

12.2.2 入口过滤器



此页面可以配置入口过滤器，该配置全局生效。可以通过配置过滤表达式以接收/丢弃特定的流量，只有接收的流量才会被分析仪分析，被丢弃的流量将不被分析仪分析。

此功能可以排除无关流量，从而只分析受关注的流量，降低分析仪的分析负载，延长内存数据库的可用数据时长。

支持对如下条件配置入口过滤表达式：

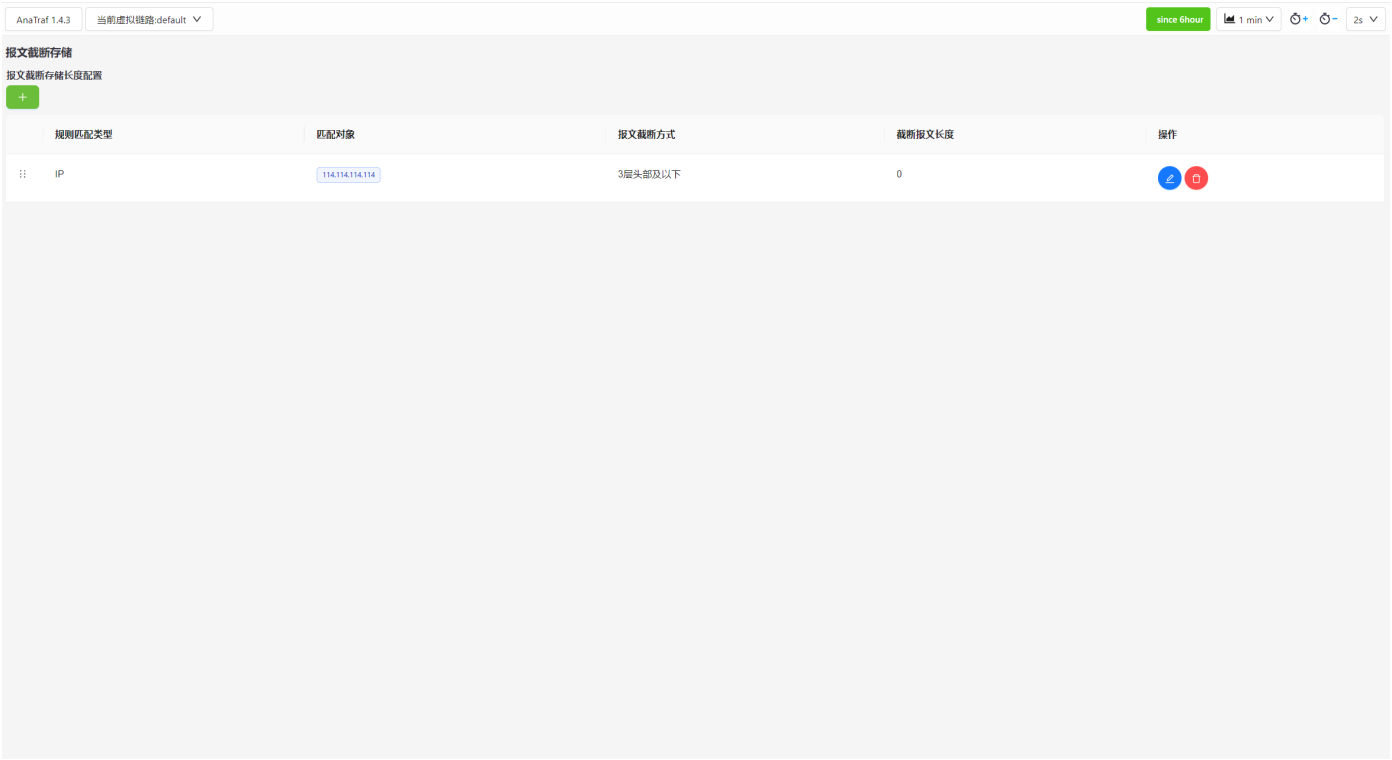
- VLAN
- MAC 地址
- IP 地址，IP 地址支持掩码的形式，如 192.168.1.1/24
- 端口，支持以 “123-456” 的形式填写端口范围，左右均为闭区间。
- L4 协议

每个过滤条件可以选择接收或丢弃被此过滤条件匹配的流量。

配置完成后，点击右上角 **保存** 按钮。

> **注意：** 同类型（如 VLAN）的过滤表达式之间为 **或（OR）** 关系，不同类型（如 VLAN 和 IP）的表达式之间为 **且（AND）** 关系。

12.2.3 报文截断存储



此页面可展示了分析仪的报文截断存储规则，配置报文截断存储，能够节省硬盘空间。

分析仪提供了两条常用的报文截断规则：

1. 截断 payload： 所有报文的 payload 将被截断。
2. 截断 HTTPS payload：所有加密流量的报文的 payload 将被截断。

点击绿色的 **“+”** 按钮可以添加自定义的截断规则。

匹配对象包括：

1. MAC地址
2. IP地址
3. VLAN ID

4. 网口号
5. 端口号
6. 7层协议
7. 所有报文

匹配值填写需匹配的值，如匹配对象选择了MAC地址，那么，此处填写需匹配的MAC地址。

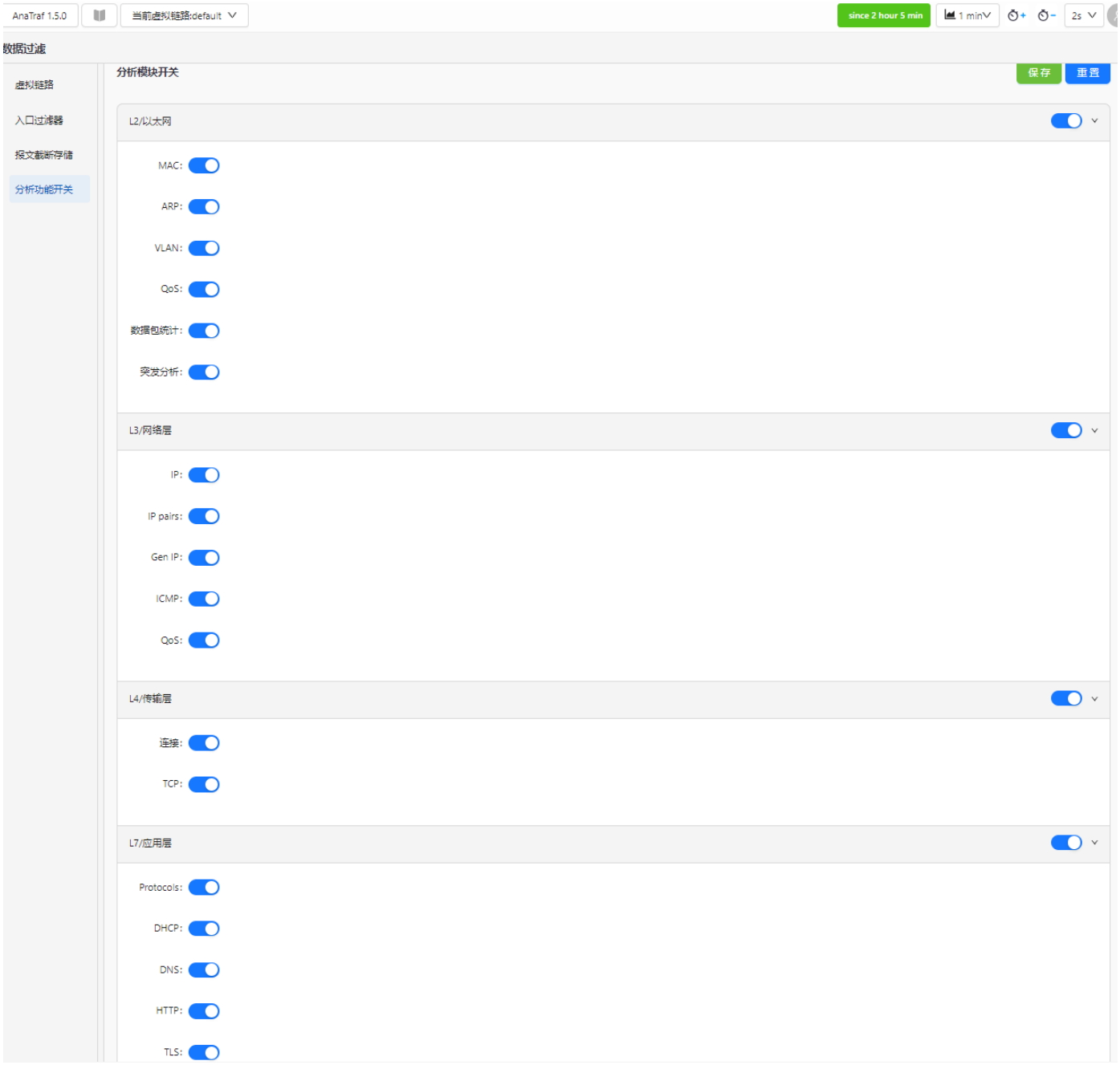
报文截断方式包括：

1. 固定报文长度
2. 丢弃报文
3. 不截断
4. 保留 3 层头部及以下
5. 保留 4 层头部及以下
6. 保留 7 层数据固定程度及以下

报文截断长度填写截断后的报文长度。

> **注意：** 如果设置了报文截断存储，被截断流量的 PCAP 下载与 TCP 流重组将不可用。

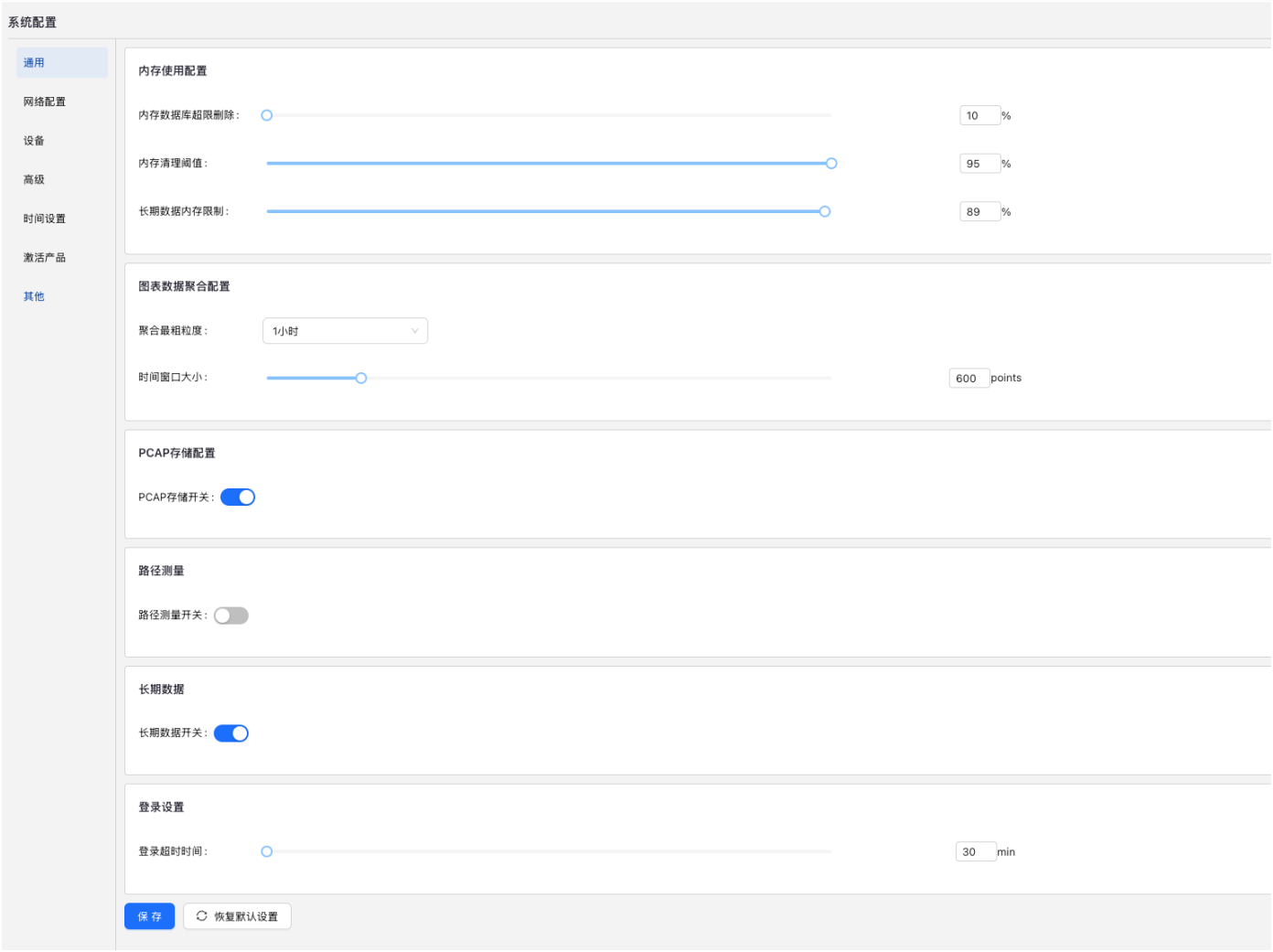
12.2.4 分析功能开关



分析功能开关设置允许配置分析仪主动处理和分析哪些 OSI 层（2，3，4，7）或者具体的一个分析模块。通过禁用一些不需要的分析模块，可以提升分析仪的性能。

> **注意：** 当关闭某个分析模块时，所有依赖此分析模块的其他模块也将关闭。

12.3 系统配置



12.3.1 通用

12.3.1.1 内存使用配置

- **内存数据库超限删除**：当内存数据库使用的内存达到阈值时，将按百分比删除数据。
- **内存清理阈值**：内存数据库可使用的最大内存占总内存的比值。
- **长期数据内存限制**：将长期数据读取到内存时，允许使用的最大内存大小。

12.3.1.2 图表数据聚合配置

- **聚合最粗粒度**：可选 1 秒、10 秒、1 分钟、10 分钟、1 小时。

为了使内存数据库能够存储的历史统计数据尽可能的长，内存数据库将对历史数据进行聚合。分析仪提供最高的统计数据精度为 1 秒。时间窗口决定了各精度统计数据的可用时长。

例如，选择聚合最粗粒度为 1 秒，意味着分析仪将不对历史数据进行聚合，从而始终提供最高精度的统计数据；选择最粗粒度为 1 小时，时间窗口设置为 600，则历史数据的聚合效果如下：

1秒粒度:趋势图显示最近 10 分钟的网络状态，最小时间粒度为 1 秒。

10秒粒度:趋势图显示最近 100 分钟的网络状态，最小时间粒度为 10 秒。

1分钟粒度:趋势图显示最近 10 小时的网络状态，最小时间粒度为 1 分钟。

10分钟粒度:趋势图显示最近 100 小时的网络状态，最小时间粒度为 10 分钟。

1小时粒度:趋势图显示最近 25 天内以最小时间粒度为 1 小时的网络状态。

12.3.1.3 PCAP 存储配置

- **PCAP存储开关**：是否开启 PCAP 存储。该开关可以控制分析仪是否对流量进行存储。

> **注意：** 当 PCAP 存储开关为关闭状态时，PCAP 下载功能、在线解码功能、TCP 时序图功能将不可用。

12.3.1.4 路径测量

- **路径测量开关**： 是否开启路径测量功能。该开关可以控制分析仪是否开启路径测量功能。

> **注意：** 为保证分析仪的分析性能，仅在需要时开启路径测量功能。

12.3.1.5 数据持久化 / 长期数据库

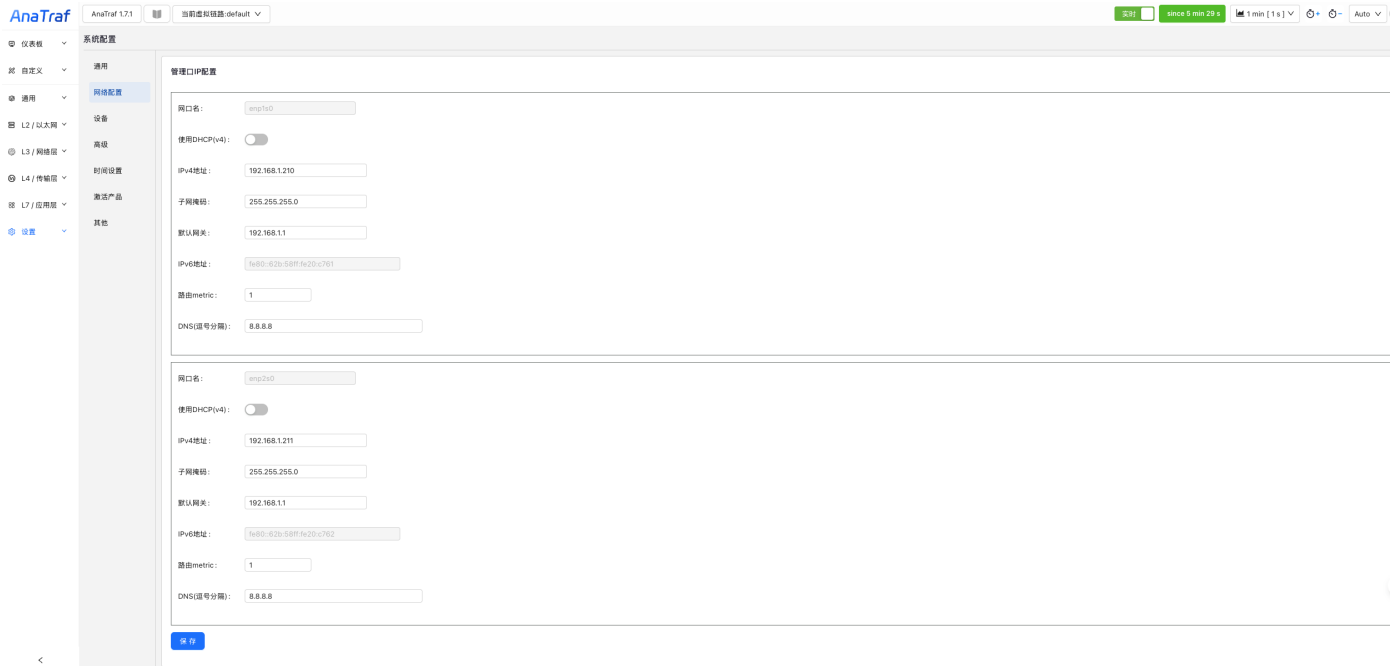
- **长期数据库开关**： 是否开启长期数据库功能。如果此功能启用，可以通过 WEB 界面右上角的长期数据库切换按钮在实时数据和长期数据之间切换。

12.3.1.6 登录超时设置

- **登录超时时间**： 可以设置登录超时时间，达到超时时间后，将自动登出。

12.3.2 网络配置

12.3.2.1 管理口网络配置



在此配置页面，可以配置流量分析仪管理网口的 IPv4 地址。

- **IPv4 地址**：填写待修改的 IPv4 地址。
- **网关**：填写待修改的网关。

- **子网掩码**：填写待修改的子网掩码。
- **路由metricc**：衡量路由的优先级数值。

填写好网络配置信息后，点击 **保存** 按钮，随后使用新的管理网口的 IP 地址访问 WEB GUI 界面。

> **注意：** 若设备支持多管理口配置，各个管理口的配置都会在此显示。

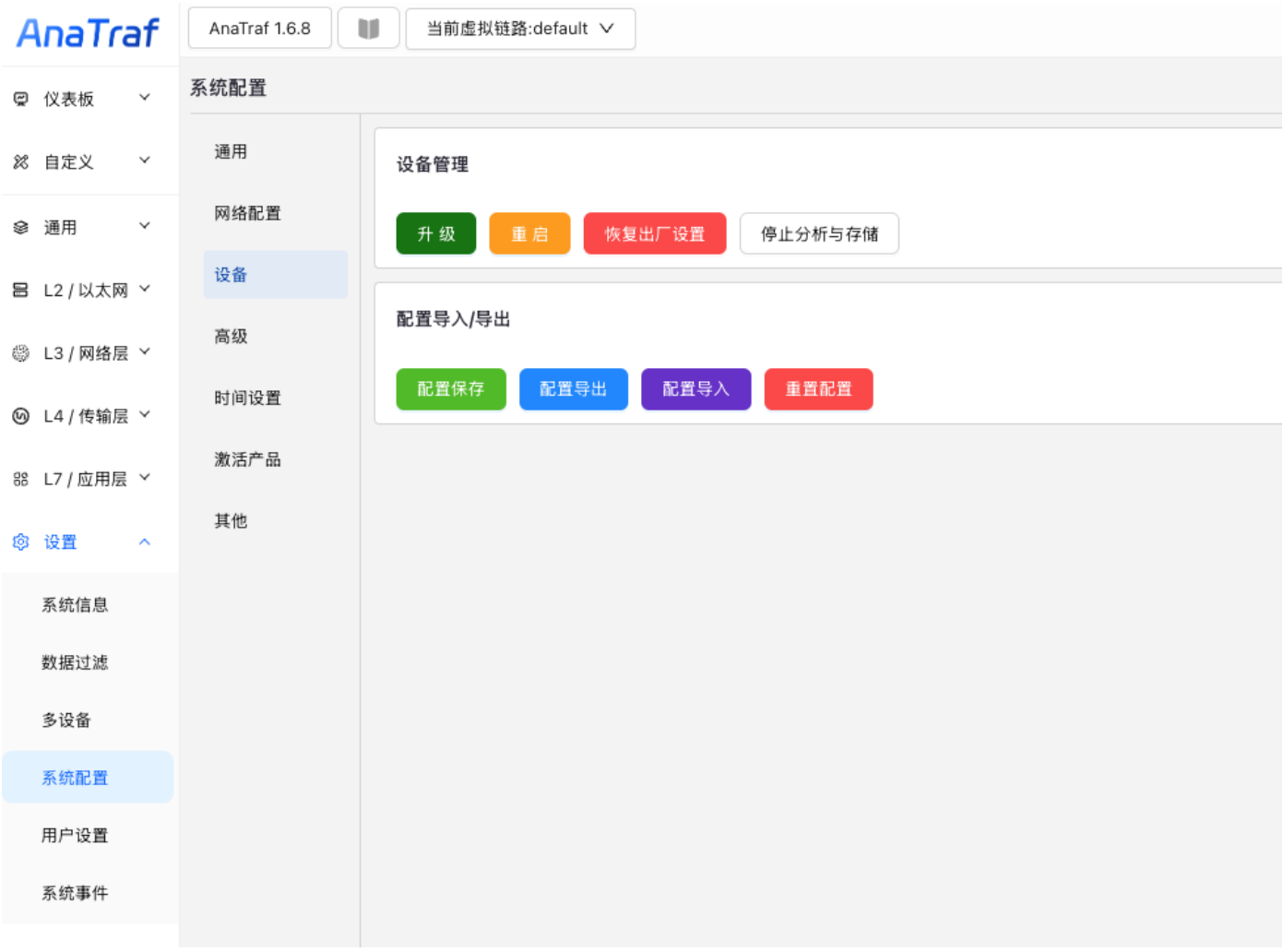
12.3.2.2 访问控制 / IP 白名单

支持基于 IP 白名单的访问控制机制，可有效提升系统安全性。启用后，仅允许白名单中指定的 IP 地址访问系统，其他所有访问请求将被拒绝。

添加白名单时支持 IPv4、IPv6 地址，支持掩码，并且可以添加任意数量的 IP 白名单规则。

> **注意：** 二层和三层网络协议的流量（如 ARP、ICMP）不受 IP 白名单限制，相关报文不会被拦截。

12.3.3 设备管理



12.3.3.1 系统重启 / 升级 / 重置

点击 **重启** 按钮，分析仪将重启。

点击 **升级** 按钮，将跳转至升级页面。

点击 **恢复出厂设置**，验证用户名和密码后，系统将重置为出厂状态。

> **注意：**
>
> 1. 重启后，内存数据库所有的流量分析数据将丢失。
> 2. 恢复出厂设置不会变更管理口的网络配置。

12.3.3.2 停止分析与存储

当开启 **停止分析与存储** 设置，分析仪将停止数据包的分析与存储。所有的统计数据和图表不再更新，但数据仍然保留，可以进行查询。

开启 / 关闭 **停止分析与存储**，无需重启。

> **注意：** 如果分析仪在转发模式下运行，即使停止数据包的分析与存储，流量仍然会正常转发。

12.3.3.3 系统配置导入/导出

系统配置导入/导出功能提供以下 4 种操作：

1. **配置保存：** 点击此按钮，将分析仪当前的配置以文件的形式保存在分析仪上。
2. **配置导出：** 点击此按钮，将下载分析仪当前的配置文件。
3. **配置导入：** 点击此按钮，可以上传分析仪的配置文件并已覆盖的形式导入到分析仪。
4. **重置配置：** 点击此按钮，可以将分析仪的配置还原为**上一次点击<配置保存>按钮时**的配置。

> **注意：**
>
> 1. 导出的配置文件不可修改。
> 2. 配置导入/导出功能设计的范围为： 系统配置中的内容、数据过滤配置、事件规则配置、用户设置。

12.3.4 高级

12.3.4.1 转发 / 镜像模式切换

可以切换分析仪的模式，支持切换转发模式和镜像模式。

> **注意：** 转发模式时，相邻的两个网口组成一对转发网口，如网口 0 和网口 1，网口 2 和网口 3 。切换模式需重启设备。

12.3.4.2 在线解码内存限制

可以设置为在线解码功能预留的内存大小。此选项影响在线解码功能预览的报文数量以及内存数据库的数据可用时长。

> **注意：** 更改此设置需重启设备。

12.3.5 时间设置

12.3.5.1 本地时间同步

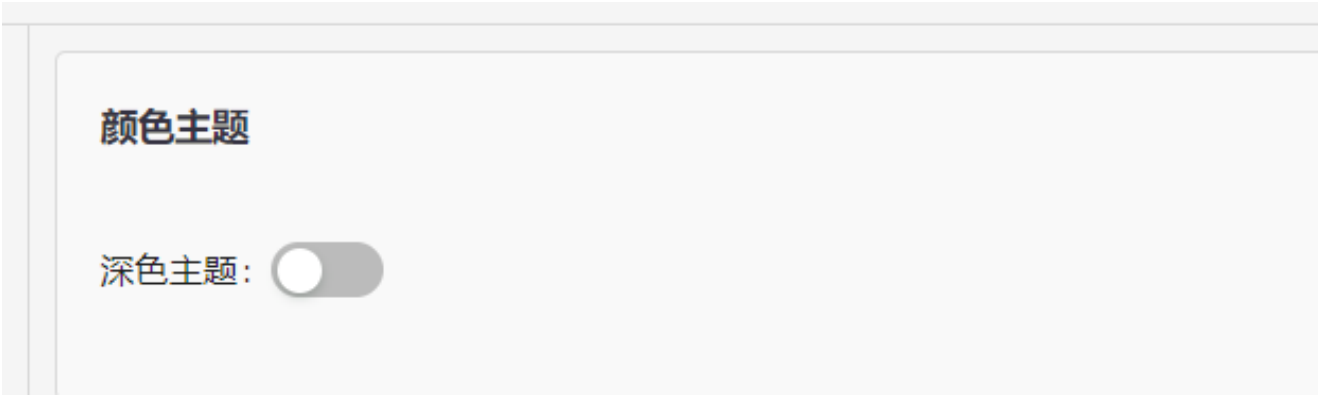
本地时间同步选项将使用控制端的时间进行同步。

12.3.5.2 NTP 时间同步

NTP 时间同步选项可指定 NTP 服务器进行时间同步。

12.3.6 其他

12.3.6.1 切换主题



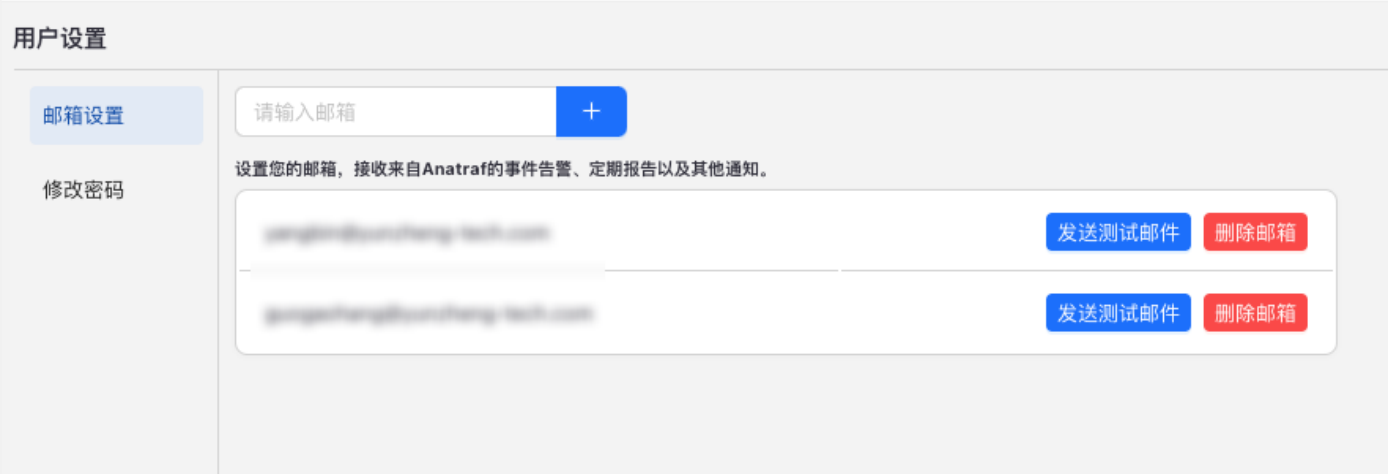
点击按钮，可以切换深色 / 浅色主题。

12.4 用户设置

12.4.1 修改密码

此页面可以修改分析界面的登陆密码。更改的新密码要求：至少为8位，且包含数字、大小写字母和特殊符号。

12.4.2 邮件设置



用户可以在此填写电子邮件地址，用于接收流量分析仪的事件告警、定期报告及其他通知。

点击 **发送测试邮件** 按钮，可以向邮箱发送一封测试邮件。如果邮箱收到测试邮件，则表明邮箱设置成功。

anatraf

发件人 anatraf <admin@anatraf.com> 隐藏

收件人 [redacted]

时间 2025年2月14日 周五 9:51

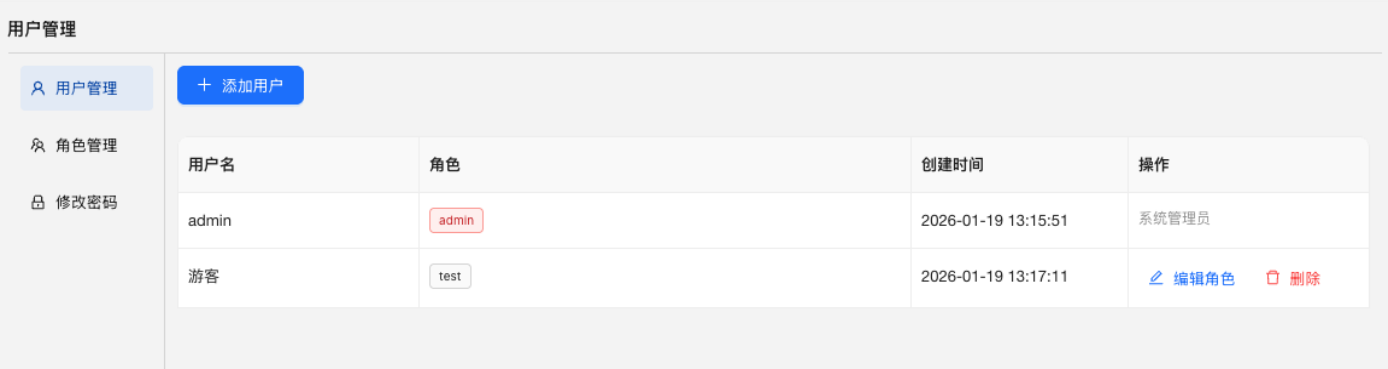
大小 1.9K

收到此邮件表示邮件设置正确

12.5 用户管理与权限管理

AnaTraf 网络流量分析仪提供了完善的用户管理与权限管理系统，支持多用户、多角色的权限控制，确保系统安全性和操作规范性。

12.5.1 用户管理



用户管理功能允许系统管理员创建、编辑和删除用户账户，并为用户分配相应的角色，从而控制用户对系统功能的访问权限。

> **注意：** 用户管理功能需要相应的权限才能访问。只有拥有 `system:user:view` 权限的用户才能查看用户列表，拥有 `system:user:create`、`system:user:edit`、`system:user:delete` 权限的用户才能执行相应的操作。

12.5.1.1 用户列表

用户列表页面显示系统中所有用户的基本信息，包括：

- **用户名**：用户的登录账号名称
- **角色**：用户当前拥有的角色，以标签形式显示，不同角色使用不同颜色标识
- **创建时间**：用户账户的创建时间
- **操作**：可对用户执行的操作（编辑角色、删除用户等）

在用户列表中，系统默认的 `admin` 用户会被特殊标记，无法删除，且必须保留管理员角色。

12.5.1.2 添加用户

点击用户列表页面的 **添加用户** 按钮，打开添加用户对话框。

添加用户时需要填写以下信息：

- **用户名**：必填，用于登录系统的账号名称，不能为空
- **密码**：必填，用户登录密码，长度至少为 6 位
- **确认密码**：必填，需要与密码保持一致
- **角色**：可选，可以为新用户选择一个或多个角色。如果不选择角色，用户将无法访问需要权限的功能

填写完成后，点击 **确定** 按钮创建用户。创建成功后，新用户将出现在用户列表中。

> **注意：**
>
> 1. 用户名不能与现有用户重复
> 2. 密码建议使用强密码，包含数字、大小写字母和特殊字符
> 3. 创建用户后，建议立即为用户分配合适的角色，以确保用户能够正常使用系统功能

12.5.1.3 编辑用户角色

在用户列表中，点击某个用户的 **编辑角色** 按钮，可以修改该用户的角色分配。

在编辑角色对话框中：

- 可以查看用户当前拥有的所有角色
- 可以通过勾选/取消勾选来添加或移除角色
- 可以为用户分配多个角色，用户将拥有所有分配角色的权限集合

修改完成后，点击 **确定** 按钮保存更改。角色修改后，用户的权限将立即更新，但需要重新登录才能生效。

> **注意：**
>
> 1. 不能移除 `admin` 用户的 `admin` 角色
> 2. 修改用户角色后，该用户的所有现有登录会话的权限版本将失效，需要重新登录
> 3. 如果用户当前没有分配任何角色，将只能访问不需要权限的公共功能

12.5.1.4 删除用户

在用户列表中，点击某个用户的 **删除** 按钮，可以删除该用户账户。

删除用户前，系统会弹出确认对话框，要求确认删除操作。确认删除后，该用户账户将被永久删除，包括：

- 用户的所有登录会话将被终止
- 用户的角色分配将被清除
- 用户相关的操作记录将保留在系统日志中

> **注意：**
>
> 1. 不能删除系统默认的 `admin` 用户
> 2. 删除用户是不可逆操作，请谨慎执行
> 3. 删除用户后，该用户的所有权限将立即失效

12.5.2 角色管理

角色管理功能允许系统管理员创建、编辑和删除角色，并为角色分配权限。通过角色管理，可以实现细粒度的权限控制，确保不同用户只能访问其职责范围内的功能。

> **注意：** 角色管理功能需要相应的权限才能访问。只有拥有 `system:role:view` 权限的用户才能查看角色列表，拥有 `system:role:create`、`system:role:edit`、`system:role:delete` 权限的用户才能执行相应的操作。

12.5.2.1 角色列表

角色列表页面显示系统中所有角色的信息，包括：

- **角色名称**：角色的标识名称
- **描述**：角色的功能描述
- **权限数量**：该角色拥有的权限总数
- **类型**：标识角色是否为系统预设角色（预设角色通常不能删除）
- **操作**：可对角色执行的操作（编辑、删除等）

系统预设了以下角色：

- **admin**：系统管理员，拥有所有权限
- **network_operator**：网络运维人员，拥有网络监控和配置相关权限
- **security_analyst**：安全分析师，拥有安全分析和事件管理相关权限
- **viewer**：查看者，仅拥有查看权限，无法进行配置修改

12.5.2.2 创建角色

点击角色列表页面的 **创建角色** 按钮，打开创建角色对话框。

创建角色时需要填写以下信息：

- **角色名称**：必填，角色的唯一标识名称，不能为空且不能与现有角色重复
- **描述**：可选，角色的功能描述，用于说明角色的用途

- **权限**：可选，可以为新角色选择一个或多个权限。创建角色时也可以不选择权限，后续再通过编辑功能添加权限

权限选择界面采用分组展示方式，权限按照功能模块进行分类：

- **仪表板**：仪表板的查看、创建、编辑、删除权限
- **数据查询**：数据查询、导出等权限
- **存储管理**：存储查看、导出、删除等权限
- **事件管理**：事件查看、规则配置等权限
- **系统配置**：系统配置查看、编辑等权限
- **用户管理**：用户和角色的管理权限
- **分析功能**：各种分析功能的权限

可以通过以下方式选择权限：

- 展开权限分组，查看该分组下的所有权限
- 使用搜索框快速查找权限
- 使用 **展开全部** 和 **收起全部** 按钮批量展开或收起所有分组
- 勾选需要的权限，取消勾选不需要的权限

填写完成后，点击 **确定** 按钮创建角色。创建成功后，新角色将出现在角色列表中。

> **注意：**
>
> 1. 角色名称建议使用有意义的名称，便于识别和管理
> 2. 创建角色时建议填写描述信息，说明角色的用途和适用场景
> 3. 可以根据实际需求，基于系统预设的角色模板快速创建角色

12.5.2.3 编辑角色

在角色列表中，点击某个角色的 **编辑** 按钮，可以修改该角色的基本信息（名称和描述）和权限分配。

在编辑角色对话框中：

- 可以修改角色的名称和描述
- 可以查看角色当前拥有的所有权限
- 可以通过勾选/取消勾选来添加或移除权限
- 系统预设角色的名称通常不能修改

修改完成后，点击 **确定** 按钮保存更改。角色权限修改后，所有拥有该角色的用户的权限将立即更新，但需要重新登录才能生效。

> **注意：**
>
> 1. 修改角色权限后，所有拥有该角色的用户的权限版本将失效，需要重新登录
> 2. 系统预设角色（如 `admin`）的某些属性可能受到保护，无法修改
> 3. 建议在修改角色权限前，先了解该角色当前被哪些用户使用，避免影响用户正常工作

12.5.2.4 分配权限

权限分配是角色管理的核心功能。系统提供了细粒度的权限控制，权限按照功能模块进行分类组织。

权限选择界面支持以下功能：

- **分组展示**：权限按照功能模块分组，便于查找和管理
- **搜索过滤**：可以通过权限名称或权限代码快速查找权限
- **批量操作**：支持展开/收起所有分组，提高操作效率
- **权限说明**：每个权限都有明确的名称和代码，便于理解权限的作用范围

常见的权限类别包括：

- **仪表板权限**：`dashboard:view`、`dashboard:create`、`dashboard:edit`、`dashboard:delete`
- **数据查询权限**：`query:view`、`query:export`、`query:ticket`
- **存储管理权限**：`storage:view`、`storage:export`、`storage:delete`
- **事件管理权限**：`incident:view`、`incident:rule:create`、`incident:rule:edit`、`incident:rule:delete`
- **系统配置权限**：`system:config:view`、`system:config:edit`、`system:control:reboot`、`system:control:reset`
- **用户管理权限**：`system:user:view`、`system:user:create`、`system:user:edit`、`system:user:delete`
- **角色管理权限**：`system:role:view`、`system:role:create`、`system:role:edit`、`system:role:delete`
- **分析功能权限**：`analysis:ws`、`analysis:replay`、`analysis:switch:edit` 等

> **注意：**
>
> 1. 用户拥有某个角色的所有权限，如果用户拥有多个角色，则用户拥有所有角色的权限集合
> 2. `admin` 角色拥有所有权限，无需单独分配
> 3. 权限分配应该遵循最小权限原则，只授予用户完成工作所需的最小权限

12.5.2.5 删除角色

在角色列表中，点击某个角色的 **删除** 按钮，可以删除该角色。

删除角色前，系统会弹出确认对话框，要求确认删除操作。确认删除后，该角色将被永久删除，包括：

- 角色的所有权限分配将被清除
- 所有拥有该角色的用户的该角色将被移除
- 如果用户删除角色后不再拥有任何角色，该用户将失去所有权限

> **注意：**
>
> 1. 不能删除系统预设角色（如 `admin`）
> 2. 删除角色是不可逆操作，请谨慎执行
> 3. 删除角色前，建议先检查哪些用户拥有该角色，并考虑是否需要先为用户分配其他角色

> 4. 删除角色后，所有拥有该角色的用户的权限版本将失效，需要重新登录

12.5.3 权限说明

系统采用基于角色的访问控制（RBAC）模型，通过权限代码来标识和控制用户对系统功能的访问。

权限代码采用 `模块:功能:操作` 的格式，例如：

- `dashboard:view`：查看仪表板
- `system:user:create`：创建用户
- `analysis:ws`：使用 Wireshark 分析功能

主要权限模块说明：

权限模块	说明	主要权限
dashboard	仪表板管理	view、create、edit、delete
query	数据查询	view、export、ticket
storage	存储管理	view、export、delete
incident	事件管理	view、delete、rule:view、rule:create、rule:edit、rule:delete
system	系统管理	config:view、config:edit、control:reboot、control:reset、user:view、user:create、user:edit、user:delete、role:view、role:create、role:edit、role:delete、network:view、network:edit、time:view、time:edit、license:edit 等
analysis	分析功能	ws、replay、switch:view、switch:edit、ingress_filter:view、ingress_filter:create 等
log	日志管理	system:view、system:export、user:view、user:export 等

权限检查机制：

- 系统在用户访问功能时，会自动检查用户是否拥有相应的权限
- 如果用户没有权限，系统会拒绝访问并提示权限不足
- 用户界面会根据用户权限动态显示或隐藏功能入口
- 权限检查在 API 层面和前端界面层面都有实现，确保安全性

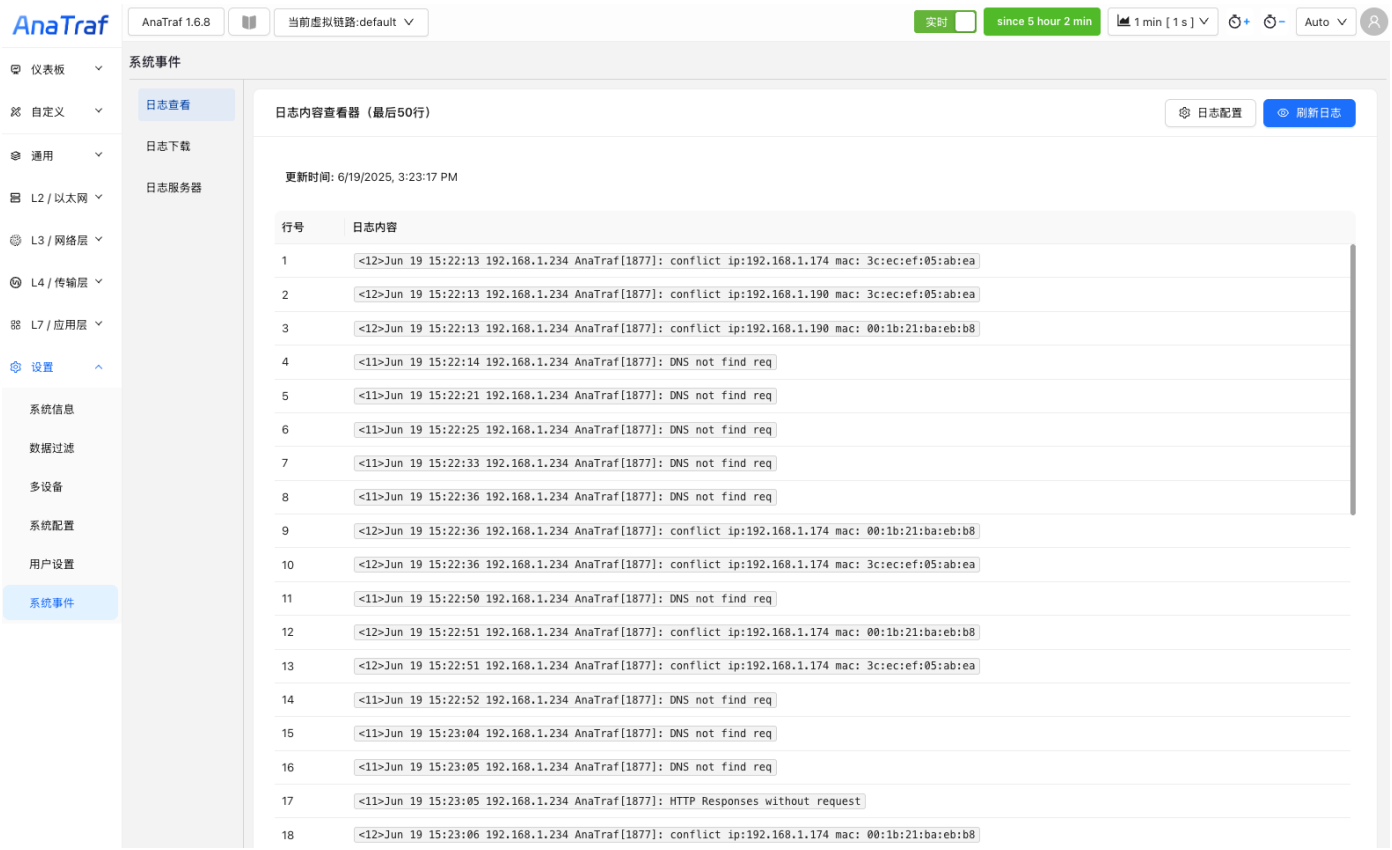
> **注意：**
>
> 1. 权限检查是实时的，权限变更后需要用户重新登录才能生效

> 2. `admin` 角色拥有所有权限，无需单独分配
> 3. 如果用户拥有多个角色，用户将拥有所有角色的权限集合（并集）
> 4. 权限分配应该遵循最小权限原则，只授予用户完成工作所需的最小权限

12.6 系统事件 / 日志

此页面展示系统事件内容，包括用户登录、登出、登录失败、操作记录、配置修改、数据导出等各类用户相关事件。

12.6.1 日志查看



此页面展示系统最新的 50 条日志。

12.6.1.1 日志配置

- **总大小**：日志文件的总大小。
- **日志级别**：有信息、警告、错误、严重四个等级，四者关系为“信息 < 警告 < 错误 < 严重”。选择某严重等级后，低于该等级的日志将不记录。
- **保存天数**：日志文件保存天数，最长30天。
- **syslog设施代码（facility）**：是一个用于标识日志消息来源模块的数字或名称，表示日志是从系统的哪个子系统或服务发出的。
- **日志主机名**：分析仪设备主机名。
- **应用程序名称**：分析仪软件应用程序名称。

设施名称	数值	描述
kern	0	内核消息
user	1	普通用户进程
mail	2	邮件系统
daemon	3	系统守护进程
auth	4	安全/认证相关（如login、sudo）
syslog	5	syslog自身的消息
lpr	6	打印系统
news	7	新闻子系统（NNTP等）
uucp	8	Unix-to-Unix Copy系统
cron	9	定时任务相关
authpriv	10	私密的认证信息
ftp	11	FTP服务
local0-7	16	本地自定义用途

设施代码与“严重性等级”（severity level）一起组成Syslog消息的优先级（priority）

```
priority = (facility × 8) + severity
```

12.6.2 日志下载

此页面可下载日志文件。

12.6.3 日志服务器 / syslog

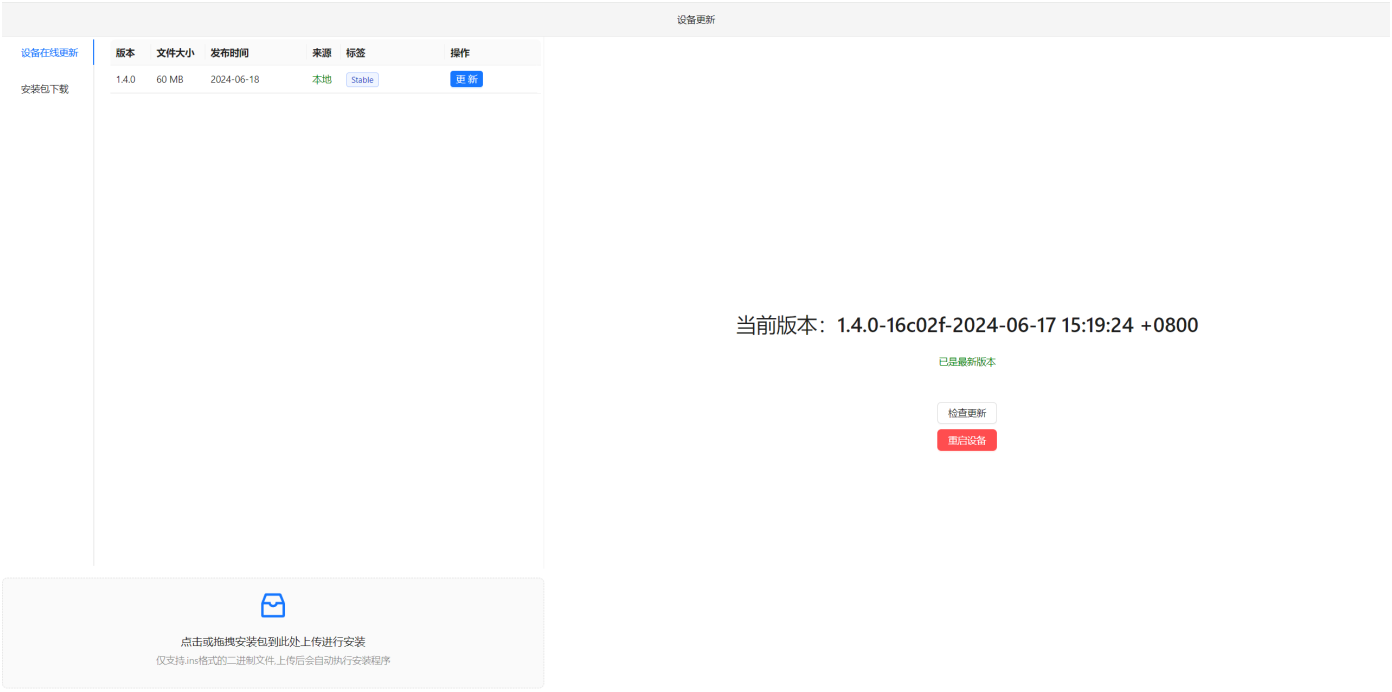
此页面可以配置 syslog 日志服务器。

- **配置名称**： 配置名称。
- **协议类型**： TCP 或 UDP。
- **服务器地址**： syslog 服务器地址。
- **端口**： syslog 服务器端口。默认 514 。
- **日志级别**： 有信息、警告、错误、严重四个等级，四者关系为“信息 < 警告 < 错误 < 严重”。选择某严重等级后，低于该等级的日志将不转发syslog服务器。
- **syslog设施代码**：是一个用于标识日志消息来源模块的数字或名称，表示日志是从系统的哪个子系统或服务发出的。
- **日志主机名**：分析仪设备主机名。
- **应用程序名称**：分析仪软件应用程序名称。

13. 系统更新

AnaTraf 网络流量分析仪提供通过 WEB 界面进行系统更新和还原的方法。

通过浏览器打开 **IP地址:8999**,进入如下页面：



> **注意：** 如果您修改了分析仪管理网口的 IP 地址，请通过浏览器访问 **“分析仪管理网口的IP地址:8999”**。

13.1 检查更新

点击检查更新，将提示当前版本是否是最新版本。

13.2 在线更新

当分析仪设备部署在能够联网的环境中时，可以使用在线更新。系统将自动检测云端的可用版本，并以列表的形式展示。

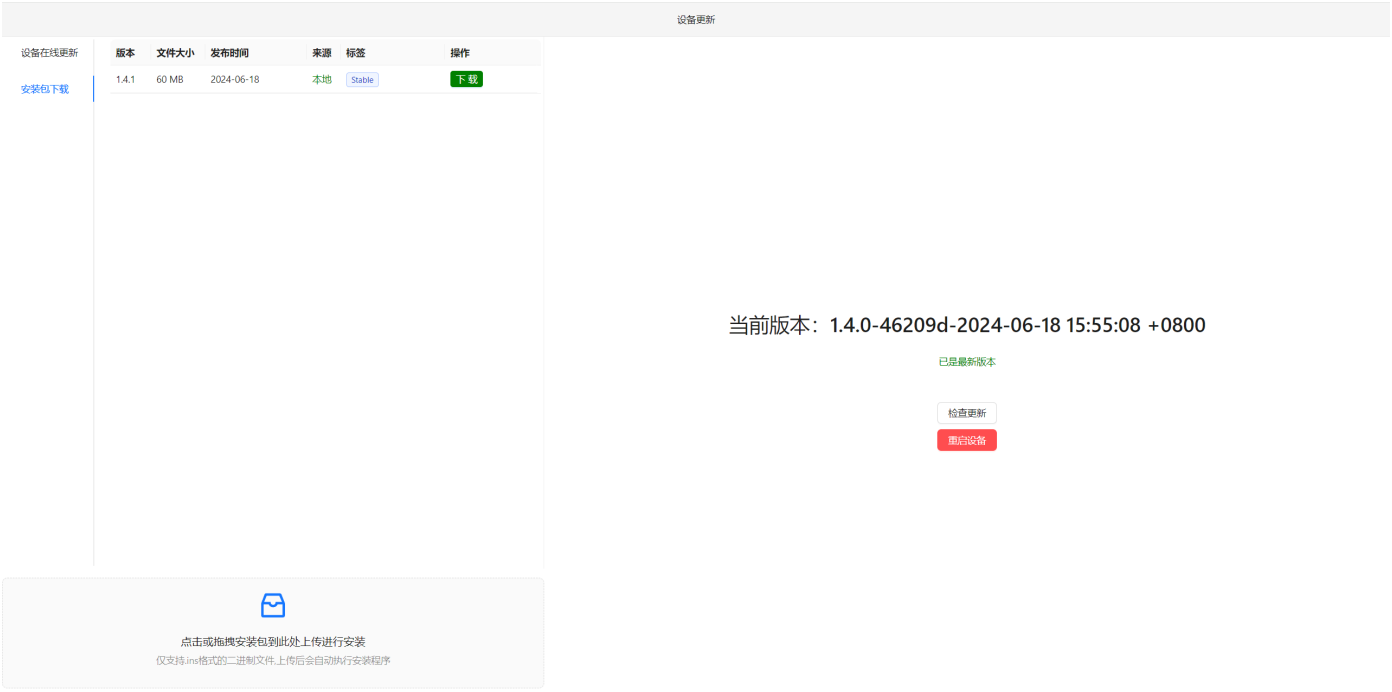
列表中每一行的版本将显示版本号、文件大小、发布时间、来源（本地或云端）和版本的标签信息。

点击特定版本对应的操作按钮，即可下载安装包进行升级。

13.3 安装包下载

当分析仪设备部署的环境不能联网时，可以在此选项卡进行更新升级。此方法要求控制端的设备能够联网。

点击特定版本对应的操作按钮，安装包将下载至控制端设备。然后，通过“点击或拖拽安装包到此处上传进行安装”，进行更新。



文件上传完成后，浏览器会弹出**上传更新成功，请重启**的窗口，点击 **重启设备**按钮。

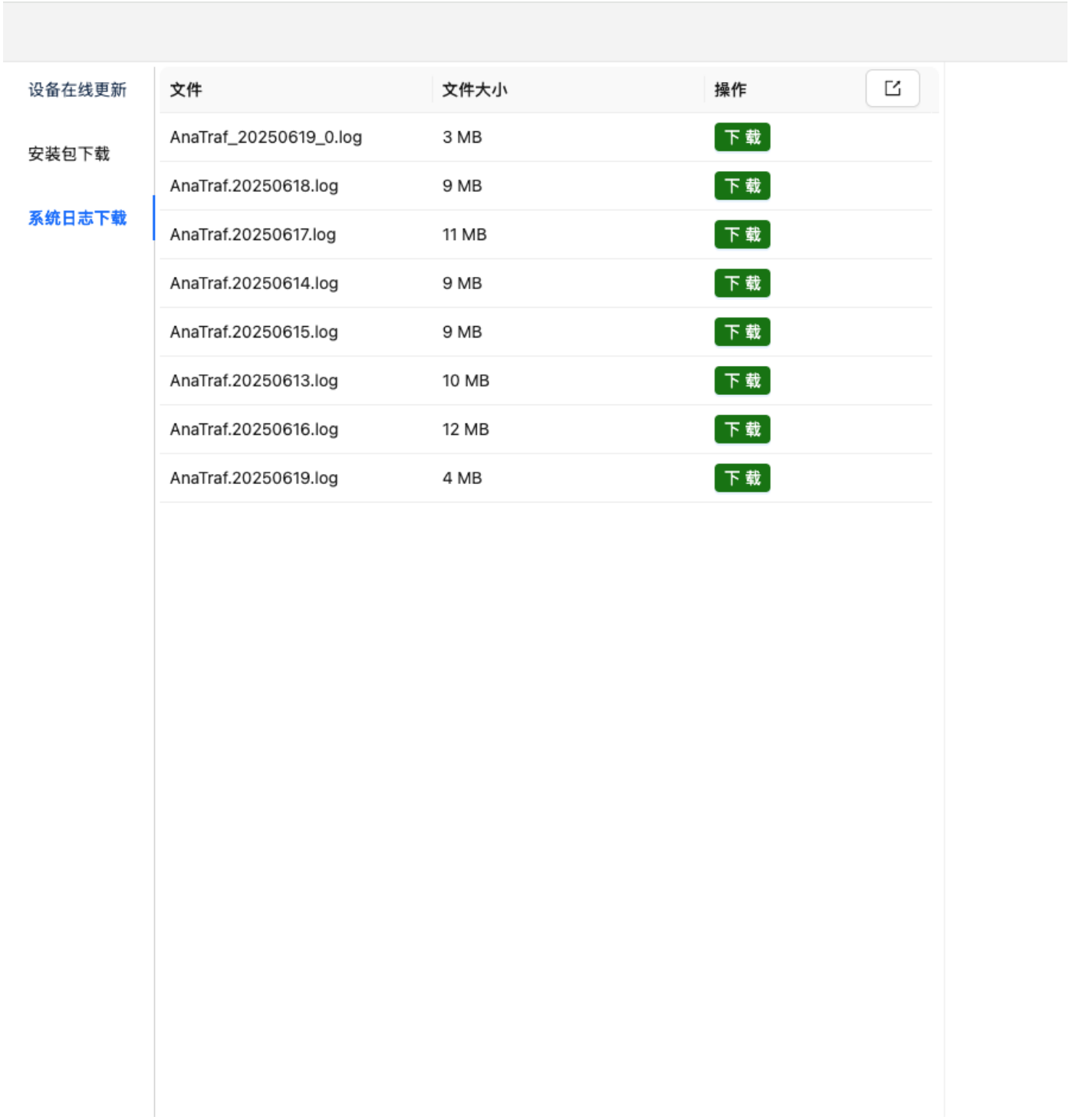
> **注意：** 设备重启后，系统更新或还原完成。系统更新后，须清空浏览器缓存，避免新的配置不生效。

13.4 自动回滚

如果分析仪当前版本发生崩溃，分析仪将会保存部分崩溃时的信息，并且当分析仪或控制端处于能够联网的环境下时，自动将崩溃信息上传至云端。详细内容请参考用户体验计划。

当系统崩溃后，设备将检测本地以及云端的可用版本列表，自动回滚至最近的稳定版本(具有 Stable 标签的版本)，回滚完成后，系统将自动重启。

13.5 日志下载



此处可以下载流量分析仪的系统运行日志。

附录一：表格过滤关键字

L2 - MAC 模块关键字

关键字	描述	示例
mac_address	MAC 地址	mac_address == aa:bb:cc:dd:ee:ff
nic_vendor	网卡供应商	nic_vendor == intel
mac_dhcp_name	DHCP 名	mac_dhcp_name == peter
mac_os_name	操作系统	mac_os_name == xxx
first_activity_time	首次活动时间	-
last_activity_time	上次活动时间	-
tx_pkts	发送包数	tx_pkts > 10
rx_pkts	接收包数	rx_pkts > 10
tx_bytes	发送字节数	tx_bytes > 10
rx_bytes	接收字节数	rx_bytes > 10
tx_pps	每秒发送包数	tx_pps > 10
rx_pps	每秒接收包数	rx_pps > 10
tx_bps	发送速率	tx_bps > 10
rx_bps	接收速率	rx_bps > 10
peer_mac_count	对等 MAC 数	peer_mac_count > 10
peer_ip_count	活跃 IP 数量	active_ip_cont > 10
peer_flow_count	活跃连接数	active_flow_count > 10
l7_protocol	L7 协议	l7_protocols == http

L2 - ARP 模块关键字

关键字	描述	示例
MAC 地址页		
mac_address	MAC 地址	mac_address == aa:bb:cc:dd:ee:ff
nic_vendor	网卡供应商	nic_vendor == intel
mac_dhcp_name	DHCP 名	mac_dhcp_name == peter
mac_os_name	操作系统	mac_os_name == xxx
request_count	ARP 请求数量	request_count > 10000
response_count	ARP 回复数量	response_count >= 10
ip_address	最近宣告 IP	ip_address == 192.168.1.141
ip_dhcp_name	DHCP 名	ip_dhcp_name == peter
dns_name	DNS 名	dns_name == peter
http_name	HTTP 名	
tls_name	TLS 名	tls_name == xxx
ip_os_name	操作系统	ip_os_name == xxx
region	地区	region == xxx
different_ips	使用过的 IP	different_ips == 192.168.1.1
IP 地址页		
different_macs	使用过的 MAC	different_macs == aa:bb:cc:dd:ee:ff

L2 - VLAN 模块关键字

关键字	描述	示例
vlan_id	VLAN ID	vlan_id == 0
pkts	数据包数	pkts == 0
bytes	总字节数	bytes == 0

L2 - QoS 模块关键字

关键字	描述	示例
vlan_qos	VLAN QOS	vlan_qos == 0
pkts	数据包数	pkts == 0
bytes	总字节数	bytes == 0
pps	每秒包数	pps > 10
bps	每秒流量	bps > 1000

L3 - IP 模块关键字

关键字	描述	示例
ip_address	IP 地址	ip_address == 192.168.1.1/24
region	地区	region == xxx
ip_dhcp_name	DHCP 名	ip_dhcp_name == peter
dns_name	DNS 名	dns_name == peter
http_name	HTTP 名	http_name == xxx
tls_name	TLS 名	tls_name == xxx
ip_os_name	操作系统	ip_os_name == xxx
mac_address	MAC 地址	mac_address == aa:bb:cc:dd:ee:ff
first_activity_time	首次活动时间	-
last_activity_time	上次活动时间	-
tx_pkts	发送包数	tx_pkts > 10
rx_pkts	接收包数	rx_pkts > 10
tx_bytes	发送字节数	tx_bytes > 10
rx_bytes	接收字节数	rx_bytes > 10
tx_pps	每秒发送包数	tx_pps > 10
rx_pps	每秒接收包数	rx_pps > 10
tx_bps	发送速率	tx_bps > 10
rx_bps	接收速率	rx_bps > 10
peer_ip_count	对等 IP 数	peer_ip_count > 10
tx_mtu	上行 MTU	tx_mtu > 1500
rx_mtu	下行 MTU	rx_mtu > 1500

tcp_count	TCP 包数量	tcp_count > 10
udp_count	UDP 包数量	udp_count > 10
tx_tcp_payload	发送 TCP 载荷	tx_tcp_payload > 10
rx_tcp_payload	接收 TCP 载荷	rx_tcp_payload > 10
tx_retransmit_bytes	发送 TCP 重传流量	tx_retransmit_bytes > 10
rx_retransmit_bytes	接收 TCP 重传流量	rx_retransmit_bytes > 10
tx_retransmit_rate	发送 TCP 重传率(比率为万分之一)	tx_retransmit_rate > 5000
rx_retransmit_rate	接收 TCP 重传率(比率为万分之一)	rx_retransmit_rate > 5000
tx_syn_count	发送 TCP SYN 包数量	tx_syn_count > 10
rx_syn_count	接收 TCP SYN 包数量	rx_syn_count > 10
tx_syn_ack_count	发送 TCP SYN-ACK 包数量	tx_syn_ack_count > 10
rx_syn_ack_count	接收 TCP SYN-ACK 包数量	rx_syn_ack_count > 10
tx_fin_count	发送 TCP FIN 包数量	tx_fin_count > 10
rx_fin_count	接收 TCP FIN 包数量	rx_fin_count > 10
tx_rst_count	发送 TCP RST 包数量	tx_rst_count > 10
rx_rst_count	接收 TCP RST 包数量	rx_rst_count > 10
tx_zero_window_count	发送 TCP 零窗口包数量	tx_zero_window_count > 10
rx_zero_window_count	接收 TCP 零窗口包数量	rx_zero_window_count > 10
peer_flow_count	连接数	peer_flow_count > 10
l7_protocol	应用层协议	-
tx_handshake_count	客户端握手次数	tx_handshake_count > 10
rx_handshake_count	服务器握手次数	rx_handshake_count > 10
tx_avg_handshake_time	客户端握手平均时延(单位为微秒 us)	tx_avg_handshake_time > 100000
tx_max_handshake_time	客户端握手最大时延(单位为微秒 us)	tx_max_handshake_time > 100000
tx_min_handshake_time	客户端握手最小时延(单位为微秒 us)	tx_min_handshake_time > 100000
rx_avg_handshake_time	服务器握手平均时延(单位为微秒 us)	rx_avg_handshake_time > 100000
rx_max_handshake_time	服务器握手最大时延(单位为微秒 us)	rx_max_handshake_time > 100000
rx_min_handshake_time	服务器握手最小时延(单位为微秒 us)	rx_min_handshake_time > 100000
avg_handshake_time	平均握手时延(单位为微秒 us)	avg_handshake_time > 100000
max_handshake_time	最大握手时延(单位为微秒 us)	max_handshake_time > 100000

min_handshake_time	最小握手时延(单位为微秒 us)	min_handshake_time > 100000
response_count	响应次数	respose_count > 10
avg_response_time	平均响应时延(单位为微秒 us)	avg_response_time > 100000
max_response_time	最大响应时延(单位为微秒 us)	max_response_time > 100000
min_response_time	最小响应时延(单位为微秒 us)	min_response_time > 100000
interface	网口	interface == 0

L3 - IP Pair 模块关键字

关键字	描述	示例
ip_address	IP 地址	ip_address == 192.168.1.1/24
region	地区	region == xxx
ip_dhcp_name	DHCP 名	ip_dhcp_name == peter
dns_name	DNS 名	dns_name == peter
http_name	HTTP 名	http_name == xxx
tls_name	TLS 名	tls_name == xxx
ip_os_name	操作系统	ip_os_name == xxx
ip_peer_address	Peer IP 地址	ip_peer_address == 192.168.1.1/24
peer_region	Peer IP 地区	peer_region == xxx
peer_dhcp_name	Peer IP DHCP 名	peer_dhcp_name == xxx
peer_dns_name	Peer IP DNS 名	dns_name == xxx
peer_http_name	Peer IP HTTP 名	peer_dns_name == xxx
peer_tls_name	Peer IP TLS 名	peer_tls_name == xxx
peer_os_name	Peer IP 操作系统	peer_os_name == xxx
first_activity_time	首次活动时间	-
last_activity_time	上次活动时间	-
tx_pkts	IP 地址到对等 IP 总包数	tx_pkts > 10
rx_pkts	对等 IP 到 IP 地址总包数	rx_pkts > 10
tx_bytes	IP 地址到对等 IP 字节数	tx_bytes > 10
rx_bytes	对等 IP 到 IP 地址字节数	rx_bytes > 10

tx_pps	IP 地址到对等 IP 每秒包数	tx_pps > 10
rx_pps	对等 IP 到 IP 地址每秒包数	rx_pps > 10
tx_bps	IP 地址到对等 IP 每秒流量	tx_bps > 10
rx_bps	对等 IP 到 IP 地址每秒流量	rx_bps > 10
retransmit_bytes	TCP 重传流量	retransmit_bytes > 10
syn_count	TCP SYN 包数量	syn_count > 10
syn_ack_count	TCP SYN-ACK 包数量	syn_ack_count > 10
fin_count	TCP FIN 包数量	fin_count > 10
rst_count	TCP RST 包数量	rst_count > 10

L3 - IP 地理模块关键字

关键字	描述	示例
region	地区	region == xxx
tx_pkts	发送包数	tx_pkts > 10
rx_pkts	接收包数	rx_pkts > 10
tx_bytes	发送字节数	tx_bytes > 10
rx_bytes	接收字节数	rx_bytes > 10
tx_pps	每秒发送包数	tx_pps > 10
rx_pps	每秒接收包数	rx_pps > 10
tx_bps	发送速率	tx_bps > 10
rx_bps	接收速率	rx_bps > 10

L3 - ICMP 模块关键字

关键字	描述	示例
tx_ip	源 IP 地址	tx_ip = 192.168.1.1
rx_ip	目的 IP 地址	rx_ip = 192.168.1.1
avg	平均响应时延(单位为微秒 us)	avg > 100000
max	最大响应时延(单位为微秒 us)	max > 100000
min	最小响应时延(单位为微秒 us)	min > 100000
request_count	请求数量	request_count > 10
response_count	响应数量	response_count > 10

L3 - OSPF 模块关键字

报文类型表（`l3.ospf.packet_types`）

关键字	描述	示例
title	OSPF 报文类型名称	title == 'hello'
pkts	总包数	pkts > 10
bytes	总字节数	bytes > 1000
pps	每秒包数	pps > 1
bps	每秒流量	bps > 1000

邻居表（`l3.ospf.neighbors`）

关键字	描述	示例
ospf_router_id	本端 Router ID	ospf_router_id == 1.1.1.1
ospf_neighbor_router_id	邻居 Router ID	ospf_neighbor_router_id == 2.2.2.2
ospf_area_id	Area ID	ospf_area_id == 0.0.0.0
interface	网口	interface == 0
tx_ip	源 IP（本端接口）	tx_ip == 10.0.0.1
rx_ip	对端接口 IP	rx_ip == 10.0.0.2
ospf_state	当前状态	ospf_state == '2-Way'
ospf_state_change_count	状态变更次数	ospf_state_change_count > 0
first_hello_time	首次 Hello 时间	-
last_hello_time	最近 Hello 时间	-
hello_interval	Hello Interval（秒）	hello_interval == 10
dead_interval	Dead Interval（秒）	dead_interval == 40

邻居历史表（`l3.ospf.neighbor_history`）

关键字	描述	示例
time_stamp	时间	-
ospf_router_id	本端 Router ID	ospf_router_id == 1.1.1.1
ospf_neighbor_router_id	邻居 Router ID	ospf_neighbor_router_id == 2.2.2.2
ospf_area_id	Area ID	ospf_area_id == 0.0.0.0
interface	网口	interface == 0
ospf_state	状态	ospf_state == 'Init'

L3 - QoS 模块关键字

关键字	描述	示例
ip_qos	IP QoS	ip_qos == 0
pkts	数据包数	pkts == 0
bytes	总字节数	bytes == 0
pps	每秒包数	pps > 10
bps	每秒流量	bps > 1000

L4 模块关键字

关键字	描述	示例
tx_ip	客户端 IP	tx_ip == 192.168.1.1
tx_port	客户端端口	tx_port == 12345
tx_dhcp_name	客户端 DHCP 名	tx_dhcp_name == xxx
tx_dns_name	客户端 DNS 名	tx_dns_name == xxx
tx_http_name	客户端 HTTP 名	tx_http_name == xxx
tx_tls_name	客户端 TLS 名	tx_tls_name == xxx
tx_os_name	客户端操作系统	tx_os_name == xxx
tx_region	客户端地区	tx_region == xxx
rx_ip	服务器 IP	rx_ip == 192.168.1.1
rx_port	服务器端口	rx_port == 12345
rx_dhcp_name	服务器 DHCP 名	rx_dhcp_name == xxx
rx_dns_name	服务器 DNS 名	rx_dns_name == xxx
rx_http_name	服务器 HTTP 名	rx_http_name == xxx
rx_tls_name	服务器 TLS 名	rx_tls_name == xxx
rx_os_name	服务器操作系统	rx_os_name == xxx
rx_region	服务器地区	rx_region == xxx
l4_protocol	传输层协议	l4_protocol == tcp
first_activity_time	首次活动时间	-
last_activity_time	上次活动时间	-
tx_pkts	发送包数	tx_pkts > 10
rx_pkts	接收包数	rx_pkts > 10
tx_bytes	发送字节数	tx_bytes > 10
rx_bytes	接收字节数	rx_bytes > 10
tx_pps	每秒发送包数	tx_pps > 10
rx_pps	每秒接收包数	rx_pps > 10
tx_bps	发送速率	tx_bps > 10
rx_bps	接收速率	rx_bps > 10
tx_l4_bytes	客户端 L4 字节	tx_l4_bytes > 10
rx_l4_bytes	服务器 L4 字节	rx_l4_bytes > 10
tx_retransmit_bytes	客户端重传字节	tx_retransmit_bytes > 10
rx_retransmit_bytes	服务器重传字节	rx_retransmit_bytes > 10
tx_retransmit_rate	客户端重传率(比率是万分之一)	tx_retransmit_rate > 5000
rx_retransmit_rate	服务器重传率(比率是万分之一)	rx_retransmit_rate > 5000

tx_retransmit_pkts	客户端重传包数	tx_retransmit_pkts > 10
rx_retransmit_pkts	服务器重传包数	tx_retransmit_pkts > 10
tx_ooo_pkts	客户端乱序包数	tx_ooo_pkts > 10
rx_ooo_pkts	服务器乱序包数	rx_ooo_pkts > 10
syn_count	TCP SYN 包数	syn_count > 10
syn_ack_count	TCP SYN-ACK 包数	syn_ack_count > 10
fin_count	TCP FIN 包数	fin_count > 10
rst_count	TCP RST 包数	rst_count > 10
tx_handshake_count	客户端握手次数	tx_handshake_count > 10
rx_handshake_count	服务器握手次数	rx_handshake_count > 10
tx_avg_handshake_time	客户端握手平均时延(单位为微秒 us)	tx_avg_handshake_time > 100000
tx_max_handshake_time	客户端握手最大时延(单位为微秒 us)	tx_max_handshake_time > 100000
tx_min_handshake_time	客户端握手最小时延(单位为微秒 us)	tx_min_handshake_time > 100000
rx_avg_handshake_time	服务器握手平均时延(单位为微秒 us)	rx_avg_handshake_time > 100000
rx_max_handshake_time	服务器握手最大时延(单位为微秒 us)	rx_max_handshake_time > 100000
rx_min_handshake_time	服务器握手最小时延(单位为微秒 us)	rx_min_handshake_time > 100000
avg_handshake_time	平均握手时延(单位为微秒 us)	avg_handshake_time > 100000
max_handshake_time	最大握手时延(单位为微秒 us)	max_handshake_time > 100000
min_handshake_time	最小握手时延(单位为微秒 us)	min_handshake_time > 100000
close_time	流结束时间	-
tx_dup_ack_count	客户端 TCP DUP ACK 包数	tx_dup_ack_count > 10
rx_dup_ack_count	服务器 TCP DUP ACK 包数	rx_dup_ack_count > 10
close_reason	会话状态	close_reason == "fin by client"
tx_mss	客户端 MSS	tx_mss > 1400
rx_mss	服务器 MSS	rx_mss > 1400
tx_window_scale	客户端窗口缩放	tx_window_scale > 64
rx_window_scale	服务器窗口缩放	rx_window_scale > 64
tx_zero_window	客户端 TCP 零窗口包数量	tx_zero_window > 10
rx_zero_window	服务器 TCP 零窗口包数量	rx_zero_window > 10
tx_max_window	客户端最大窗口	tx_max_window > 1000
rx_max_window	服务器最大窗口	rx_max_window > 1000
tx_max_flight	客户端最大 TCP 未确认传输	tx_max_flight > 1000
rx_max_flight	服务器最大 TCP 未确认传输	rx_max_flight > 1000
tx_mtu	客户端 MTU	tx_mtu > 1500
rx_mtu	服务器 MTU	rx_mtu > 1500
l7_protocols	应用层协议	l7_protocols == http

flow_info	流信息	-
tx_response_count	客户端响应次数	tx_response_count > 10
rx_response_count	服务器响应次数	rx_response_count > 10
tx_avg_response_time	客户端平均响应时延(单位为微秒 us)	tx_avg_response_time > 100000
tx_max_response_time	客户端最大响应时延(单位为微秒 us)	tx_max_response_time > 100000
tx_min_response_time	客户端最小响应时延(单位为微秒 us)	tx_min_response_time > 100000
rx_avg_response_time	服务器平均响应时延(单位为微秒 us)	rx_avg_response_time > 100000
rx_max_response_time	服务器最大响应时延(单位为微秒 us)	rx_max_response_time > 100000
rx_min_response_time	服务器最小响应时延(单位为微秒 us)	rx_min_response_time > 100000
avg_response_time	平均响应时延(单位为微秒 us)	avg_response_time > 100000
max_response_time	最大响应时延(单位为微秒 us)	max_response_time > 100000
min_response_time	最小响应时延(单位为微秒 us)	min_response_time > 100000
avg_l7_response_time	应用层平均响应时延(单位为微秒 us)	avg_l7_response_time > 100000
max_l7_response_time	应用层最大响应时延(单位为微秒 us)	max_l7_response_time > 100000
min_l7_response_time	应用层最小响应时延(单位为微秒 us)	min_l7_response_time > 100000
interface	网口	interface == 0
application_latency	应用时延(单位为微秒 us)	application_latency > 100000
tls_hello_avg_handshake_time	TLS Hello 握手平均时延(单位为微秒 us)	tls_hello_avg_handshake_time > 100000
tls_hello_max_handshake_time	TLS Hello 握手最大时延(单位为微秒 us)	tls_hello_max_handshake_time > 100000
tls_hello_min_handshake_time	TLS Hello 握手最小时延(单位为微秒 us)	tls_hello_min_handshake_time > 100000
tls_hello_handshake_count	TLS Hello 握手次数	tls_hello_handshake_count > 10
tls_data_avg_response_time	TLS 第一次数据响应平均时延(单位为微秒 us)	tls_data_avg_response_time > 100000
tls_data_max_response_time	TLS 第一次数据响应最大时延(单位为微秒 us)	tls_data_max_response_time > 100000
tls_data_min_response_time	TLS 第一次数据响应最小时延(单位为微秒 us)	tls_data_min_response_time > 100000
tls_data_response_count	TLS 数据响应次数	tls_data_response_count > 10
tls_cipher	TLS 协商的加密算法	tls_cipher == xxx
tls_version	TLS 版本	tls_version == xxx
validity	连接有效性	validity == invalid

L7 - 应用层协议模块关键字

关键字	描述	示例
l7_proto	应用层协议	l7_proto == http
first_activity_time	首次活动时间	-
last_activity_time	上次活动时间	-
pkts	发送包数	pkts > 10
bytes	发送字节数	bytes > 10
pps	每秒发送包数	pps > 10
bps	发送速率	bps > 10

L7 - HTTP 模块关键字

关键字	描述	示例
HTTP 服务器页		
ip_address	IP 地址	ip_address == 192.168.1.1/24
region	地区	region == xxx
ip_dhcp_name	DHCP 名	ip_dhcp_name == xxx
dns_name	DNS 名	dns_name == xxx
hostname	主机名	hostname == xxx
ip_os_name	操作系统	ip_os_name == xxx
访问量最大的 HTTP 服务器页		
request_cnt	请求数量	request_cnt > 10
HTTP 响应时间		
avg	平均响应时延(单位为微秒 us)	avg > 100000
max	最大响应时延(单位为微秒 us)	max > 100000
min	最小响应时延(单位为微秒 us)	min > 100000
HTTP 响应代码		
http_response_1xx_type_cnt	1xx(信息)响应数量	http_response_1xx_type_cnt > 10
http_response_2xx_type_cnt	2xx(成功)响应数量	http_response_2xx_type_cnt > 10
http_response_3xx_type_cnt	3xx(重定向)响应数量	http_response_3xx_type_cnt > 10
http_response_4xx_type_cnt	4xx(客户端错误)响应数量	http_response_4xx_type_cnt > 10
http_response_5xx_type_cnt	5xx(服务器错误)响应数量	http_response_5xx_type_cnt > 10
http_response_other_type_cnt	其他响应数量	http_response_other_type_cnt > 10

L7 - TLS 模块关键字

关键字	描述	示例
ip_address	IP 地址	ip_address == 192.168.1.1/24
region	地区	region == xxx
ip_dhcp_name	DHCP 名	ip_dhcp_name == xxx
dns_name	DNS 名	dns_name == xxx
hostname	主机名	hostname == xxx
ip_os_name	操作系统	ip_os_name == xxx
http_name	HTTP 名	http_name == xxx
tls_hello_avg_handshake_time(单位为微秒 us)	Hello 握手平均时延	tls_hello_avg_handshake_time > 100000
tls_hello_max_handshake_time(单位为微秒 us)	Hello 握手最大时延	tls_hello_max_handshake_time > 100000
tls_hello_min_handshake_time(单位为微秒 us)	Hello 握手最小时延	tls_hello_min_handshake_time > 100000
tls_hello_handshake_count	Hello 握手次数	tls_hello_handshake_count > 10
tls_data_avg_response_time	第一次数据响应平均时延(单位为微秒 us)	tls_data_avg_response_time > 100000
tls_data_max_response_time	第一次数据响应最大时延(单位为微秒 us)	tls_data_max_response_time > 100000
tls_data_min_response_time	第一次数据响应最小时延(单位为微秒 us)	tls_data_min_response_time > 100000
tls_data_response_count	第一次数据响应次数	tls_data_response_count > 10
tls_cipher	TLS 协商的加密算法	tls_cipher == xxx
tls_version	TLS 版本	tls_version == xxx
tls_cert_server_names	证书中服务器名称	tls_cert_server_names == xxx
tls_cert_issuer_dn	证书发布者名称	tls_cert_issuer_dn == xxx
tls_cert_subject_dn	证书主题名称	tls_cert_subject_dn == xxx

L7 - DHCP 模块关键字

关键字	描述	示例
概述页		
ip_address	IP 地址	ip_address == 192.168.1.1/24
hostname	主机名	hostname == xxx
mac_address	MAC 地址	mac_address == aa:bb:cc:dd:ee:ff
subnet_mask	子网掩码	subnet_mask == 255.255.255.0
rx_ip	DHCP 服务器 IP 地址	rx_ip == 192.168.1.1/24
update_time	分配时间	-
lease_time	租期	-
DHCP 服务器		
last_activity_time	最近更新时间	-
succeed_request_cnt	成功请求数量	succeed_request_cnt > 10
different_ips	分配 IP 数量	different_ips > 10

L7 - DNS 模块关键字

关键字	描述	示例
DNS 服务器页		
ip_address	IP 地址	ip_address == 192.168.1.1/24
hostname	主机名	hostname == xxx
request_cnt	请求数量	request_cnt > 10
response_cnt	响应数量	response_cnt > 10
DNS 解析页		
domain_name	请求域名	domain_name == xxx
resolved_ip	解析结果(IP)	resolved_ip == 192.168.1.1/24
rx_ip	服务器 IP	rx_ip == 192.168.1.1/24
update_time	更新时间	-
expire_time	过期时间	-
服务器响应时间页		
avg	平均响应时延(单位为微秒 us)	avg > 100000
max	最大响应时延(单位为微秒 us)	max > 100000
min	最小响应时延(单位为微秒 us)	min > 100000
服务器响应代码页		
succeed_request_cnt	成功响应数量	succeed_request_cnt > 10
format_error_cnt	格式错误请求数量	format_error_cnt > 10
server_error_cnt	服务器错误请求数量	server_error_cnt > 10
not_exist_cnt	查询不存在错误数量	not_exist_cnt > 10
other_error_cnt	其他错误数量	other_error_cnt > 10
DNS 记录类型页		
packet_a_record_type_cnt	A 记录类型包数量	packet_a_record_type_cnt > 10
packet_aaaa_record_type_cnt	AAAA 记录类型包数量	packet_aaaa_record_type_cnt > 10
packet_cname_record_type_cnt	CNAME 记录类型包数量	packet_cname_record_type_cnt > 10
packet_mx_record_type_cnt	MX 记录类型包数量	packet_mx_record_type_cnt > 10
packet_srv_record_type_cnt	SRV 记录类型包数量	packet_srv_record_type_cnt > 10
packet_other_record_type_cnt	其它记录类型包数量	packet_other_record_type_cnt > 10

附录二：应用层支持协议

Protocol	L4 协议	UDP 端口	TCP 端口	描述
Unknown	TCP	-	-	-
FTP_CONTROL	TCP	-	21	文件传输协议的控制通道，用于管理文件传输会话
POP3	TCP	-	110	邮件接收协议，用于从服务器下载邮件
SMTP	TCP	-	25,587	邮件发送协议，用于电子邮件的传输
IMAP	TCP	-	143	邮件协议，支持在服务器上管理和同步邮件
DNS	TCP/UDP	53	53	域名系统协议，用于将域名解析为IP地址
IPP	TCP/UDP	-	-	网络打印协议，用于远程打印和打印机管理
HTTP	TCP	-	80	超文本传输协议，用于浏览网页和数据传输
MDNS	TCP	5353,5354	-	多播DNS协议，用于局域网内的设备名称解析和发现
NTP	UDP	123	-	网络时间协议，用于同步设备的时间
NetBIOS	TCP/UDP	137,138,139	139	局域网设备名解析和服务发现协议
NFS	TCP/UDP	2049	2049	网络文件系统协议，用于文件共享
SSDP	UDP	-	-	简单服务发现协议，用于设备发现和连接
BGP	TCP	-	179,2605	边界网关协议，用于路由器间的互联网路由交换
SNMP	UDP	161,162	-	简单网络管理协议，用于设备监控和管理
XDMCP	TCP/UDP	177	177	远程图形界面会话管理协议
SMBv1	TCP	-	445	早期的服务器消息块协议，用于文件和打印共享
Syslog	TCP/UDP	514	514,601,6514	系统日志协议，用于传输日志消息
DHCP	UDP	67,68	-	动态主机配置协议，用于 IP 地址分配
PostgreSQL	TCP	-	5432	开源关系数据库的通信协议
MySQL	TCP	-	3306	流行的关系数据库系统通信协议
Outlook	TCP	-	-	微软邮件和日历服务的通信协议
VK	TCP	-	-	俄罗斯社交平台VK的网络通信协议
POPS	TCP	-	995	使用 SSL 加密的 POP 邮件协议
Tailscale	UDP	41641	-	简化 VPN 配置的对等网络协议
Yandex	TCP	-	-	Yandex 在线服务的通信协议
ntop	TCP	-	-	网络流量监控和分析工具的通信协议
COAP	UDP	5683,5684	-	受限应用协议，用于物联网设备通信
VMware	UDP	902,903	903	VMware虚拟化平台的管理通信协议
SMTPS	TCP	-	465	使用 SSL / TLS 加密的SMTP邮件协议
DTLS	UDP	-	-	基于UDP的传输层安全协议
UBNTAC2	UDP	10001	-	Ubiquiti 设备的配置和监控协议
BFCP	TCP/UDP	-	-	基层会议控制协议，用于多媒体会议
YandexMail	TCP	-	-	Yandex 邮件服务的通信协议
YandexMusic	TCP	-	-	Yandex 音乐流媒体服务的通信协议
Gnutella	TCP/UDP	-	-	分布式文件共享协议
eDonkey	TCP	-	-	对等文件共享协议，用于资源分发
BitTorrent	TCP/UDP	6771,51413	51413,53646	高效的对等文件共享协议
Skype_TeamsCall	TCP	-	-	Skype 和 Microsoft Teams 的语音和视频通话协议
Signal	TCP	-	-	注重隐私的即时通讯和语音通话协议

Memcached	TCP/UDP	11211	11211	高性能分布式内存缓存协议
SMBv2/3	TCP	-	445	现代化的服务器消息块协议，用于文件共享和远程资源访问
Mining	TCP	-	-	用于加密货币挖矿的网络协议
NestLogSink	TCP	-	11095	用于谷歌 Nest 设备的日志收集协议
Modbus	TCP	-	502	工业自动化中广泛使用的通信协议
WhatsAppCall	TCP	-	-	WhatsApp 语音和视频通话的网络协议
DataSaver	TCP	-	-	移动设备的流量节省通信协议
Xbox	UDP	-	-	微软 Xbox 游戏平台的网络通信协议
QQ	UDP	-	-	腾讯即时通讯平台的通信协议
TikTok	TCP	-	-	TikTok 短视频分享平台的网络通信协议
RTSP	TCP/UDP	554	554	实时流协议，用于控制流媒体服务器
IMAPS	TCP	-	993	使用 SSL/TLS 加密的IMAP邮件协议
IceCast	TCP	-	-	用于音频和视频流媒体广播的协议
CPHA	UDP	8116	-	用于加密通信的内容保护协议
iQIYI	UDP	-	-	爱奇艺视频流媒体平台的通信协议
Zattoo	TCP/UDP	-	-	在线电视流媒体服务的网络协议
YandexMarket	TCP	-	-	Yandex电商平台的通信协议
YandexDisk	TCP	-	-	Yandex的云存储和文件共享服务协议
Discord	UDP	-	-	用于实时聊天和语音的社区通信协议
AdobeConnect	TCP	-	-	Adobe 提供的在线会议和协作工具协议
MongoDB	TCP	-	27017	MongoDB 非关系型数据库的通信协议
Pluralsight	TCP	-	-	Pluralsight 在线学习平台的内容流媒体协议
YandexCloud	TCP	-	-	Yandex 提供的云服务通信协议
OCSP	TCP	-	-	在线证书状态协议，用于验证SSL证书有效性
VXLAN	UDP	4789	-	虚拟扩展局域网协议，用于数据中心的网络虚拟化
IRC	TCP	194	194	网络中继聊天协议，用于实时文本通信
MerakiCloud	UDP	-	-	Cisco Meraki设备的云管理通信协议
Jabber	TCP	-	-	基于 XMPP 协议的即时通讯和协作平台
Nats	TCP	-	-	用于云原生分布式系统的消息传递协议
AmongUs	UDP	22023	-	《Among Us》游戏的多人在线通信协议
Yahoo	TCP	-	-	雅虎提供的在线服务和通信协议
DisneyPlus	TCP	-	-	迪士尼流媒体服务的网络通信协议
HART-IP	TCP/UDP	-	5094	工业传感器通信的高速协议
VRRP	TCP	-	-	虚拟路由冗余协议，用于路由备份和故障切换
Steam	UDP	-	-	用于游戏下载和社区功能的通信协议
HalfLife2	UDP	-	-	《半条命2》在线多人游戏的网络通信协议
WorldOfWarcraft	TCP	-	-	MMORPG《魔兽世界》的在线游戏通信协议
Telnet	TCP	-	23	提供远程登录和命令行控制的网络协议
STUN	TCP/UDP	3478	-	用于 NAT 穿越的会话穿越实用程序协议
IPSec	UDP	500,4500	500	提供加密和验证的网络层安全协议
GRE		-	-	通用路由封装协议，用于隧道化 IP 数据包
ICMP		-	-	用于网络设备间发送控制消息的协议（如Ping）
IGMP		-	-	用于管理IP组播成员资格的协议

EGP		-	-	外部网关协议，用于自治系统之间的路由
SCTP		-	-	流控制传输协议，用于多流和多宿主通信
OSPF		-	2604	开放最短路径优先路由协议，用于内部网路由
IP_in_IP		-	-	在IP网络中封装另一个IP数据包的协议
RTP	TCP/UDP	-	-	实时传输协议，用于音视频流传输
RDP	TCP/UDP	3389	3389	远程桌面协议，用于远程访问 Windows 系统
VNC	TCP	-	5900,5901,5800	虚拟网络计算协议，用于远程桌面共享
Tumblr	TCP	-	-	一个以图片和短文分享为主的社交平台协议
TLS	TCP	-	443	传输层安全协议，用于加密网络通信
SSH	TCP	-	22	安全外壳协议，用于加密的远程登录和数据传输
Usenet	TCP	-	-	新闻组服务的通信协议，用于信息分发
MGCP	UDP	-	-	媒体网关控制协议，用于 VoIP 呼叫控制
IAX	UDP	4569	4569	用于 IP 语音通信的协议，支持语音和数据传输
TFTP	UDP	69	-	轻量级文件传输协议，用于简单文件传输
AFP	TCP	548	548	Apple 文件协议，用于文件共享服务
YandexMetrika	TCP	-	-	Yandex 的流量分析服务协议
YandexDirect	TCP	-	-	Yandex 的在线广告服务通信协议
SIP	TCP/UDP	5060,5061	5060,5061	会话初始协议，用于管理音视频通话和会议
TruPhone	TCP	-	-	用于 TruPhone 网络的 VoIP 通信协议
ICMPV6		-	-	IPv6 的网络控制消息协议，用于诊断和报告错误
DHCPV6	UDP	-	-	动态主机配置协议，用于 IPv6 地址分配
Armagetron	UDP	-	-	在线《光轮战》游戏的网络通信协议
Crossfire	TCP/UDP	-	-	《穿越火线》多人在线射击游戏的通信协议
Dofus	TCP	-	-	用于 MMORPG《Dofus》的在线游戏通信协议
ADS_Analytic_Track	TCP	-	-	分析和跟踪广告数据的通信协议
AdultContent	TCP	-	-	访问和流媒体成人内容的协议标识
Guildwars	TCP	-	-	《激战》系列网络游戏的通信协议
AmazonAlexa	TCP	-	-	亚马逊语音助手Alexa的通信协议
Kerberos	TCP/UDP	88	88	安全的网络认证协议，用于用户验证
LDAP	TCP/UDP	389	389	用于访问目录服务的轻量级协议
MapleStory	TCP	-	-	MMORPG《冒险岛》的网络通信协议
MsSQL-TDS	TCP	-	1433,1434	微软SQL Server的表数据流协议
PPTP	TCP	-	-	点对点隧道协议，用于 VPN 连接
Warcraft3	TCP/UDP	-	-	《魔兽争霸3》的在线多人游戏协议
WorldOfKungFu	TCP	-	-	MMORPG《功夫世界》的网络通信协议
Slack	TCP	-	-	团队协作和即时通讯平台的通信协议
Facebook	TCP	-	-	Facebook 社交网络平台的在线通信协议
Twitter	TCP	-	-	Twitter 社交媒体平台的网络通信协议
Dropbox	UDP	17500	-	Dropbox 提供文件同步和存储服务的协议
GMail	TCP	-	-	Google 的电子邮件服务通信协议
GoogleMaps	TCP	-	-	Google 地图的定位和导航服务协议
YouTube	TCP	-	-	视频流媒体平台的网络通信协议
Skype_Teams	TCP	-	-	Skype 和 Microsoft Teams 的通信协议
Google	TCP	-	-	谷歌提供的多种在线服务的协议

MS-RPCH	TCP	-	-	微软远程过程调用协议的变种
NetFlow	UDP	2055	-	用于监控和分析网络流量的协议
sFlow	UDP	6343	-	实时流量监控协议，用于网络设备
HTTP_Connect	TCP	-	8080	用于代理服务器的HTTP连接协议
HTTP_Proxy	TCP	-	8080,3128	HTTP协议的代理转发通信
Citrix	TCP	-	1494,2598	Citrix 提供的远程桌面和应用程序访问协议
NetFlix	TCP	-	-	Netflix 流媒体视频平台的通信和传输协议
LastFM	TCP	-	-	LastFM 音乐流媒体和推荐平台的网络协议
Waze	TCP	-	-	Waze 社交化导航应用的定位和交通信息协议
YouTubeUpload	TCP	-	-	用于上传视频到 YouTube 的通信协议
Hulu	TCP	-	-	Hulu 视频流媒体平台的传输和通信协议
CHECKMK	TCP	-	6556	网络和服务器监控工具的通信协议
AJP	TCP	-	8009,8010	用于 Web 服务器和应用服务器之间的通信协议
Apple	TCP	-	-	苹果提供的多种设备和服务的协议
Webex	TCP	-	-	思科提供的在线会议和协作服务协议
WhatsApp	TCP	-	-	WhatsApp 即时通讯和文件传输平台的协议
AppleiCloud	TCP	-	-	苹果的云存储和同步服务协议
Viber	TCP/UDP	7985,7987,5242,5243,4244	7985,5242,5243,4244	提供即时通讯及语音、视频通话的应用
AppleiTunes	TCP	-	-	苹果设备的音乐和多媒体内容管理服务
Radius	UDP	1812,1813	1812,1813	用于网络接入认证、授权和计费的协议
WindowsUpdate	TCP	-	-	微软系统的自动更新服务协议
TeamViewer	TCP/UDP	5938	5938	用于远程桌面控制和支持的软件协议
EthernetGlobalData	UDP	-	-	工业以太网数据交换协议
LotusNotes	TCP	-	1352	IBM 提供的企业邮件和协作平台协议
SAP	TCP	-	3201	企业资源计划（ERP）和管理软件的通信协议
GTP	UDP	2152,2123	-	移动通信中数据和信令的隧道协议
WSD	UDP	3702	-	Windows设备之间的服务发现协议
LLMNR	TCP	5355	5355	局域网内的名称解析协议
TocaBoca	UDP	5055	-	儿童教育游戏的网络通信协议
Spotify	TCP/UDP	-	-	提供音乐流媒体和个性化播放列表的平台
FacebookMessenger	TCP	-	-	Facebook 的即时通讯服务协议
H323	TCP/UDP	1719,1720	1719,1720	音视频会议的通信和多媒体传输协议
OpenVPN	TCP/UDP	1194	1194	提供加密和安全连接的开源 VPN 协议
NOE	UDP	-	-	阿尔卡特电话系统的网络通信协议
CiscoVPN	UDP	10000	10000,8008	思科提供的虚拟专用网络协议
TeamSpeak	TCP/UDP	-	-	用于语音通信和在线会议的软件协议
Tor	TCP	-	-	匿名网络通信的路由协议
CiscoSkinny	TCP	-	2000	思科电话设备的轻量化通信协议
RTCP	TCP	-	-	实时传输控制协议，用于音视频流质量监测
RSYNC	TCP	-	873	高效的文件同步和传输工具协议
Oracle	TCP	-	1521	Oracle 数据库及其服务通信协议
Corba	TCP/UDP	-	-	用于分布式系统的对象请求代理架构协议
UbuntuONE	TCP	-	-	Ubuntu 提供的云存储和文件同步服务
Whois-DAS	TCP	-	43,4343	域名和 IP 地址信息查询协议的扩展版本

SD-RTN	UDP	-	-	软件定义实时传输网络协议
SOCKS	TCP	1080	1080	一种用于网络流量路由的代理协议
Nintendo	UDP	-	-	任天堂游戏平台及其网络服务协议
RTMP	TCP	-	1935	用于流媒体音视频传输的实时消息传输协议
FTP_DATA	TCP	-	20	文件传输协议的数据通道
Wikipedia	TCP	-	-	用于访问和编辑维基百科内容的网络协议
ZeroMQ	TCP	-	-	异步消息队列库，用于高性能通信
Amazon	TCP	-	-	亚马逊电商平台及其相关网络服务协议
eBay	TCP	-	-	eBay的电子商务平台及其通信协议
CNN	TCP	-	-	CNN 有线新闻网络的在线内容分发协议
Megaco	UDP	2944	-	多媒体网关控制协议，用于IP网络中的媒体服务
RESP	TCP	-	6379	简单的二进制协议，用于Redis等键值存储系统
Pinterest	TCP	-	-	一个用于分享和发现创意图片的社交平台
VHUA	UDP	58267	-	华为的 VoIP 通信协议
Telegram	TCP/UDP	-	-	注重隐私和安全的即时通讯应用
CoD_Mobile	UDP	-	-	《使命召唤》移动端版本的网络通信协议
Pandora	TCP	-	-	提供音乐流媒体和个性化电台服务的平台
QUIC	UDP	443	-	谷歌开发的快速 UDP 互联网连接协议
Zoom	UDP	-	-	用于视频会议和网络协作的通信工具
EAQ	UDP	6000	-	EA游戏的在线服务通信协议
Ookla	TCP/UDP	-	-	互联网速度测试服务协议（如 Speedtest）
AMQP	TCP	-	-	高级消息队列协议，用于消息传递
KakaoTalk	TCP	-	-	韩国的即时通讯应用
KakaoTalk_Voice	UDP	-	-	KakaoTalk的语音通话服务协议
Twitch	TCP	-	-	提供实时游戏直播和视频流媒体的平台
DoH_DoT	TCP	784,853	853	使用HTTPS或TLS加密DNS流量的协议
WeChat	TCP	-	-	微信，腾讯开发的多功能即时通讯和支付平台
MPEG_TS	UDP	-	-	用于音视频流的MPEG传输流协议
Snapchat	TCP	-	-	Snapchat 短视频和消息分享的社交平台
Sina	TCP	-	-	新浪旗下的社交和内容服务协议
GoogleMeet	TCP	-	-	Google 提供的在线会议和协作工具
IFLIX	TCP	-	-	专注于东南亚地区的视频流媒体服务
Github	TCP	-	-	Github 代码托管和协作开发平台
BJNP	UDP	8612	-	佳能打印机和扫描设备的网络协议
Reddit	TCP	-	-	Reddit 用户生成内容的社交新闻和讨论平台
WireGuard	UDP	51820	-	高效、安全的虚拟专用网络（VPN）协议
SMPP	TCP	-	-	短信对等协议，用于短信发送和接收
DNScrypt	TCP/UDP	-	-	加密DNS流量以提高隐私和安全的协议
TINC	TCP/UDP	655	655	一个跨平台的虚拟专用网络（VPN）协议
Deezer	TCP	-	-	Deezer 高质量音乐流媒体服务的平台
Instagram	TCP	-	-	Instagram 社交平台
Microsoft	TCP	-	-	微软公司开发的在线服务和软件协议
Starcraft	TCP/UDP	1119	1119	《星际争霸》游戏协议

Teredo	UDP	-	-	在IPv6和IPv4之间提供隧道通信的协议
HotspotShield	TCP	-	-	一种增强隐私的VPN服务工具
IMO	UDP	-	-	用于即时通讯和视频通话的跨平台应用
GoogleDrive	TCP	-	-	Google 提供的云存储和文件共享服务
OCS	TCP	-	-	微软用于实时通信的办公通信协议
Microsoft365	TCP	-	-	微软的云办公工具套件及服务协议
Cloudflare	TCP	-	-	提供内容分发、网络安全和DNS服务的协议
MS_OneDrive	TCP	-	-	微软提供的云存储服务
MQTT	TCP	-	1883,8883	轻量级物联网设备通信协议
RX	UDP	-	-	一种用于并发处理的响应式编程库
AppleStore	TCP	-	-	苹果设备的官方应用和内容商店
OpenDNS	TCP	-	-	提供安全和内容过滤的DNS解析服务
Git	TCP	-	9418	分布式版本控制系统，用于代码管理
DRDA	TCP	-	-	分布式关系型数据库访问协议
PlayStore	TCP	-	-	Google Android 设备的官方应用商店
SOMEIP	TCP/UDP	30491,30501,30490	30491,30501	汽车中基于以太网通信的服务导向协议
FIX	TCP	-	-	金融信息交换协议，用于证券交易
Playstation	TCP	-	-	索尼的游戏主机及在线服务协议
Pastebin	TCP	-	-	分享和存储文本内容的在线工具
LinkedIn	TCP	-	-	职业社交网络和招聘平台
SoundCloud	TCP	-	-	在线音频分享和流媒体平台
SteamDatagramRelay	UDP	-	-	Valve 用于优化游戏连接的网络服务
LISP	TCP/UDP	4342,4341	-	位置标识分离协议，用于路由优化
Diameter	TCP	-	3868	认证、授权和计费协议，继承自 RADIUS
ApplePush	TCP	-	-	苹果设备的通知推送服务
GoogleServices	TCP	-	-	Google 生态系统中的核心在线服务
AmazonVideo	TCP/UDP	-	-	亚马逊提供的流媒体视频服务
GoogleDocs	TCP	-	-	在线文档编辑和协作平台
WhatsAppFiles	TCP	-	-	WhatsApp 的文件共享功能协议
TargusDataspeed	TCP	5001,5201	5001,5201	数据传输优化工具，提升速度和性能
DNP3	TCP	-	20000	分布式网络协议，用于电力系统自动化
IEC60870	TCP	-	2404	用于工业自动化和电力控制的通信协议
Bloomberg	TCP	-	-	金融信息和交易平台的服务协议
CAPWAP	UDP	5246,5247	-	无线接入点和控制器间的通信协议
Zabbix	TCP	-	10050,10051	网络和应用性能监控工具
S7Comm	TCP	-	-	西门子PLC的通信协议，用于自动化设备
Teams	TCP	-	-	微软的团队协作和通信工具
WebSocket	TCP	-	-	提供全双工通信的实时网络协议
AnyDesk	TCP	-	-	远程桌面访问和控制工具
SOAP	TCP	-	-	用于 Web 服务的基于 XML 的通信协议
AppleSiri	TCP	-	-	苹果设备的语音助手通信协议
SnapchatCall	TCP	-	-	Snapchat 的语音和视频通话服务
HP_VIRTGRP	TCP	-	-	惠普虚拟化设备管理的协议
GenshinImpact	TCP/UDP	22102	-	《原神》米哈游开发的开放世界动作角色扮演游戏

Activision	UDP	-	-	动视游戏平台及在线服务
FortiClient	TCP	-	8013,8014	Fortinet 提供的网络安全和 VPN 解决方案
Z3950	TCP	-	210	用于图书馆系统间信息检索的标准协议
Likee	TCP	-	-	Likee 短视频分享和创作的社交平台
GitLab	TCP	-	-	提供代码托管、CI/CD等功能的开发平台
AVASTSecureDNS	UDP	-	-	提供DNS流量加密和钓鱼网站防护的服务
Cassandra	TCP	-	7000,9042	高可扩展性和高可用性的分布式数据库
AmazonAWS	TCP	-	-	亚马逊的云计算和存储服务平台
Salesforce	TCP	-	-	基于云的客户关系管理（CRM）平台
Vimeo	TCP	-	-	主打高质量视频分享和流媒体服务的平台
FacebookVoip	TCP	-	-	Facebook提供的语音通话功能协议
SignalVoip	TCP	-	-	Signal应用中的语音和视频通话服务
Fuze	TCP	-	-	用于企业通信和协作的云服务
GTP_U	TCP	-	-	GPRS隧道协议的用户面，用于数据传输
GTP_C	TCP	-	-	GPRS隧道协议的控制面，用于会话管理
GTP_PRIME	TCP	-	-	增强版的GPRS隧道协议
Alibaba	TCP	-	-	阿里巴巴的电商及云计算服务平台
Crashlytics	TCP	-	-	用于跟踪和报告移动应用崩溃的工具
Azure	TCP	-	-	微软提供的云计算和存储服务
iCloudPrivateRelay	TCP	-	-	苹果用于保护用户隐私的网络传输服务
EthernetIP	TCP	-	44818	工业自动化中的以太网通信协议
Badoo	TCP	-	-	在线社交和约会平台
AccuWeather	TCP	-	-	提供天气预报数据和服务的平台
GoogleClassroom	TCP	-	-	谷歌提供的在线学习和教育管理工具
HSRP	UDP	1985	-	热备路由协议，用于实现网络冗余和容错
Cybersec	TCP	-	-	一种增强在线安全的网络保护工具
GoogleCloud	TCP	-	-	谷歌提供的云计算和存储服务
Tencent	TCP	-	-	腾讯公司的通信、娱乐和云计算服务
RakNet	UDP	-	-	网络游戏开发中常用的网络通信协议
Xiaomi	TCP	-	-	小米生态系统内的设备通信和服务协议
Edgecast	TCP	-	-	提供内容交付网络（CDN）服务的平台
Cachefly	TCP	-	-	全球分布式内容交付网络服务提供商
Softether	UDP	-	-	开源的多协议虚拟专用网络（VPN）解决方案
MpegDash	TCP	-	-	动态自适应流媒体技术，用于高质量视频传输
Dazn	TCP	-	-	专注于体育内容的流媒体服务平台
GoTo	TCP	-	-	提供远程访问和会议解决方案的工具
RSH	TCP	-	-	远程 Shell 协议，用于命令行远程访问
1kxun	TCP	-	-	中国本地的短视频或直播平台协议
PGM		-	-	通用组播协议，用于可靠的多播通信
IP_PIM		-	-	协议无关组播，用于多播路由的核心协议
collectd	UDP	25826	-	收集和报告系统性能数据的开源工具
TunnelBear	TCP	-	-	注重隐私和用户友好的 VPN 服务
CloudflareWarp	UDP	-	-	Cloudflare提供的加速和加密网络流量的 VPN
i3D	UDP	-	-	提供低延迟的全球游戏托管和网络服务

RiotGames	UDP	-	-	开发和发行在线多人游戏的公司及协议
Psiphon	TCP	-	-	用于绕过网络审查和保护隐私的工具
UltraSurf	TCP	-	-	保护在线隐私和突破网络限制的工具
Threema	TCP	-	-	注重安全性和隐私的加密即时通讯工具
AliCloud	TCP	-	-	阿里巴巴提供的云计算和存储服务
AVAST	TCP	-	-	提供防病毒和网络安全保护的软件
TiVoConnect	TCP/UDP	2190	2190	TiVo设备用于节目传输和同步的协议
Kismet	TCP	-	-	无线网络分析和入侵检测工具
FastCGI	TCP	-	-	高效的CGI协议，用于动态内容生成
FTPS	TCP	-	-	支持TLS加密的安全文件传输协议
NAT-PMP	UDP	5351	-	自动配置网络地址转换映射的协议
Syncthing	UDP	-	-	去中心化的文件同步工具
CryNetwork	UDP	-	-	CryEngine游戏引擎的网络通信模块
Line	TCP	-	-	流行的即时通讯和社交媒体应用
LineCall	UDP	-	-	Line应用中的语音和视频通话服务
AppleTVPlus	TCP	-	-	苹果的流媒体视频服务
DirecTV	TCP	-	-	卫星电视和流媒体服务提供商
HBO	TCP	-	-	提供高质量影视内容的流媒体平台
Vudu	TCP	-	-	数字视频租赁和购买服务
Showtime	TCP	-	-	提供影视和流媒体内容的订阅服务
Dailymotion	TCP	-	-	视频分享和流媒体平台
Livestream	TCP	-	-	实时视频流媒体服务
Tencentvideo	TCP	-	-	腾讯旗下的视频流媒体平台
IHeartRadio	TCP	-	-	提供在线广播和音乐流媒体服务
Tidal	TCP	-	-	主打高质量音乐流媒体的平台
TuneIn	TCP	-	-	提供广播、新闻和音乐流媒体的服务
SiriusXMRadio	TCP	-	-	卫星广播和在线流媒体服务
Munin	TCP	-	4949	用于系统性能监控的开源工具
Elasticsearch	TCP	-	-	分布式搜索和数据分析引擎
TuyaLP	UDP	6667	-	涂鸦智能的低功耗物联网协议
TPLINK_SHP	TCP/UDP	9999	9999	TP-Link 智能家居设备协议
Source_Engine	UDP	27015	-	用于开发游戏的 Valve 游戏引擎
BACnet	UDP	47808	-	建筑自动化控制的通信协议
OICQ	UDP	8000	-	腾讯早期的即时通讯协议（QQ）
Heroes_of_the_Storm	UDP	-	-	暴雪娱乐的多人在线战术竞技游戏
FbookReelStory	TCP	-	-	Facebook 中的短视频与故事功能
SRTP	TCP	-	-	安全的实时传输协议，用于音视频数据
OperaVPN	TCP	-	-	pera浏览器内置的虚拟专用网络功能
EpicGames	UDP	-	-	在线游戏分发平台及开发商
GeForceNow	TCP	-	-	NVIDIA 提供的云游戏服务
Nvidia	TCP	-	-	NVIDIA 显卡驱动、软件及相关服务协议
BITCOIN	TCP	-	8333	去中心化的数字加密货币和支付系统
ProtonVPN	TCP	-	-	强调隐私保护的安全VPN服务
Thrift	TCP/UDP	-	-	高效的跨语言远程过程调用（RPC）框架

Roblox	TCP	-	-	在线多人游戏平台及游戏开发工具
Service_Location_Protocol	TCP/UDP	427	427	自动发现网络服务的协议
Mullvad	TCP	-	-	注重隐私的虚拟专用网络（VPN）服务
HTTP2	TCP	-	-	高效的下一代超文本传输协议
HAProxy	TCP	-	-	开源的高性能负载均衡和代理服务器
RMCP	UDP	623	-	远程管理控制协议，用于硬件管理
Controller_Area_Network	TCP/UDP	-	-	用于嵌入式系统的实时数据通信总线
Protobuf	TCP/UDP	-	-	高效的跨平台序列化协议
ETHEREUM	TCP/UDP	-	30303	去中心化的区块链和智能合约平台
TelegramVoip	TCP	-	-	Telegram中的语音通话协议
SinaWeibo	TCP	-	-	中国的社交媒体和微博服务平台
TeslaServices	TCP	-	-	特斯拉汽车的网络服务接口
PTPv2	UDP	319,320	-	精确时间协议，用于高精度时间同步
RTPS	UDP	7401	-	实时发布订阅协议，用于数据分发
OPC-DA	TCP	-	-	工业自动化通信标准，用于实时数据的采集与传输
OPC-UA	TCP	-	4840	工业自动化中安全的互操作通信协议
S7CommPlus	TCP	-	-	西门子PLC的专有通信协议
FINS	TCP/UDP	9600	9600	欧姆龙PLC的通信协议
EtherSIO	UDP	6060	-	用于工业以太网通信的协议
UMAS	TCP	-	-	Schneider电气的设备管理协议
BeckhoffADS	TCP	-	48898	Beckhoff自动化设备的通信协议
ISO9506-1-MMS	TCP	-	-	制造消息规范，用于工业控制系统通信
IEEE-C37118	TCP/UDP	4713	4712	智能电网中使用的通信标准
Ether-S-Bus	UDP	5050	-	一种工业通信协议
Monero	TCP	-	-	注重隐私和匿名的加密货币
DCERPC	TCP/UDP	135	135	分布式计算环境的远程过程调用协议
PROFINET_IO	UDP	-	-	工业以太网标准，支持实时数据传输
HiSLIP	TCP	-	4880	高速仪器远程控制协议
UFTP	UDP	1044	-	安全的组文件传输协议
OpenFlow	TCP	-	6653	软件定义网络（SDN）协议
JSON-RPC	TCP	-	-	轻量级的远程过程调用协议，基于JSON格式
WebDAV	TCP	-	-	基于HTTP的分布式文件管理协议
Kafka	TCP	-	9092	分布式消息队列系统
NoMachine	TCP/UDP	4000	4000	远程桌面访问软件
IEC62056	TCP/UDP	4059	4059	用于智能电表数据交换的标准协议
HL7	TCP	-	2575	医疗数据交换的国际标准协议
Ceph	TCP	-	3300,6789	分布式存储系统
GoogleChat	TCP	-	-	Google提供的即时通讯与协作工具
Roughtime	TCP/UDP	2002	2002	去中心化的时间同步协议
PrivateInternetAccess	TCP	-	-	提供匿名浏览服务的VPN
KCP	TCP/UDP	-	-	高性能传输协议，优化延迟和可靠性
Dota2	TCP	-	-	一款流行的多人在线战术竞技游戏
Mumble	UDP	-	-	开源的低延迟语音聊天应用
Yojimbo	UDP	-	-	简化的加密文件存储和传输工具

ElectronicArts	TCP	-	-	EA 公司开发和发行的电子游戏及相关服务
STOMP	TCP	-	61613	简单的文本协议，用于消息队列的交互
Radmin	TCP	-	4899	远程桌面管理和控制软件
Raft	TCP	-	-	一种用于分布式系统的一致性算法
CIP	UDP	2222	-	通用工业协议，用于工业自动化设备通信
Gearman	TCP	-	4730	任务分发和负载均衡的工作分配系统
TencentGames	TCP	-	-	腾讯开发和运营的游戏及相关服务
GaijinEntertainment	UDP	20011	-	开发和发布多人在线游戏的公司
ANSI_C1222	TCP/UDP	1153	1153	用于公用事业计量和设备管理的协议标准
Huawei	TCP	-	-	华为技术有限公司的通信及设备服务协议
HuaweiCloud	TCP	-	-	华为提供的云计算和存储服务
DLEP	TCP/UDP	854	854	动态链路交换协议
BFD	UDP	3784,3785	-	快速检测网络连接故障的协议
NetEaseGames	UDP	-	-	网易开发和运营的网络游戏及服务
PathofExile	TCP	-	-	免费的在线动作角色扮演游戏
GoogleCall	TCP	-	-	Google生态系统中的语音和视频通话服务
PFCP	UDP	8805	-	用于5G核心网会话管理的协议
FLUTE	UDP	-	-	文件传输协议，适用于广播环境
LoLWildRift	UDP	-	-	《英雄联盟》的移动端版本
TES_Online	TCP	-	-	《上古卷轴Online》大型多人在线角色扮演游戏
LDP	TCP/UDP	646	646	标签分发协议，用于多协议标签交换（MPLS）
KNXnet_IP	TCP/UDP	3671	3671	智能楼宇自动化中的网络通信协议
Bluesky	TCP	-	-	去中心化的社交网络协议和平台
Mastodon	TCP	-	-	开源的分布式社交媒体平台
Threads	TCP	-	-	Meta推出的即时通讯和社交应用
ViberVoip	TCP	-	-	Viber提供的语音和视频通话服务
ZUG	UDP	-	-	瑞士国家铁路相关的通信协议
JRMI	TCP	-	1099	Java远程方法调用协议，用于分布式计算
RipeAtlas	UDP	-	-	网络性能监测和分析平台的协议
HLS	TCP	-	-	HTTP实时流协议，用于视频流媒体传输
ClickHouse	TCP	-	-	高性能的开源列式数据库管理系统
Nano	TCP	-	7075	一种快速、免手续费、环保的加密货币。
OpenWire	TCP	-	61616	用于消息传递的跨平台通信协议
CNP-IP	UDP	-	-	一种用于铁路通信网络的工业协议
ATG	TCP	-	-	自动油箱测量系统的通信协议
TRDP	TCP/UDP	17224,17225	17225	铁路运输中实时数据交换的协议
Lustre	TCP	-	-	高性能并行分布式文件系统，常用于超级计算
NordVPN	TCP	-	-	专注于隐私和安全的虚拟专用网络服务
SurfShark	TCP	-	-	提供加密和隐私保护的VPN服务
CactusVPN	TCP	-	-	支持隐私浏览和智能DNS的VPN服务
Windscribe	TCP	-	-	提供流量加密和隐私保护的VPN工具
Sonos	TCP	-	-	用于多房间无线音频设备的通信协议
DingTalk	TCP	-	-	钉钉企业版的即时通讯和协作工具
PalTalk	TCP	-	-	一款视频聊天和即时通讯应用

Naver	TCP	-	-	韩国最大的搜索引擎和在线平台
Shein	TCP	-	-	中国的一家快时尚零售商
Temu	TCP	-	-	拼多多控股运营的在线市场
TaoBao	TCP	-	-	中国的一个在线购物平台
MikroTik	UDP	-	-	邻居发现协议
DICOM	TCP	-	-	用于医学图像和相关信息数字存储和传输的技术标准
ParamountPlus	TCP	-	-	美国订阅式视频点播网络流媒体服务
Alice	TCP	-	-	雅虎开发的一款语音助手
Vivox	UDP	-	-	一个语音和文本聊天技术平台
DigitalOcean	TCP	-	-	一家云服务提供商
RUTUBE	TCP	-	-	俄罗斯的视频分享和流媒体平台
LagoFast	UDP	-	-	一款游戏加速器
GearUp Booster	TCP/UDP	-	-	一款游戏加速器
Rumble	TCP	-	-	一个视频分享和流媒体平台
Ubiquity		-	-	一家美国网络技术公司
MSDO	UDP	-	-	负责分发 Windows 更新和内容
Rockstar Games	TCP/UDP	-	-	一家游戏发行商
KICK	TCP	-	-	一家澳大利亚视频直播服务平台
Hamachi	TCP/UDP	-	-	VPN 服务（主要用于游戏和远程访问）
GLBP	UDP	-	-	网关负载均衡协议 (GLBP) - Cisco 专有协议，为 IPv4 和 IPv6 网络提供第一跳冗余和负载均衡
EasyWeather	UDP	-	-	一种专有的基于 UDP 的协议，一些气象站使用它通过网络发布和导出天气数据
Mudfish	TCP/UDP	-	-	一款专为游戏设计的 VPN，可以减少延迟并提高连接质量
TRISTATION	UDP	-	-	专有的工业级安全仪表系统 (SIS) 协议，用于安全停机技术
SAMSUNG_SDP	UDP	-	-	三星设备（例如电视、条形音箱或智能手机）使用的专有服务发现协议
Matter	TCP/UDP	-	-	一个开源、免版税的智能家居设备连接标准
Cognito	TCP	-	-	一个面向 Web 和移动应用程序的身份平台
Amazon API Gateway	TCP	-	-	一项完全托管的服务，使开发人员能够轻松创建、发布、维护、监控和保护任何规模的 API
Amazon Kinesis	TCP	-	-	亚马逊网络服务 (AWS) 提供的一系列服务，用于大规模处理和分析实时流数据
Amazon EC2	TCP	-	-	Amazon Elastic Compute Cloud (EC2) 是亚马逊云计算平台 Amazon Web Services (AWS) 的一部分，它允许用户租用虚拟计算机来运行自己的计算机应用程序
Amazon EMR	TCP	-	-	Amazon EMR 是一个托管集群平台，它简化了在 AWS 上运行 Apache Hadoop 和 Apache Spark 等大数据框架的过程，从而可以处理和分析海量数据
Amazon S3	TCP	-	-	Amazon Simple Storage Service (Amazon S3) 是一种对象存储服务，提供业界领先的可扩展性、数据可用性、安全性和性能
Amazon CloudFront	TCP	-	-	Amazon CloudFront 是一项网络服务，可加速将您的静态和动态 Web 内容（例如 .html、.css、.js 和图像文件）分发给用户
Amazon DynamoDB	TCP	-	-	Amazon DynamoDB 是 Amazon Web Services 提供的完全托管的 NoSQL 数据库服务，可为键值数据和文档数据提供高性能、无服务器和无限可扩展的存储
ESPN	TCP	-	-	一间 24 小时专门播放体育节目的美国有线电视联播网

Akamai	TCP	-	-	一家专门从事内容分发网络 (CDN)、网络安全、DDoS 缓解和云服务的美国公司

- 江门市云争科技有限公司
- www.anatraf.com