AnaTraf 网络流量分析仪

技术白皮书

江门市云争科技有限公司

2025 年 5 月

目录

1 前言.....4
2 系统部署.....5
3 核心功能.....7
3.1 网络流量可视化.....7
3.2 网络故障排除.....7
3.3 全流量存储与回溯分析.....7
3.4 在线解码.....8
3.5 OSI 2-7 层分析.....10
3.5.1 MAC分析.....10
3.5.2 ARP分析.....11
3.5.3 VLAN分析.....12
3.5.4 L2 QoS分析.....13
3.5.5 数据包大小统计.....14
3.5.6 突发分析.....15
3.5.7 L3 IP 分析.....16
3.5.8 L3 IP Pairs分析.....16
3.5.9 L3 IP Group分析.....17
3.5.9 L3 QoS分析.....18
3.5.10 L3 ICMP 分析.....19
3.5.11 L4 连接分析.....20
3.5.12 L4 TCP分析.....21
3.5.13 L7 应用层协议分析.....22
3.5.14 L7 HTTP 分析.....23
3.5.15 L7 TLS 分析.....24
3.5.16 L7 DNS 分析.....24
3.5.17 L7 DHCP 分析.....25

4 应用场景.....26
4.1 发现并解决网络问题.....26
4.2 基于报文的流量可视化和资产清单.....26
4.3 SSL/TLS服务器连接有效性和故障分析.....27
4.4 多节点数据关联分析和故障排除.....27
4.5 数据包快速过滤和在线解码分析.....27
4.6 全流量回溯分析.....27
4.7 工业以太网协议分析与故障排除.....28
4.8 业务系统性能分析与质量监控.....28
5 技术架构.....28

1 前言

在当今信息社会中，网络已成为支撑各类业务系统、工业控制和社会生活的关键基础设施。伴随数据通信规模的日益增长与网络环境的日趋复杂，传统的网络管理手段已难以应对多样化、动态化的网络流量行为。特别是在面对大规模数据交互、高并发连接等场景时，网络运营者、信息安全团队与科研人员对高效、精准、可视化的网络流量分析工具的需求日益迫切。

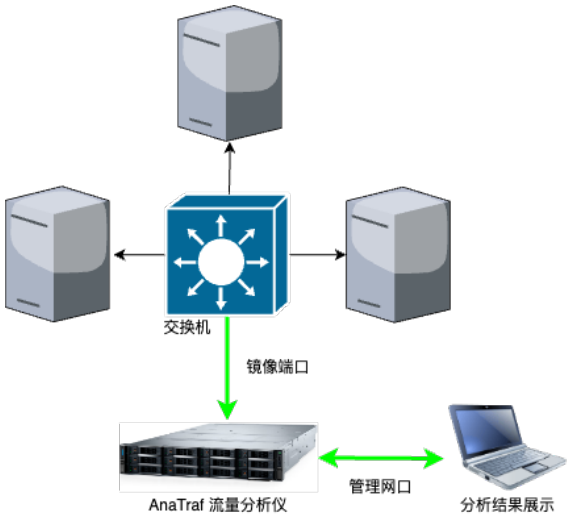
AnaTraf 网络流量分析仪正是在这一背景下应运而生的一款高性能网络流量监测与分析系统。该系统结合了深度包检测（DPI）、协议解析、可视化呈现等多项先进技术，能够实现对复杂网络环境中流量的实时捕获与分析。AnaTraf 不仅支持对 TCP/IP 协议族的分析，还具备对应用层协议如 HTTP、DNS、TLS 等的深入分析能力，从而为网络管理、异常检测与性能优化提供了坚实的数据支撑。

AnaTraf 的设计理念强调模块化、可扩展性与高吞吐能力，既可部署于校园网、企业网等中小规模网络环境，也适用于骨干网级别的高负载场景。系统支持实时和历史两种分析模式，既可对历史流量数据进行回溯挖掘，也可实现对实时流的高精度处理。通过灵活的规则引擎与丰富的接口支持，AnaTraf 能够集成至现有的安全防御系统、网络运维平台或科研分析环境之中。

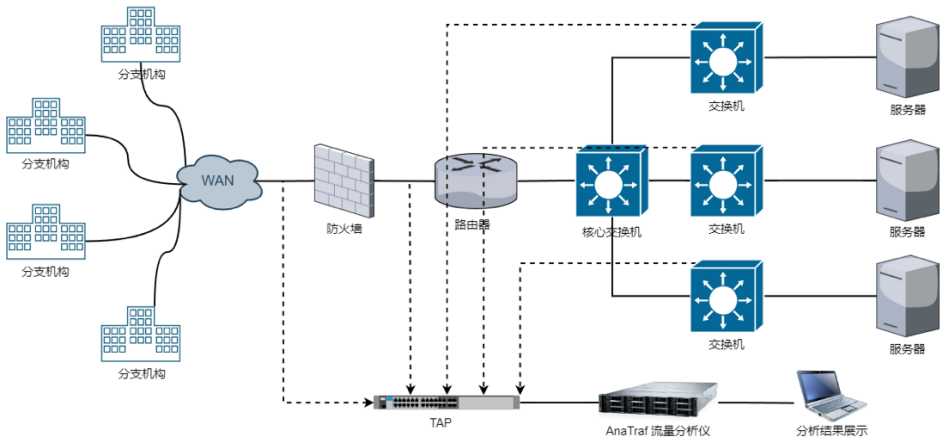
2 系统部署

AnaTraf 网络流量分析仪在设计上充分考虑了实际网络环境中的部署便捷性与兼容性，支持多种主流的部署方式，能够在不中断现有业务系统的前提下，实现对目标网络的高效监测与分析。系统可通过镜像端口（SPAN）、网络 TAP 设备或桥接（串联）模式进行流量接入，具备“零侵入、旁路部署”的特性，对生产网络不产生任何干扰或性能影响。

在镜像端口模式下，AnaTraf 可连接至交换机或路由器的镜像口，对指定端口或 VLAN 的流量进行实时复制与分析。



在 TAP 模式中，通过专用硬件设备实现流量的无损复制，适用于对流量完整性要求较高的场景。



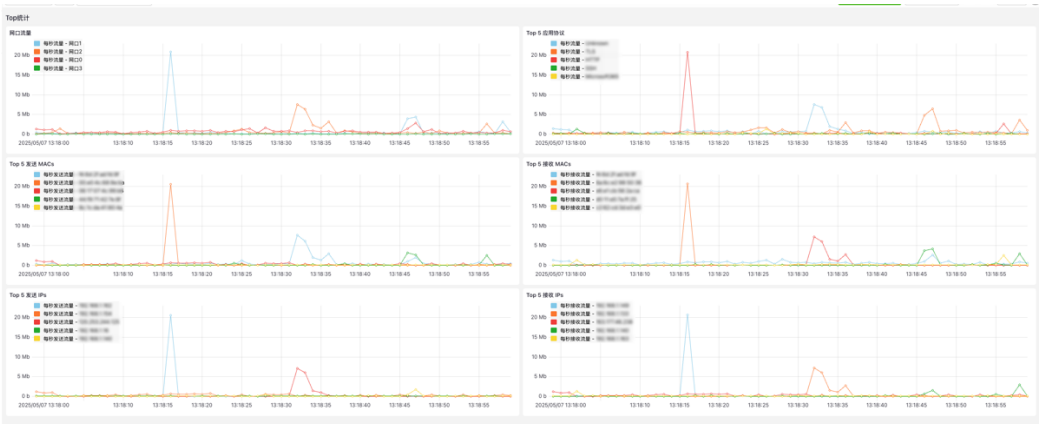
而桥接模式则允许 AnaTraf 直接串联在网络路径中，适合需要双向流量完整掌握的部署需求。

通过灵活的部署方式与强大的适配能力，AnaTraf 能够广泛适用于数据中心、企业网络、校园网以及运营商边界等多种应用场景。

3 核心功能

3.1 网络流量可视化

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。



3.2 网络故障排除

全流量采集网络故障期间的全部通信数据并存储至磁盘，借助海量数据索引和高性能内存数据库，实现快速定位问题点并提取分析。

全流量回溯重现故障，以及简单直观的 WEB 界面实时显示 L2-L7 网络性能和质量指标的趋势、非常详细的统计数据和指标。这加快了故障排除并降低了 MTTR，明确故障责任界定。

3.3 全流量存储与回溯分析

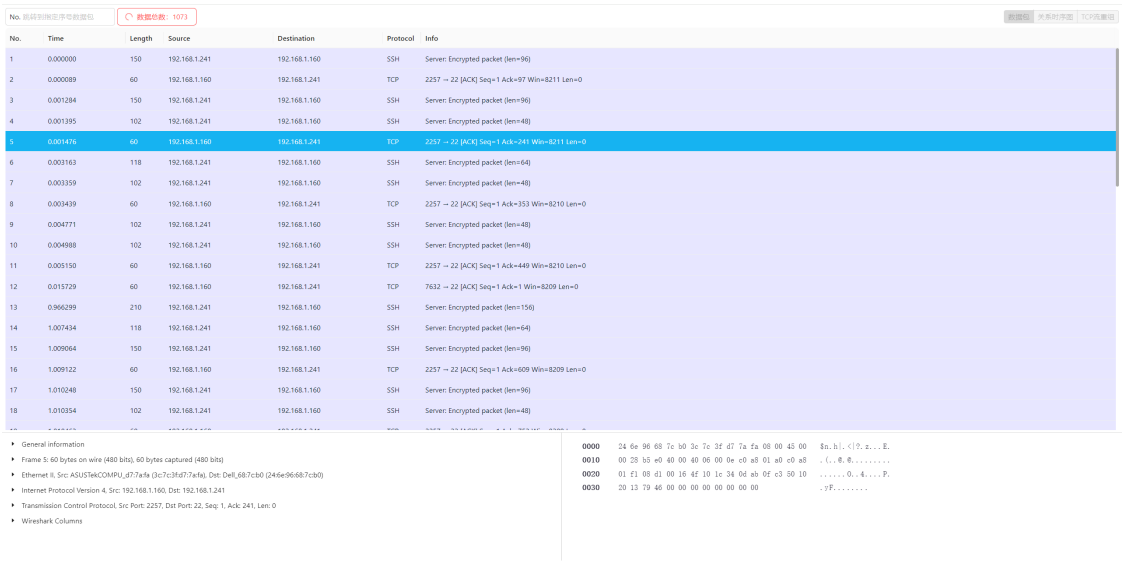
全流量存储与回溯分析功能是 AnaTraf 网络流量分析仪的一项核心优势，旨在帮助用户全面记录并有效回溯网络流量数据。该功能使网络管理员能够在 故障排除、事件

审计、性能分析或安全监控中，轻松访问和重现特定时间段内的完整网络流量，从而为决策提供准确的数据支持。

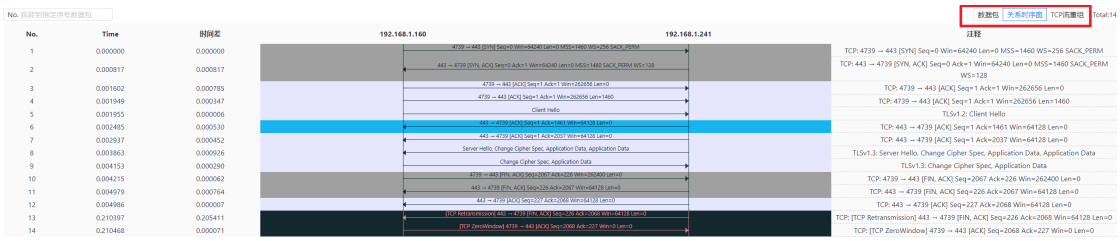
全流量存储功能允许网络流量在不影响实时监控性能的前提下进行高效存储。系统可配置根据需要保存 长时间段的网络流量数据，并具备灵活的存储管理选项，确保流量数据的安全性、可访问性和完整性。回溯分析 功能提供了对历史流量的 深入分析，用户只需在 Web 界面 中简单操作，选择需要回溯的时间段，即可快速过滤和提取相关数据。该功能不仅能高效支持故障排除，还能帮助用户追踪 特定事件、异常行为 或 安全攻击。回溯的流量数据可以再导入其他系统，如 IDS/IPS，为 安全事件检测与响应 提供有效支持。

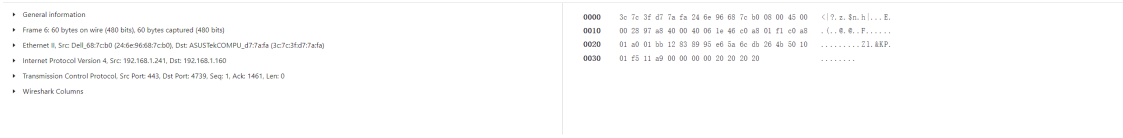
通过全流量存储与回溯分析，AnaTraf 网络流量分析仪为用户提供了强大的流量追溯能力，确保了网络问题能够被快速识别与定位，并在安全审计、性能评估等场景中提供宝贵的历史数据支持。这不仅提升了网络运维效率，还增强了网络安全防护能力，保障了企业网络的稳定和安全。

3.4 在线解码



AnaTraf 网络流量分析仪内置强大的在线解码功能，用户可通过系统提供的 Web GUI 界面，快速实现对网络流量的检索、过滤与深度分析，无需本地安装任何工具，即可在线对抓取的网络数据包进行逐帧解析，直观展示各层协议字段及其内容，极大提升了网络故障排查的效率。





通过灵活的查询条件，用户可快速定位目标流量，例如指定 IP、端口、协议类型、关键字等，从海量数据中筛选出关注的通信会话。同时，AnaTraf 支持 TCP 会话重组与交互时序图展示，能够完整还原一次 TCP 通信的上下文交互过程，帮助用户清晰理解通信行为和应用逻辑，尤其适用于故障诊断、异常检测及入侵分析等场景。

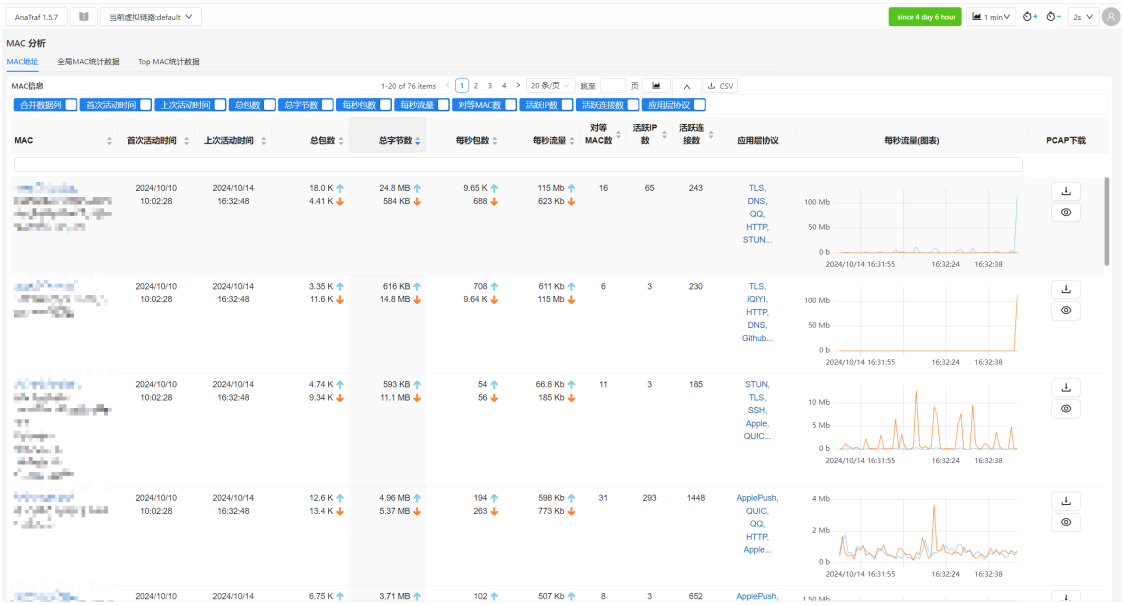
3.5 OSI 2-7 层分析

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。

3.5.1 MAC分析

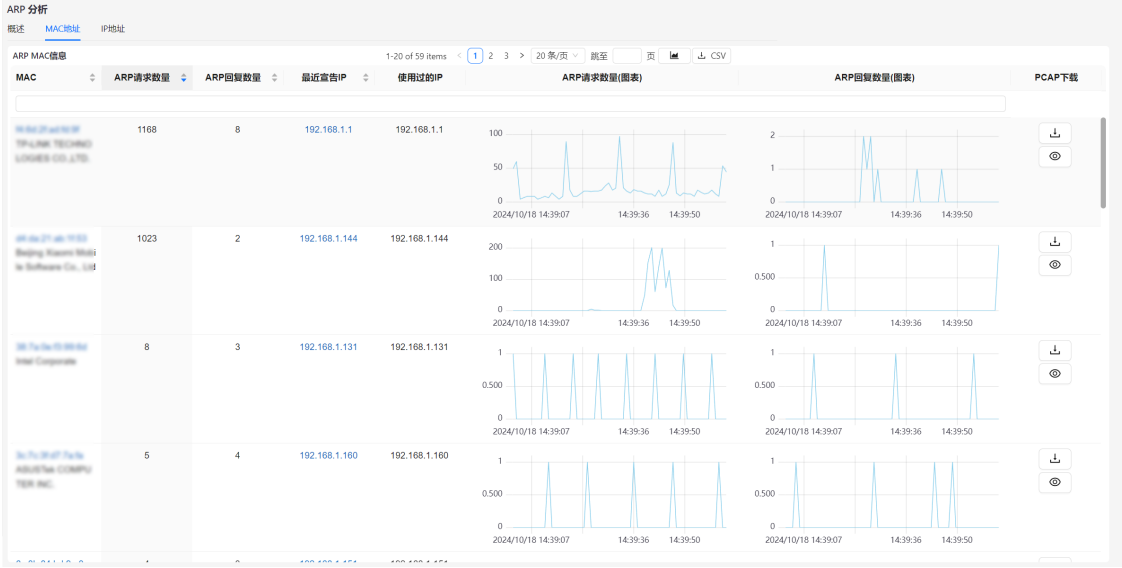
AnaTraf 网络流量分析仪内置的 **MAC 分析功能**运行于网络协议栈的第二层，专注于以太网帧级别的流量观测与分析。该模块能够全面展示网络中出现的所有 MAC 地址信息，并关联其对应的通信行为与协议类型，帮助用户深入理解链路层通信结构与设备间的数据交互情况。



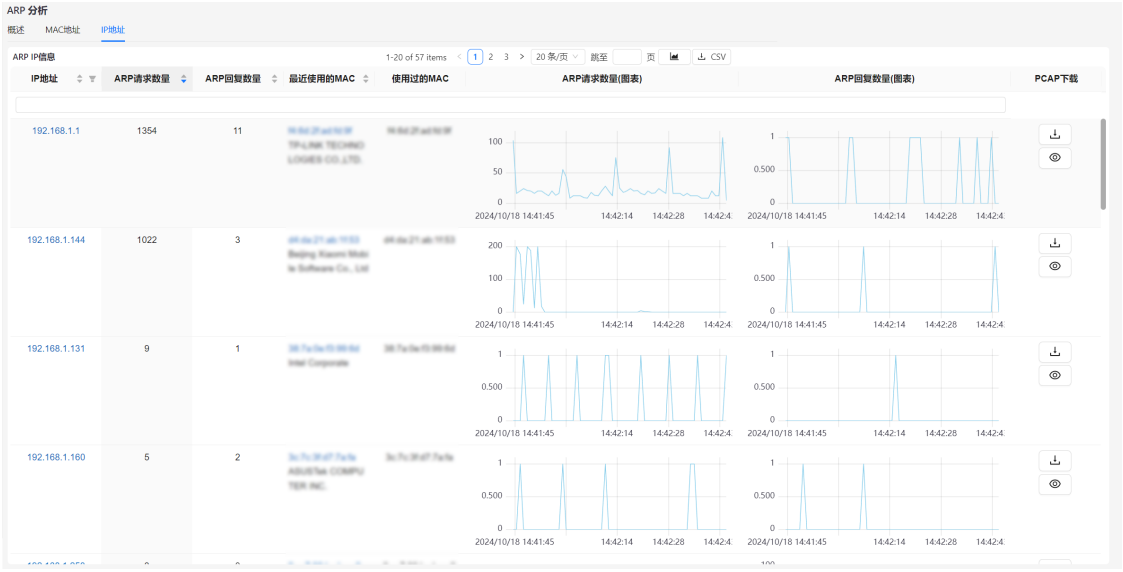
通过 MAC 分析功能，用户可直观查看各个 MAC 地址在一定时间窗口内所产生的网络流量总量、所使用的协议类型（如 ARP、IPv4、IPv6 等），以及每种协议所占的带宽比例，便于发现异常通信行为或带宽占用异常的设备。此外，系统还提供 **MAC Peer 分析视图**，可展示任意两个 MAC 地址之间的双向通信流量详情，帮助识别网络中的关键通信对。

3.5.2 ARP分析

AnaTraf 网络流量分析仪的 **ARP 分析功能**运行在网络协议栈的第二层，专注于分析地址解析协议（ARP）相关的通信行为，用于揭示 MAC 地址与 IP 地址之间的映射关系。通过持续跟踪网络中的 ARP 请求与响应数据包，系统可动态构建一套完整的 **MAC-IP 关联数据库**，为设备识别、地址解析异常检测及网络安全审计提供基础数据支撑。

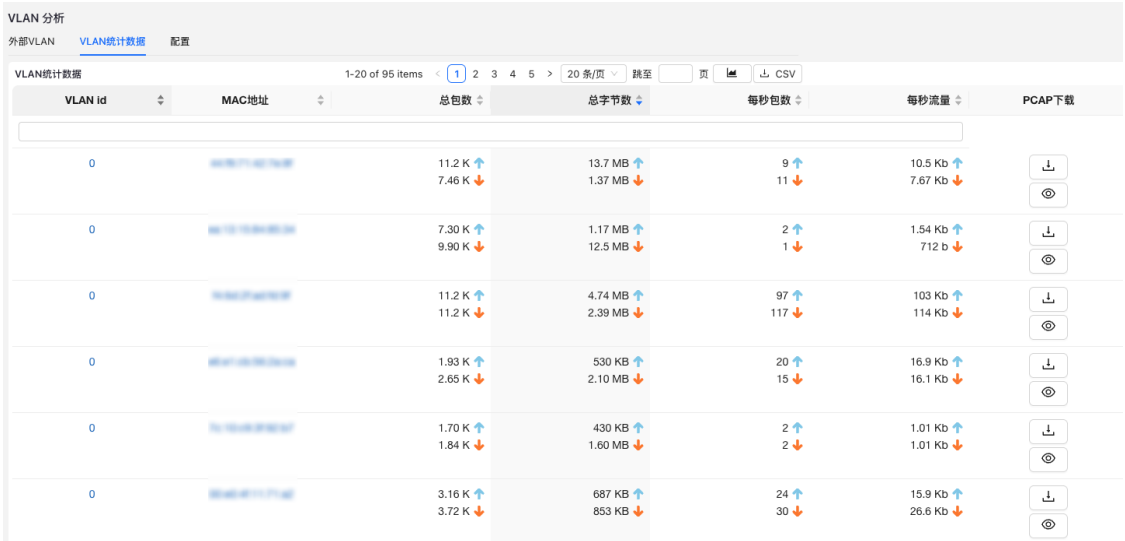


该模块不仅能够实时记录每个 ARP 交互过程，还能识别网络中各个 MAC 地址当前所对应的 IP 地址，帮助网络管理员准确掌握终端设备的身份与位置。通过可视化界面，用户可以查看每一条 ARP 记录的发起方、响应方、所用 IP 与 MAC、时间戳等详细信息，并能快速筛查出异常模式，如 **ARP 欺骗**、IP 冲突或频繁变更的绑定关系。



3.5.3 VLAN分析

AnaTraf 网络流量分析仪提供的 **VLAN 分析功能** 使用户能够深入掌握网络中基于虚拟局域网（VLAN）的流量分布与隔离情况。该模块自动识别并解析所有经由分析仪观测到的 VLAN 标签信息，全面展示当前网络中各个 VLAN 的活跃情况与数据传输行为。



系统对每个被检测到的 **VLAN ID** 进行统计，详细列出该 VLAN 内的总流量、协议类型分布及通信设备的 MAC 地址与各自的流量占比，帮助管理员快速掌握不同虚拟网络之间的带宽使用状况与通信模式。通过关联 MAC 地址信息，用户还可以识别出每个 VLAN 中的核心通信节点，及时发现高流量设备或异常通信行为。

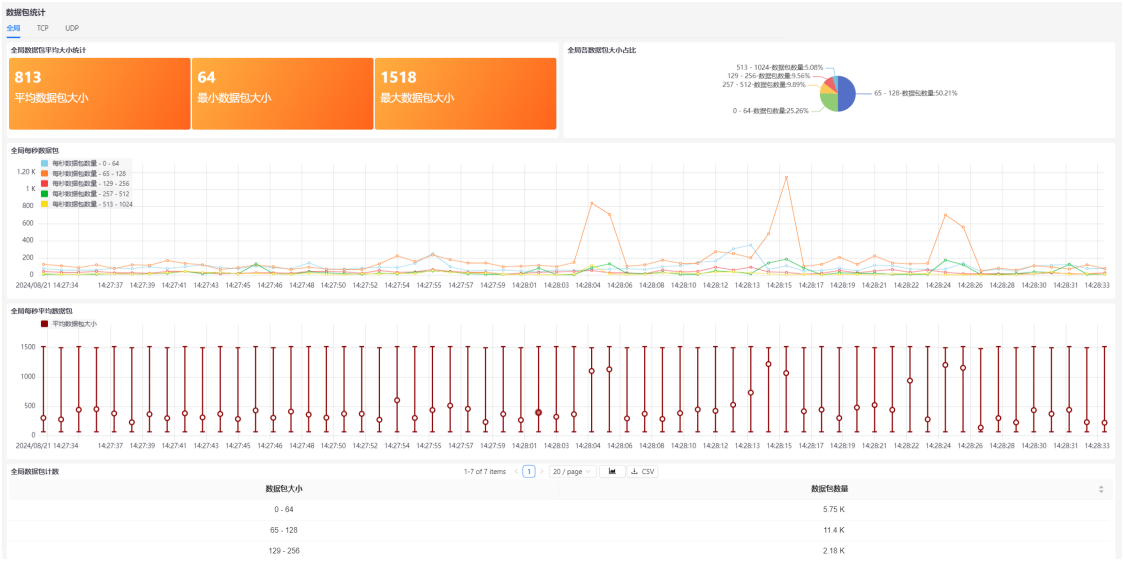
3.5.4 L2 QoS分析

AnaTraf 网络流量分析仪支持对二层网络服务质量（**L2 QoS**）的精确分析，能够对基于 VLAN 标签中的优先级字段的流量进行全面统计与分类。该模块可实时展示网络中各个 VLAN 所使用的优先级（Priority Class）对应的流量分布情况，帮助用户深入理解不同业务类型在网络中所占的资源比例与服务级别。

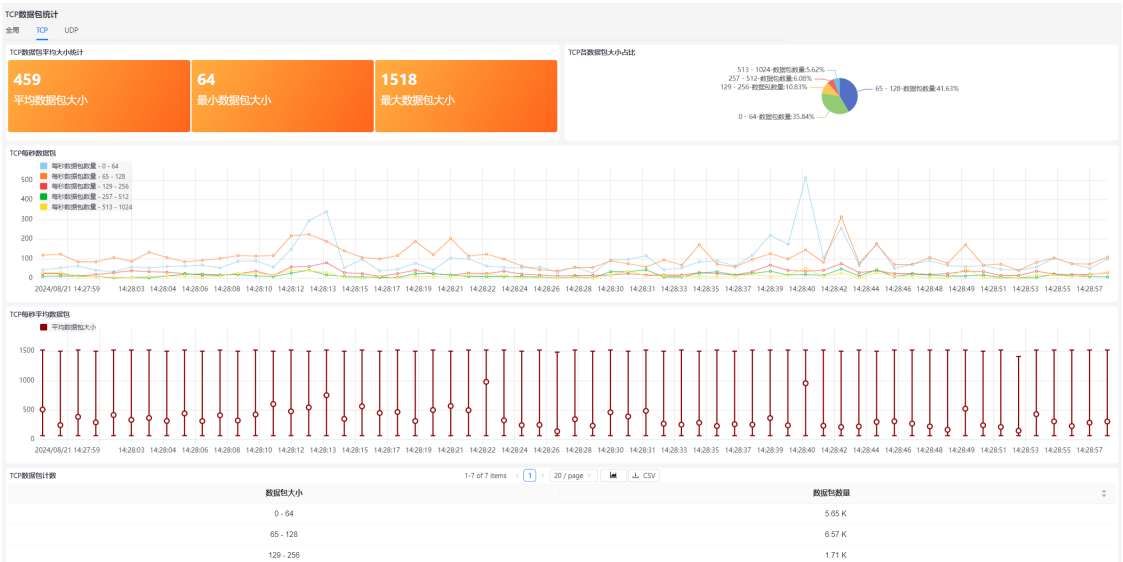
PCP	优先级	简称	描述
1	0（最低）	BK	背景流量
0	1（默认）	BE	尽力而为
2	2	EE	极大努力
3	3	CA	关键应用程序
4	4	VI	视频，< 100ms 延迟和抖动
5	5	VO	音频，<10 ms 延迟和抖动
6	6	IC	网间控制
7	7（最高）	NC	网络控制

通过对 VLAN 标签中 3 位优先级字段的解析，L2 QoS 分析功能将流量细分为多个服务等级（例如语音、视频、普通数据等），并提供各优先级队列的流量统计、占比变化和趋势分析。借助这一功能，管理员可以快速评估当前 QoS 策略的实际执行效果，发现资源分配不均、优先级滥用或关键业务带宽被压缩等问题。

3.5.5 数据包大小统计



AnaTraf 网络流量分析仪提供全面的**数据包大小统计**功能，帮助用户从微观维度理解网络流量的组成与特征。该模块针对分析仪接收到的全部流量，统计并展示数据包的**最大值、最小值、平均大小**，以及不同数据包大小范围的分布情况，直观反映出网络通信的负载特性与行为模式。

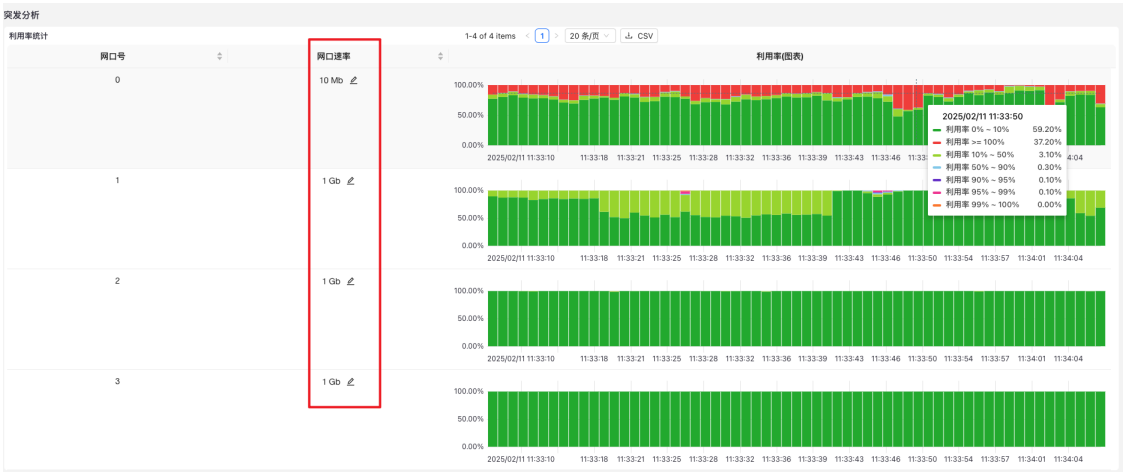


统计内容不仅覆盖全量网络流量，还对 **TCP** 与 **UDP** 两种主要传输层协议进行独立分析。用户可以分别查看 TCP 与 UDP 流量中数据包大小的分布图表和关键统计指标。

3.5.6 突发分析

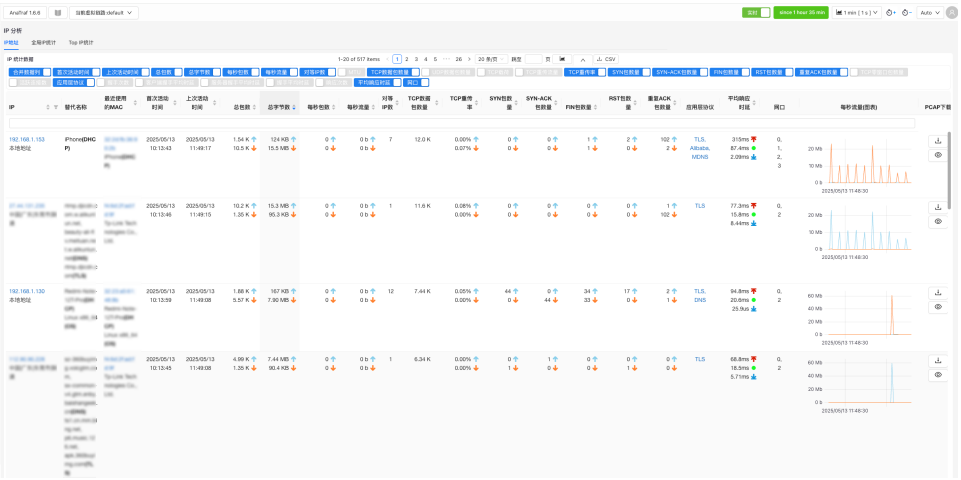
突发分析模块以 1 ms 的时间间隔测量每个网口的利用率，并显示利用率的图表。利用率的图表上显示：“利用率 0% ~ 10%”、“利用率 10% ~ 50%”、“利用率 50% ~ 90%”、“利用率 90% ~ 95%”、“利用率 99% ~ 100%”、“利用率 >= 100%”。

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%。



3.5.7 L3 IP 分析

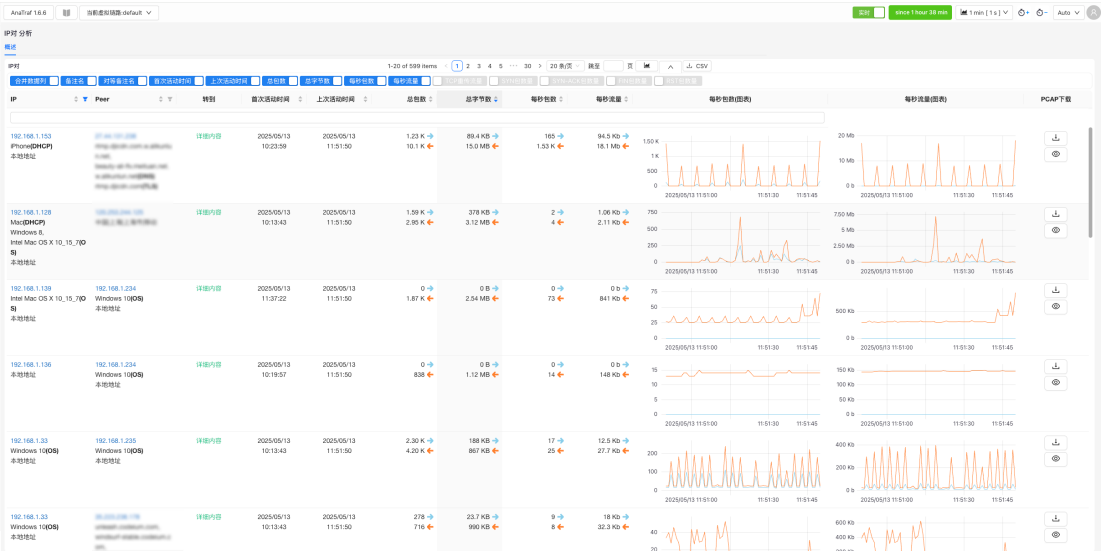
AnaTraf 网络流量分析仪的 L3 IP 分析功能 工作于网络协议栈的第三层，专注于对 IPv4 和 IPv6 地址相关的通信行为进行全面监测与统计。该模块能够实时记录网络中出现的所有 IP 地址，并详细统计每个地址产生或接收的总流量、所使用的传输协议（如 TCP、UDP、ICMP 等）。



通过对 IP 层通信的持续跟踪，系统不仅提供每个独立 IP 的流量视图，还构建起 IP 之间双向通信的完整记录，支持对每对通信 IP 地址之间的交互流量进行详细分析。这包括每个连接会话所使用的协议类型、方向、数据包数量和字节数等关键指标，为用户提供全景式的第三层流量视图。

3.5.8 L3 IP Pairs分析

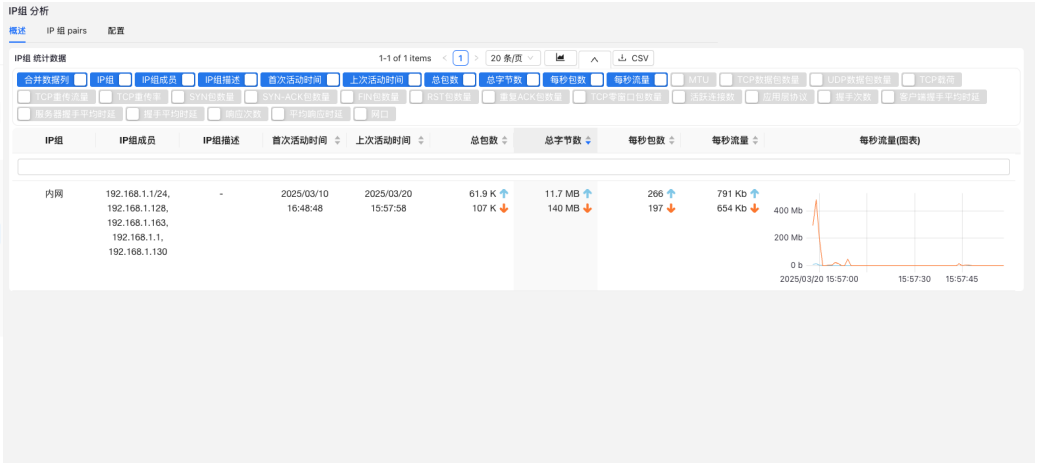
AnaTraf 网络流量分析仪的 L3 IP Pairs 分析功能 提供了基于通信对的精细化流量统计，帮助用户全面掌握网络中任意两个 IP 地址之间的交互行为与通信状态。该模块深入分析所有观测到的 IP 对（IP Pairs），并记录每一对通信双方的详细数据，包括流量方向、通信时序以及关键协议行为特征。



对于每一组 IP 地址对，系统提供如下信息：对端 IP 地址、首次活动时间、上次活动时间、上下行数据包与字节数、TCP 重传流量，以及 SYN、SYN-ACK、FIN 和 RST 包的数量。这些统计项不仅揭示了通信的持续性与流量模式，还能有效反映连接建立与终止的过程是否正常，是否存在异常重传或连接失败等问题。

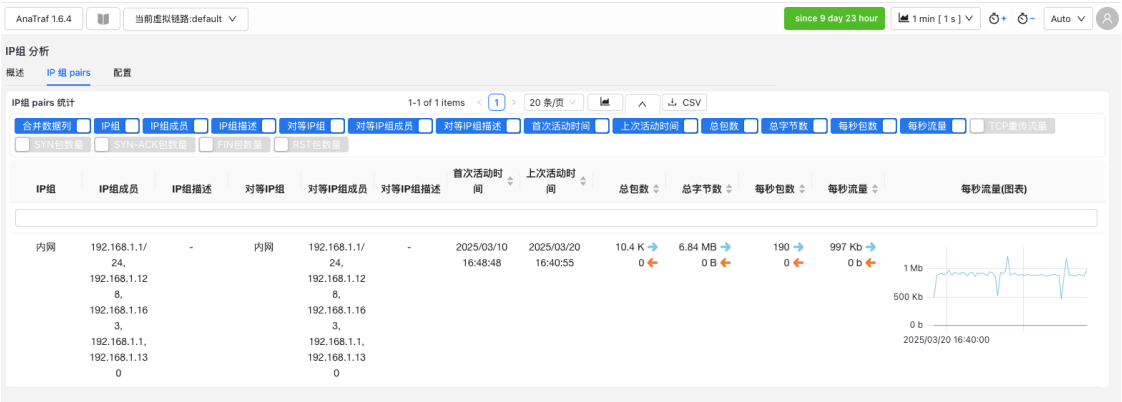
3.5.9 L3 IP Group分析

AnaTraf 网络流量分析仪的 L3 IP Group 分析功能 提供了基于自定义 IP 地址集合的高维度流量统计与行为分析能力。该模块允许用户将任意单个 IP 地址、IP 网段划分为一个或多个逻辑性的 IP 组，以实现对特定主机群体、业务系统、区域网络等进行定向的通信行为分析与性能监控。IP 组之间支持重叠，单个 IP 地址也可以同时归属多个组，为多维视角下的分析提供了极高的灵活性。



系统针对每个 IP 组，提供丰富的统计信息，包括组成员列表、组描述、首次与最近活动时间、收发的包数与字节数、收发速率与包速、上下行 MTU、TCP 与 UDP 包数量、各类 TCP 控制报文（SYN、SYN-ACK、FIN、RST、零窗口）的统计数据等。此外，还支持对组内 TCP 会话数量、活跃连接数、应用层协议类型、客户端与服务器握手行为（次数与时延）以及响应时延进行分析，覆盖从网络层到应用层的关键性能指标。

系统还支持对 IP 组之间的通信流量进行统计分析，揭示不同逻辑区域间的交互模式与数据流向。



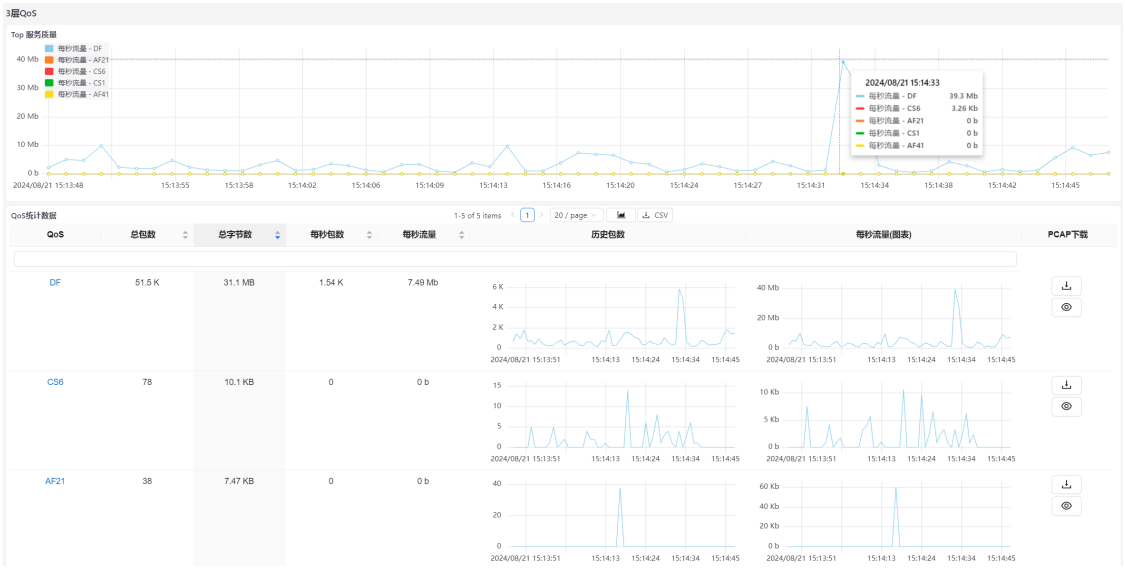
3.5.9 L3 QoS分析

AnaTraf 网络流量分析仪的 L3 QoS 分析功能 支持对 IP 层服务质量策略的全面监控与评估，主要针对差分服务编码点（DSCP，Differentiated Services Codepoint）字段进行实时流量统计与分类分析。通过解析 IP 头部中的 DSCP 标记，该模块可以准确识别网络中不同服务等级（如 EF、AF、CS 等）的流量分布情况。

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

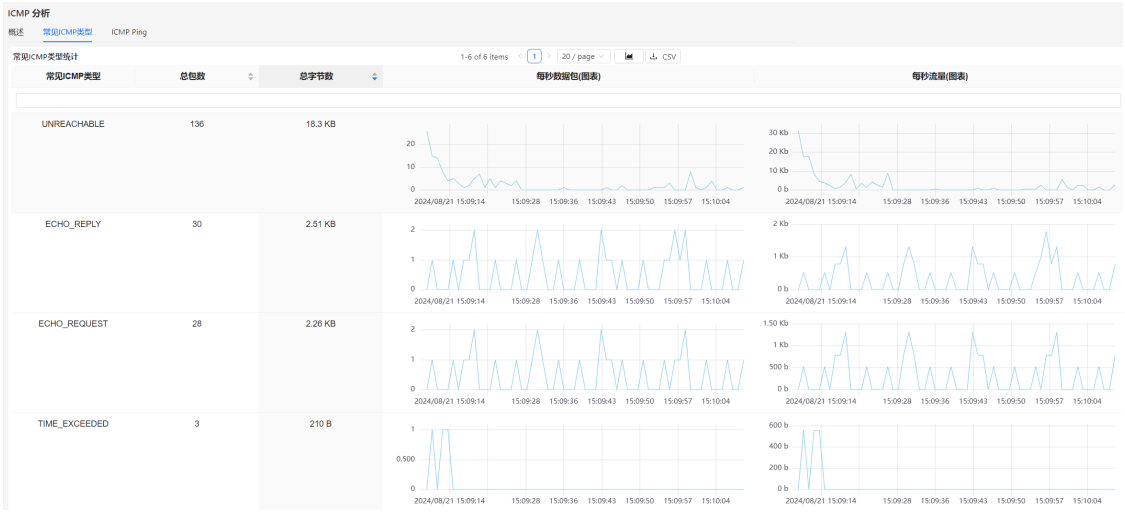
业务类型	DSCP 名	DSCP 值
OAM	CS2	16
High-Throughput Data	AF11, AF12, AF13	10, 12, 14
Standard	DF (CS0)	0
Low-Priority Data	CS1	8

系统按各个 DSCP 值对流量进行聚合和统计，展示各类业务流的带宽占用、数据包数量、占比变化等关键指标，帮助用户了解不同类型业务（如语音、视频、普通数据、控制类通信）在网络中的优先级配置及其实际传输状态。



3.5.10 L3 ICMP 分析

AnaTraf 网络流量分析仪的 L3 ICMP 分析功能 专注于 ICMP 流量的实时监测与详细分析，帮助用户深入了解网络中的控制消息传输情况。该功能通过展示一段时间内观测到的所有 ICMP 报文的数量和总字节大小，提供了全面的流量概况。用户可以查看每秒流量（bps）和每秒数据包数量（pps）的历史曲线图，从而分析 ICMP 流量的变化趋势和峰值波动，迅速发现网络性能问题或异常活动。

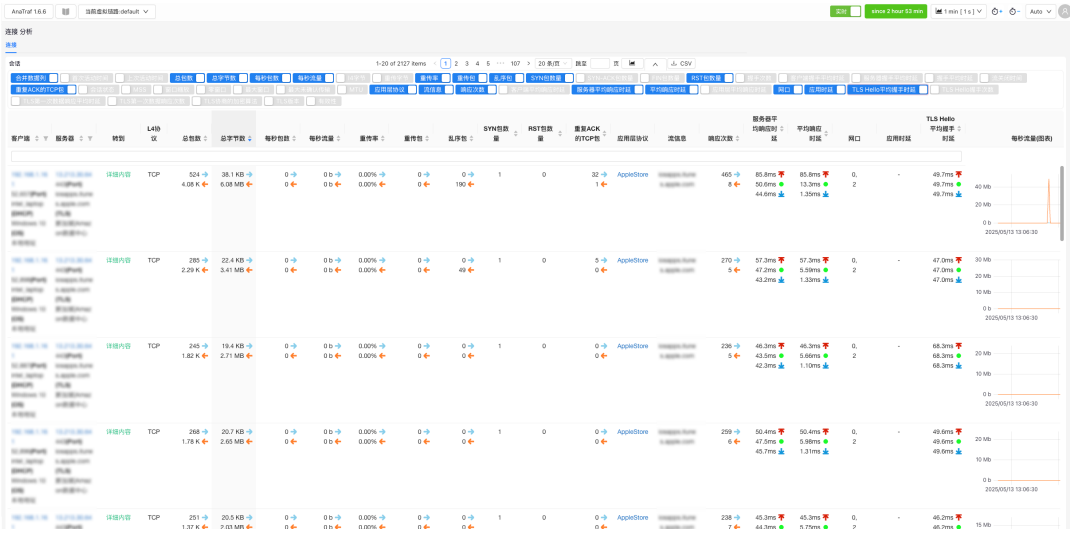


此外，L3 ICMP 分析功能 还提供了对所有 ICMP 类型的流量统计，包括常见的 Echo 请求与响应、目标不可达、时间超时等类型的流量数据。通过对不同 ICMP 类型的独立统计，用户可以清晰地了解每种 ICMP 类型的流量占比、网络健康状态以及是否存在异常的 ICMP 流量模式。

3.5.11 L4 连接分析

AnaTraf 网络流量分析仪的 L4 连接分析功能 负责对网络传输层的 TCP 和 UDP 连接进行全面、细致的监测与分析。该模块实时展示分析仪所观测到的所有 IP 地址之间建立的传输层连接，涵盖 TCP 会话与 UDP 通信活动，帮助用户掌握网络中主机间的连接关系与交互模式。

在 TCP 连接方面，系统不仅记录了连接的基础信息，还提供了丰富的性能与行为指标，包括 三次握手时延、首包响应时延、各类 TCP Flags（如 SYN、ACK、FIN、RST 等） 的统计数据。通过这些关键参数，用户可以深入分析连接建立与终止过程的时效性与稳定性，识别可能存在的连接延迟、丢包重传或异常中断问题。



3.5.12 L4 TCP分析

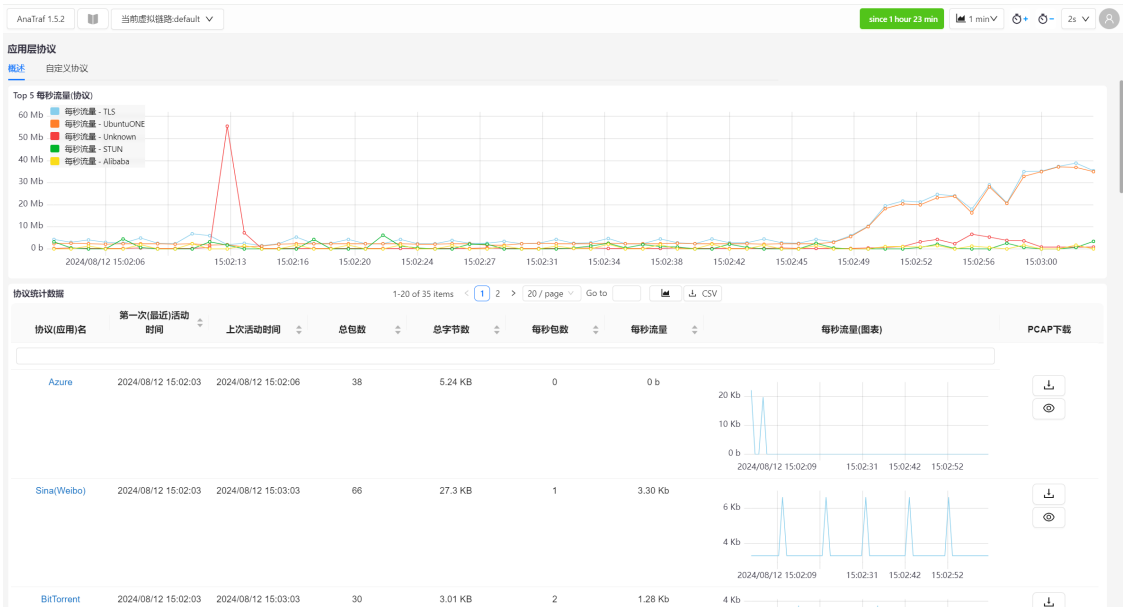
AnaTraf 网络流量分析仪的 L4 TCP 分析功能 旨在深入评估网络中 TCP 协议的通信质量与稳定性。该模块对所有观测到的 TCP 连接进行逐一分析，从连接建立、数据传输到连接释放的全过程中提取关键指标，为网络性能优化和故障诊断提供详实的数据支撑。

功能覆盖包括 TCP 三次握手的完整性分析、握手过程中的时延测量、应用首包响应时间 等，有助于评估服务器响应速度和连接建立效率。系统还对 TCP 报文中的各类标志位（Flags） 进行统计，例如 SYN、ACK、FIN、RST 等，便于用户识别连接异常中断、重置或非正常关闭等问题。

此外，该模块还重点监控影响 TCP 通信质量的关键现象，包括 TCP 重传（反映网络丢包、链路不稳定等问题）和 TCP 零窗口事件（表示接收方因缓存资源不足暂时无法继续接收数据）。通过这些指标，用户可以快速定位链路瓶颈、传输延迟原因，或识别潜在的协议栈或系统性能问题。

3.5.13 L7 应用层协议分析

AnaTraf 网络流量分析仪的 L7 应用层协议分析功能，致力于对网络中识别出的各类应用层协议进行深度识别与精确统计。该模块不仅支持主流应用协议（如 HTTP、HTTPS、DNS、SMTP、FTP、SSH 等）的自动识别，还支持对用户定义的私有或行业专用协议进行灵活扩展与分类，实现更全面的协议覆盖。

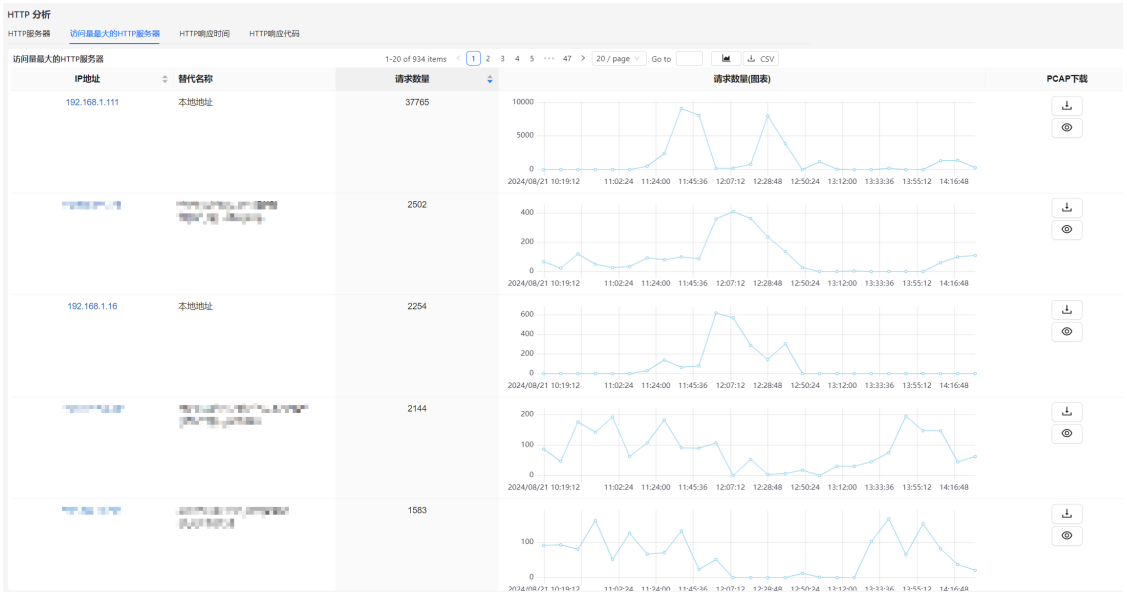


系统通过 DPI（深度包检测）技术识别协议特征，并以此为基础进行精细化的 流量统计分析，包括每种协议所产生的流量大小、数据包数量及其在整体流量中的占比，帮助用户全面掌握网络中应用行为的组成结构。

除了协议本身的流量分析，AnaTraf 还提供了与之关联的 IP 地址分析 和 连接统计，展示各个应用协议对应的通信主机、连接数量、活跃会话、数据方向及传输效率等信息。借助这些信息，用户可以快速定位高频使用的业务系统、识别异常活跃的通信主机，或发现潜在的协议滥用与安全隐患。

3.5.14 L7 HTTP 分析

AnaTraf 网络流量分析仪的 L7 HTTP 分析功能 负责对网络中传输的 HTTP 协议流量进行深入解析和多维度统计，帮助用户全面了解 Web 应用服务的运行状态与性能表现。该模块能够准确识别和提取所有通过 HTTP 协议进行通信的流量数据，对其中的请求与响应内容进行分类处理和行为分析。

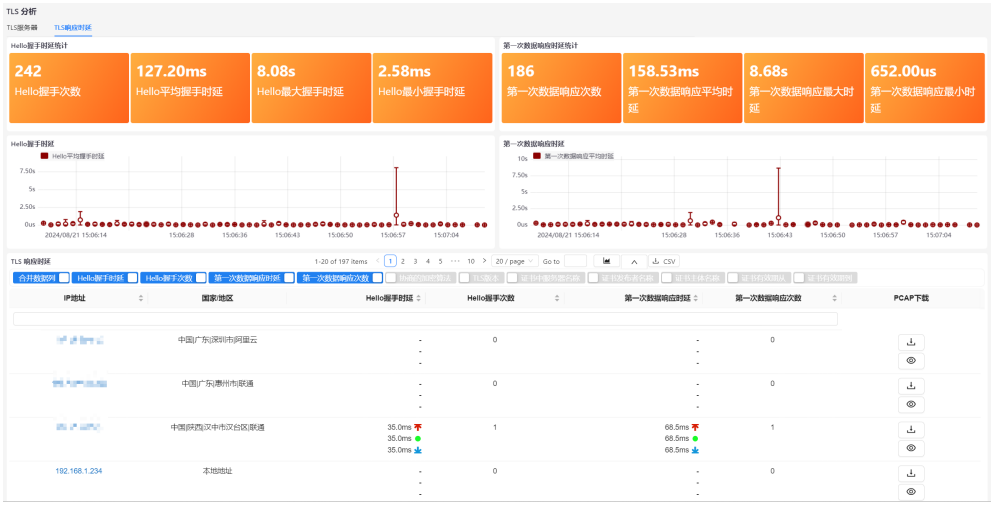


在功能层面，HTTP 分析模块提供了针对 HTTP 服务器的流量统计，包括各服务器 IP 的访问量、传输字节数、请求次数等指标，便于用户评估各 Web 服务节点的负载情况与活跃度。同时，该模块还支持对 HTTP 响应时间 的监控，反映客户端从发起请求到接收到响应所需的时延，用于评估 Web 应用的响应效率与用户体验。

此外，系统还对 HTTP 响应状态码（如 200、404、500 等） 进行汇总与统计，帮助用户快速发现异常响应情况，识别服务故障、资源未找到或内部错误等问题。结合时序图与流量趋势，用户可进一步定位性能瓶颈、分析访问模式或排查攻击行为（如异常爬虫、大量 4xx 请求等）。

3.5.15 L7 TLS 分析

AnaTraf 网络流量分析仪的 L7 TLS 分析功能 专注于对网络中传输的 TLS 加密通信进行识别与分析，为用户提供对加密流量的可视化洞察，确保在保障隐私的前提下实现对加密会话质量和行为的有效监控。



该模块能够自动检测分析仪所观测到的所有 TLS 流量，并提取关键的连接信息，包括 TLS 握手过程的时延 与 响应延迟，用于评估加密通信链路的建立速度和服务响应效率，有助于及时发现性能瓶颈或潜在故障。

同时，TLS 分析功能还支持解析 TLS 会话中的证书信息，如证书颁发机构（CA）、证书有效期、使用的加密算法等。通过对证书的统计与管理，用户可以识别过期、不可信或异常的证书，防范中间人攻击、伪造服务器等安全风险。

3.5.16 L7 DNS 分析

AnaTraf 网络流量分析仪的 L7 DNS 分析功能 专注于对网络中域名解析通信的全过程进行实时追踪与深入分析，帮助用户全面掌握 DNS 服务的运行状态、解析效率以及潜在的异常行为。

该模块可识别并解析所有观测到的 DNS 请求与响应报文，并统计对应的 DNS 服务器流量，包括每台 DNS 服务器处理的查询次数、传输字节量及访问频度，便于评估服务器负载及其在网络中的角色和活跃度。

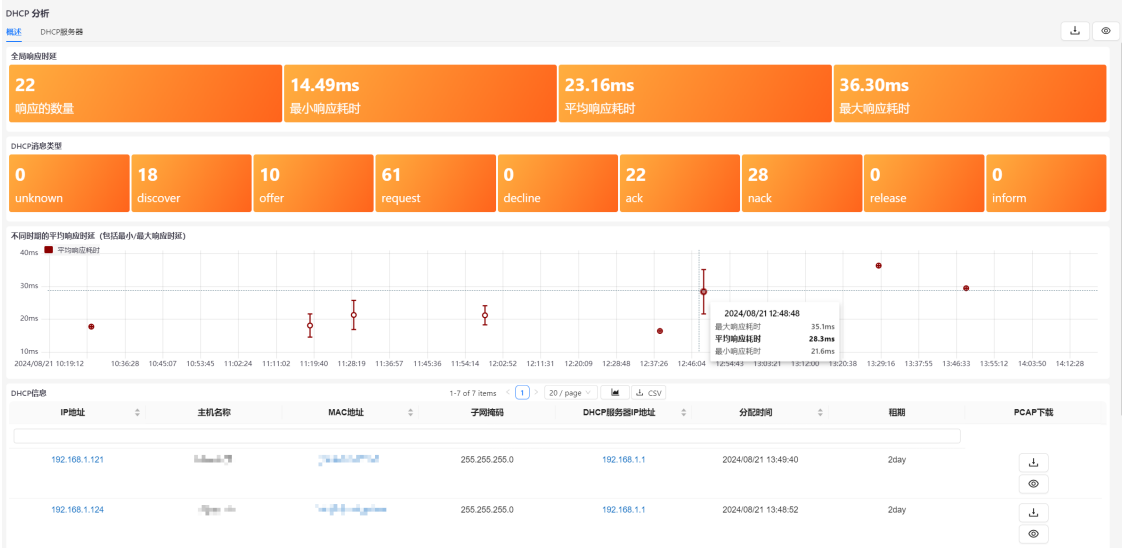
同时，系统详细记录每条 DNS 请求解析出的 IP 地址，帮助用户准确了解域名与 IP 的映射关系。模块还提供了 DNS 响应时间统计，用于评估域名解析的性能表现，辅助判断网络延迟、服务器响应慢或递归查询耗时等问题。此外，通过对 DNS 响应代码（如

NOERROR、NXDOMAIN、SERVFAIL 等） 的分析，用户可以快速识别解析失败、配置异常或潜在攻击（如 DNS Flood）等行为。

3.5.17 L7 DHCP 分析

AnaTraf 网络流量分析仪的 L7 DHCP 分析功能 专注于对网络中动态 IP 地址分配过程的实时监控与分析。该模块能够跟踪并解析所有 DHCP 请求和响应，帮助用户全面了解 IP 地址分配的动态过程，确保网络中设备能够高效、正确地获取所需的 IP 地址。

系统能够自动识别并统计 DHCP 消息类型，如 DHCP Discover、Request、Offer、ACK 等，并通过对这些消息的流量分析，用户可以清楚地了解每个设备的 IP 地址分配情况和网络活动。此外，模块还提供了 DHCP 响应时延 的统计分析，帮助用户评估 IP 地址分配过程中的响应效率，识别潜在的网络延迟或配置问题。



4 应用场景

4.1 发现并解决网络问题

当网络、服务器、客户端或应用程序发生故障时，AnaTraf 网络流量分析仪通过直观的 Web 界面 提供实时的 L2-L7 网络性能与质量指标 趋势图，详细的统计数据和指标展示，有效加速故障排除过程。通过精确的数据可视化和深度分析，网络管理员可以迅速定位问题来源，大幅度降低 平均修复时间（MTTR），确保网络和服务的高效运行。

4.2 基于报文的流量可视化和资产清单

AnaTraf 网络流量分析仪提供全面的 报文可视化功能，能够精准识别和捕获网络中每个设备、服务和协议的通信。它通过对 MAC、ARP、IP、DNS、端口及应用协议 的详细可视化，结合实时匹配、过滤功能以及灵活的导出机制，帮助用户快速发现网络中的潜在故障或异常。这样的功能不仅提升了故障排除的效率，还为资产清单和网络拓扑结构的维护提供了有力支持。

4.3 SSL/TLS服务器连接有效性和故障分析

随着加密流量的普及，AnaTraf 网络流量分析仪提供全面的 SSL/TLS 握手分析，实时检测 握手时延、数据响应时间 等性能指标，帮助管理员有效排查加密通信中的潜在故障。此外，AnaTraf 能够提供 TLS 协商版本、TLS 警告、加密密钥强度 以及 证书有效性 等关键信息，帮助用户深入分析 SSL/TLS 连接的健康状况，确保加密服务的可靠性和安全性。

4.4 多节点数据关联分析和故障排除

AnaTraf 网络流量分析仪支持跨多个数据采集点对同一应用的流量进行 关联分析。通过比对不同节点的流量数据，系统可以帮助用户发现网络中 分段丢失、重传 以及时延 等问题，准确定位影响应用服务质量的网络瓶颈或故障点。这使得网络管理员能够迅速找到网络问题的根源，优化应用性能，确保服务质量不受影响。

4.5 数据包快速过滤和在线解码分析

AnaTraf 网络流量分析仪通过强大的 数据包过滤功能，帮助网络管理员快速从实时流量或大规模 PCAP 文件 中提取感兴趣的数据包。用户可以选择特定的 IP、MAC 地址或 单一连接 进行精准过滤。系统完全支持 Wireshark 数据包分析，同时提供强大的 在线解码引擎，便于用户对捕获的流量进行深入分析，确保故障诊断的精确性和效率。

4.6 全流量回溯分析

AnaTraf 网络流量分析仪提供强大的 全流量回溯分析功能，使得用户能够便捷地记录并回溯网络流量。无论是出于故障排除、安全审计，还是数据保留的需求，网络管理员都可以通过 WEB 界面 轻松过滤和提取原始网络流量。提取的流量可进一步导入如 IDS/IPS 系统，为特定的安全事件创建触发机制，从而加强网络安全防护和事件响应能力。

4.7 工业以太网协议分析与故障排除

在工业环境中，AnaTraf 网络流量分析仪提供对多种工业以太网协议的支持和分析，包括 PROFINET、IEC 60870、S7、OPC 等协议。通过对这些协议的质量监控和性能分析，用户能够实时掌握工业自动化网络的健康状况，预防生产过程中可能出现的故障，降低生产停机时间，确保工控系统的稳定与安全运行。

4.8 业务系统性能分析与质量监控

在企业环境中，AnaTraf 网络流量分析仪帮助用户评估和监控 业务系统的性能。当业务系统未能按预期运行时，用户可以通过流量分析确定问题是源自内部网络、外部服务，还是客户端设备。系统通过提供对特定客户端、子网甚至全公司范围内的 服务质量分析，帮助 IT 团队识别问题源并评估其影响，确保业务系统始终处于最佳性能状态。

5 技术架构

网络流量分析仪软件架构如下图所示，主要分为管理面、控制面、收发面。

管理面提供了可视化的Web GUI页面以及 API 自动化对网络流量分析仪进行配置。

控制面中的设备管理系统允许用户进行偏好设置以及初始化设备，同时在日志中提供错误记录。网络流量分析仪为了提高用户的使用体验，提供了保存和上传配置的功能。同时提供数据列表、流量图表、在线解码工具，帮助用户清晰、直观地对流量进行分析。软件可在线升级，方便用户操作。

I/O面主要是控制报文的收发。


管理面
Web 服务器
API
控制面
设备管理系统
初始化管理
参数配置
偏好设置及状态管理
日志及错误管理
服务质量保障
数据列表及流量图表
在线解码
数据及配置保存、上传模块
软件在线升级
协议分析子系统
L2层分析
L3层分析
L4层分析
L7层分析
I/O面
收发驱动
操作系统
Linux操作系统
协议栈