虹科 Allegro 功能概览

目录

1. 网络流量分析与故障诊断

虹科 Allegro 是用于网络故障排除设备和网络分析的诊断工具，只需点击几下就能检测出网络中的错误和问题。它们由网络管理员部署以分析网络流量，既可以实时分析当前流量和事件也可以进行回溯分析。

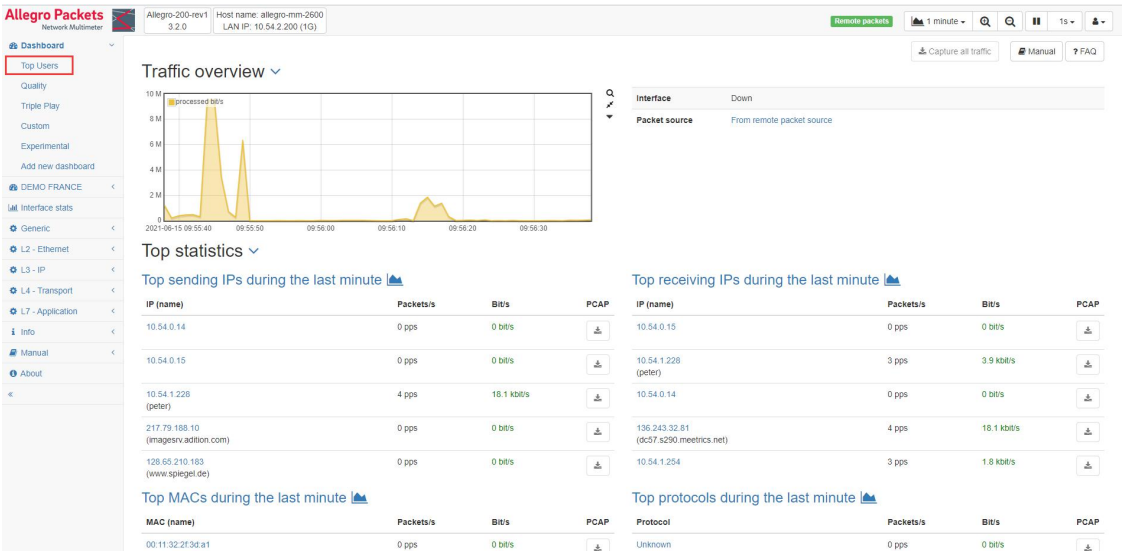
它能提供高粒度和详细的分析。因此，可以快速识别网络故障、性能瓶颈和数据包丢失等问题。

虹科 Allegro 使用高性能、强大的软件算法来分析负载峰值和干扰。同时，它能充当强大的网络监控工具，以确保高网络质量。

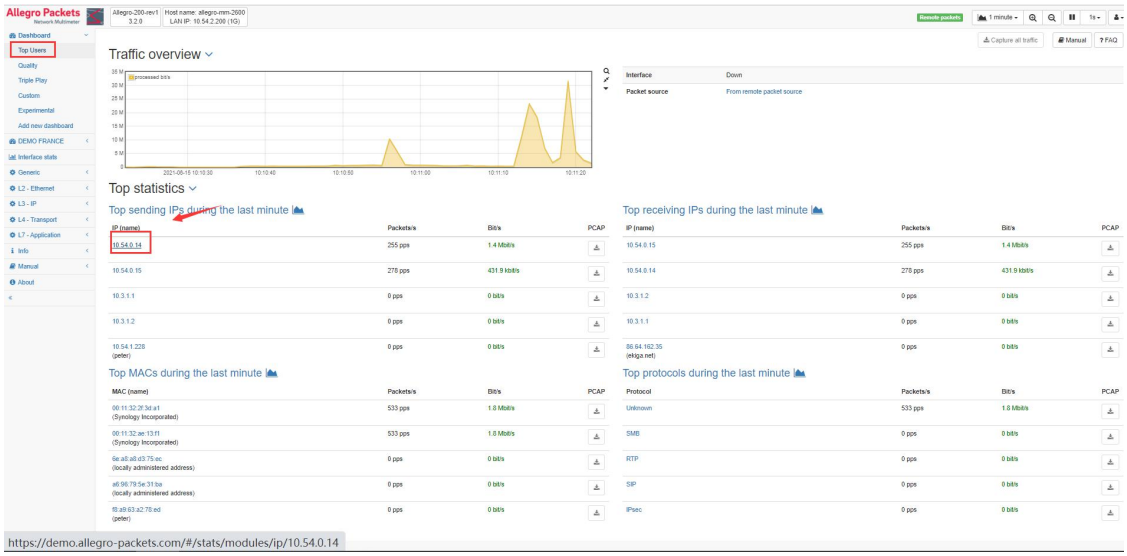
2. 全局视图

2.1 顶级用户

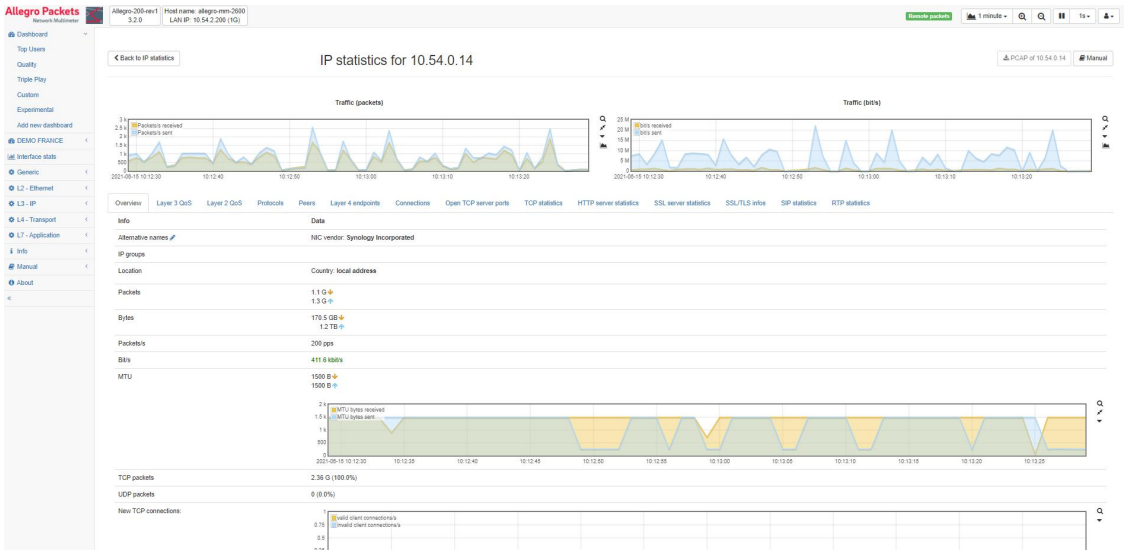
提供网络吞吐量概览视图，Top 发送 IP,Top 接收 IP，Top MAC,Top 应用协议。



注：视图中所有的蓝色字体，均可以点击进入进行详细分析，如点击 Top 发送 IP 中 10.50.0.14,进入详细分析。


Allegro Packets
Traffic overview
Top statistics
Top sending IPs during the last minute
Top receiving IPs during the last minute
Top MACs during the last minute
Top protocols during the last minute
https://demo.allegro-packets.com/#/stats/modules/ip/10.54.0.14

详细分析视图：

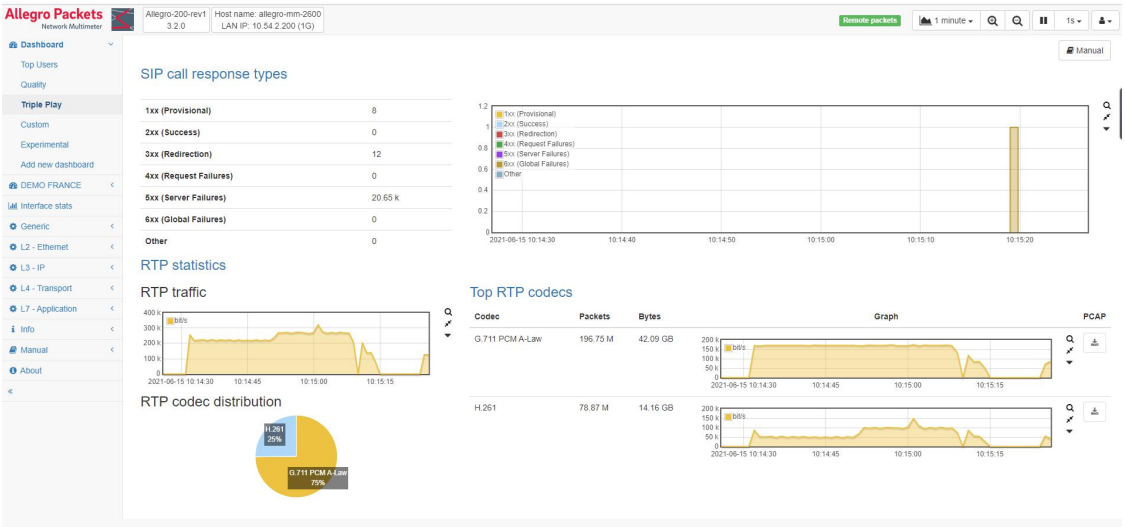

Allegro Packets
IP statistics for 10.54.0.14
Traffic (packets)
Traffic (bit/s)

2.2 质量分析

提供网络利用率视图，网络抖动指标和详细的 TCP 指标分析。

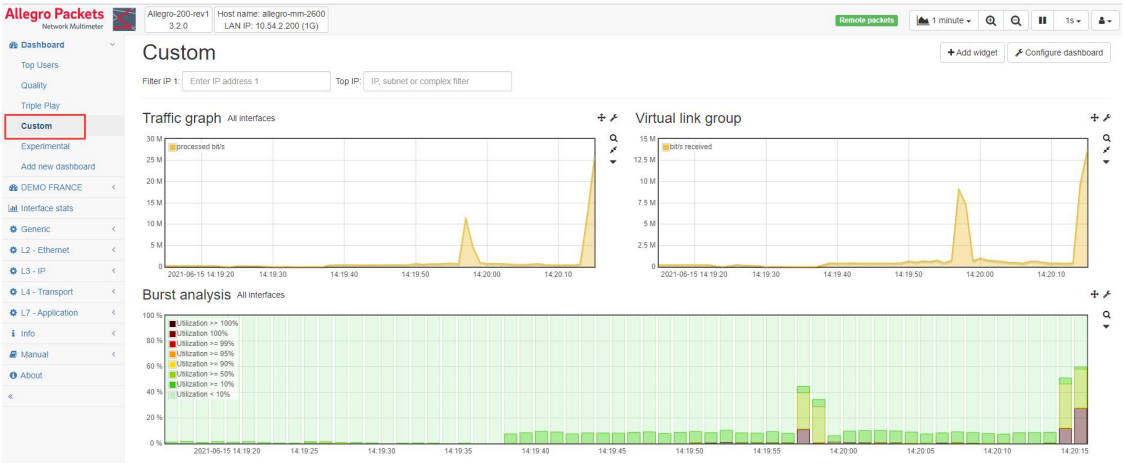
2.3 三重播放（Triple play）

SIP，RTP 分析视图。



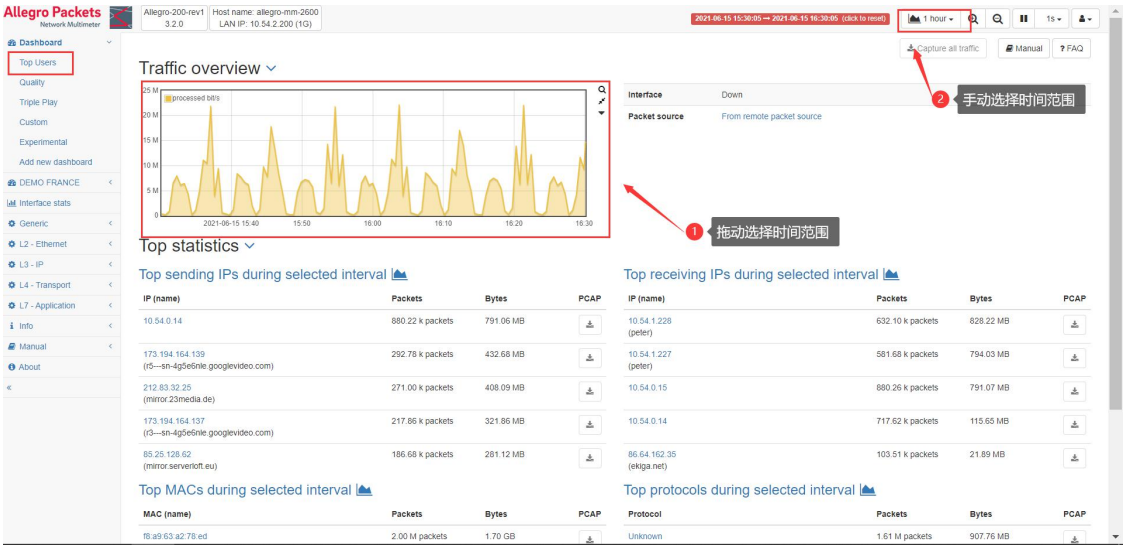
2.4 自定义仪表盘

自定义监控图表组。



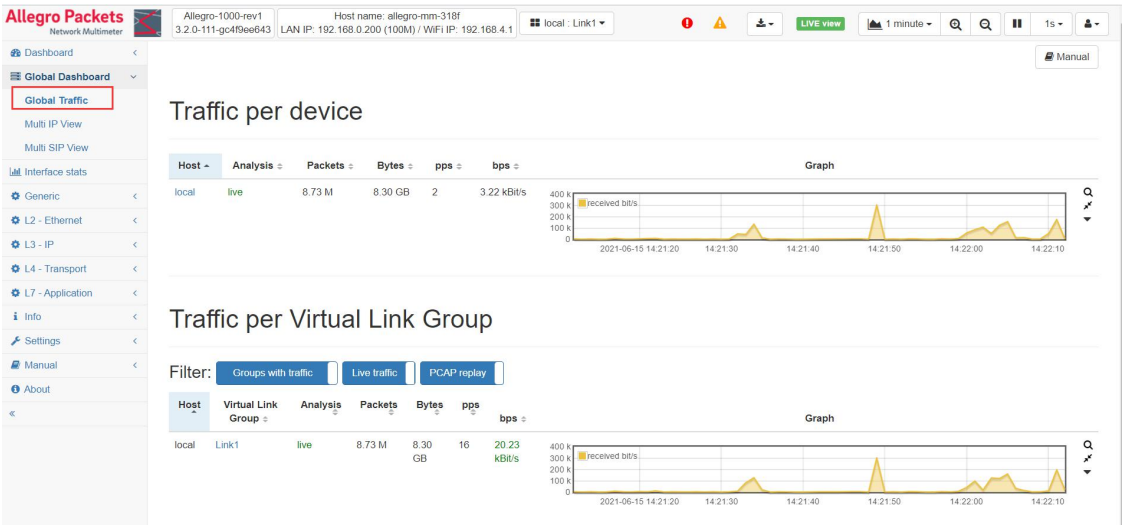
2.5 回溯分析

在任意图表内拖动选择时间范围，或者在右上角手动选择时间范围，可以对过去特定时间段进行回溯分析，也可下载该时间段的完整数据包到本地进行详细分析。



3. 全局流量统计信息

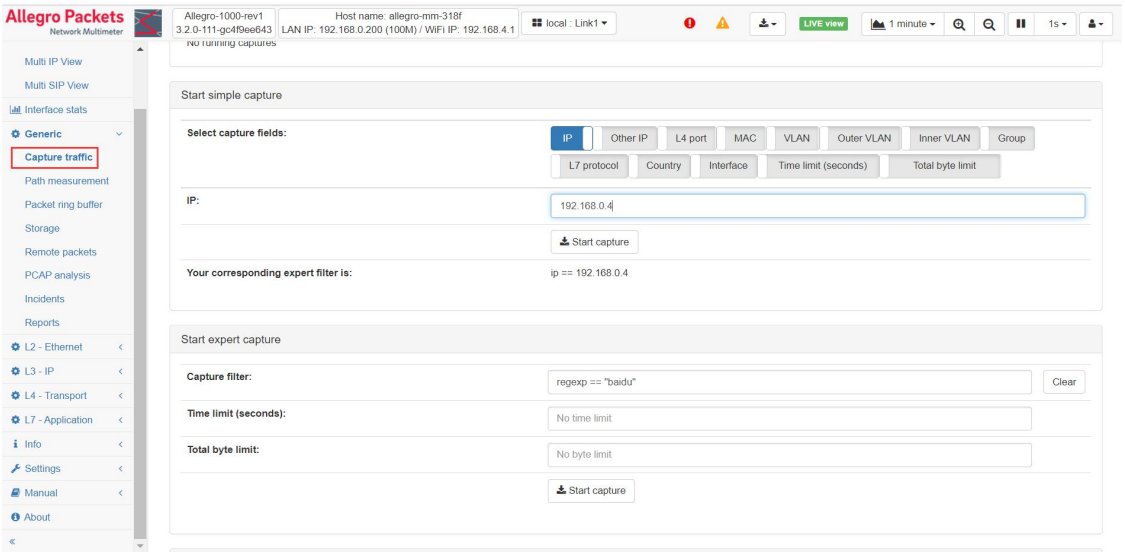
查看各个自定义虚拟链路，和全局流量统计信息。



4. 常用

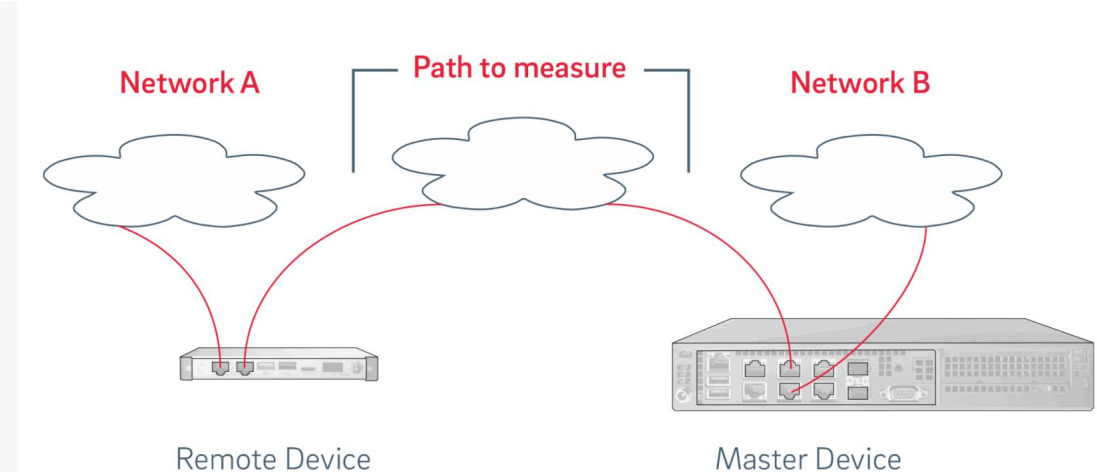
4.1 流量捕获

自定义过滤规则进行抓包分析。

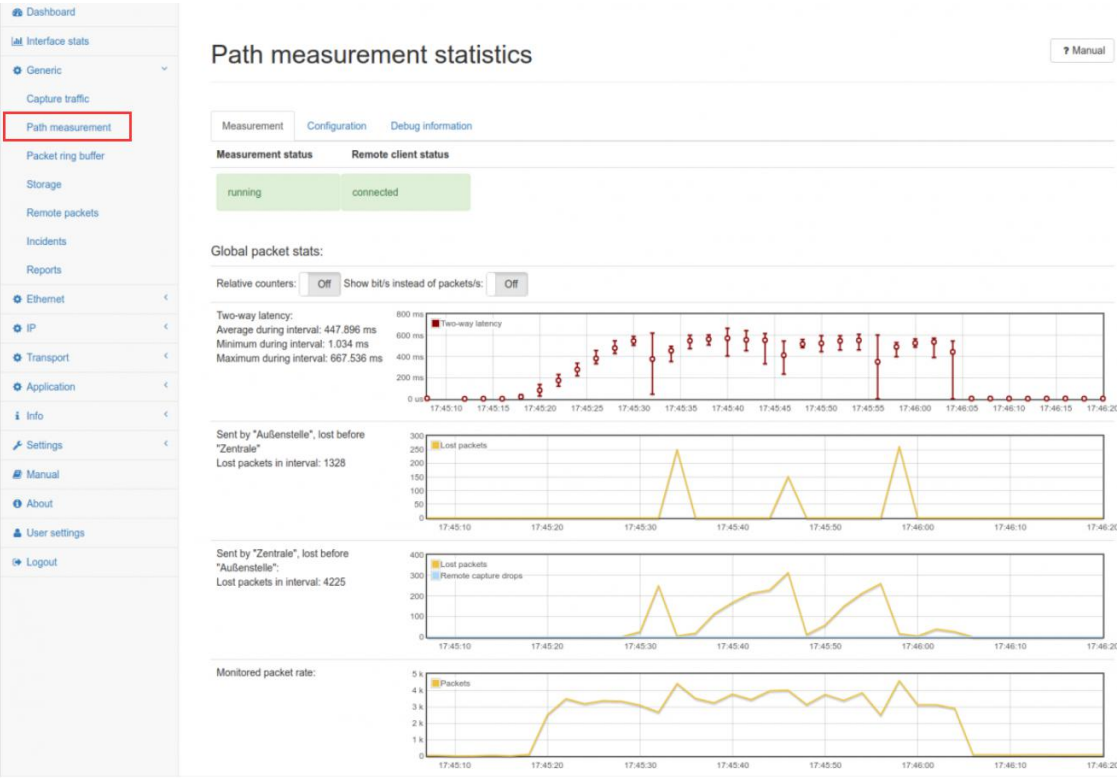


4.2 路径测量

测量通过互联网连接的两个网络之间的数据包丢失，延迟等等。

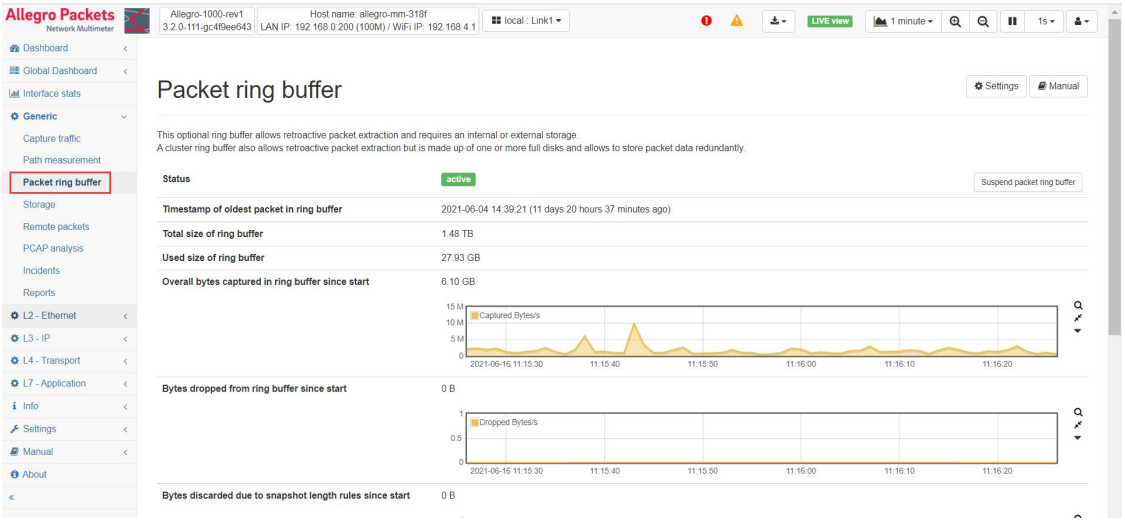


测量视图如下：



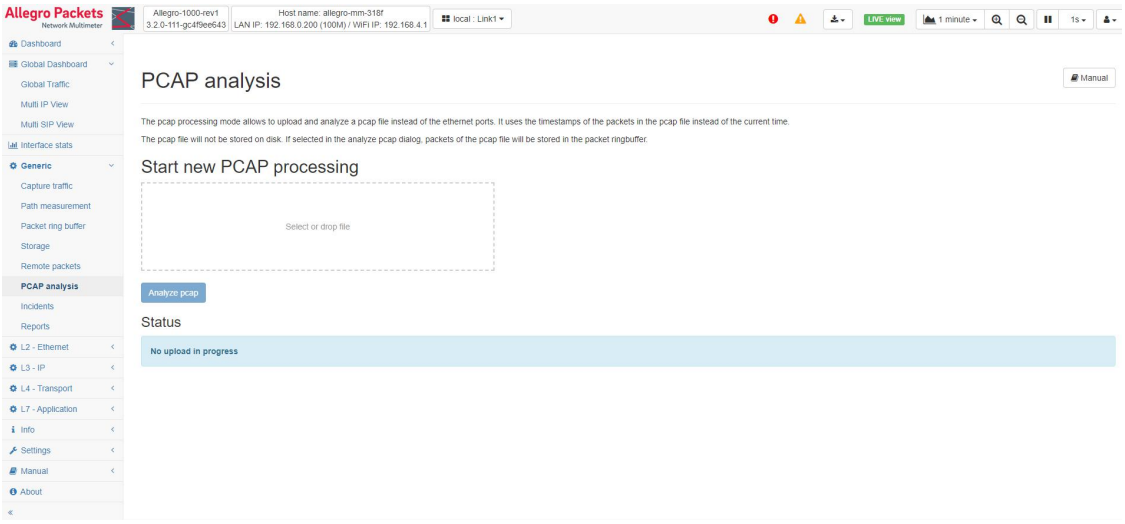
4.3 全流量存储

Allegro 提供了全流量存储功能，将捕获的流量存储在环形缓冲区内，环形缓冲区功能允许在外部存储设备上创建一个固定大小的缓冲区，所有处理过的数据包都将被记录到该缓冲区中。如果固定大小的缓冲区已满，则缓冲区中最旧的数据包将以循环方式替换为新数据包。



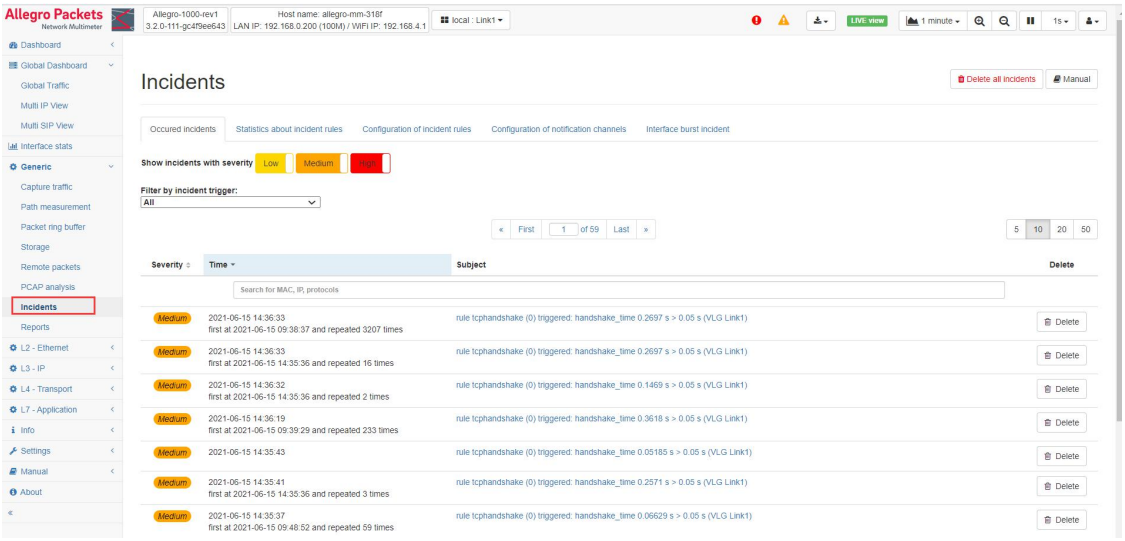
4.4 离线数据包分析

将需要分析的 PCAP 数据包导入 Allegro 进行分析。



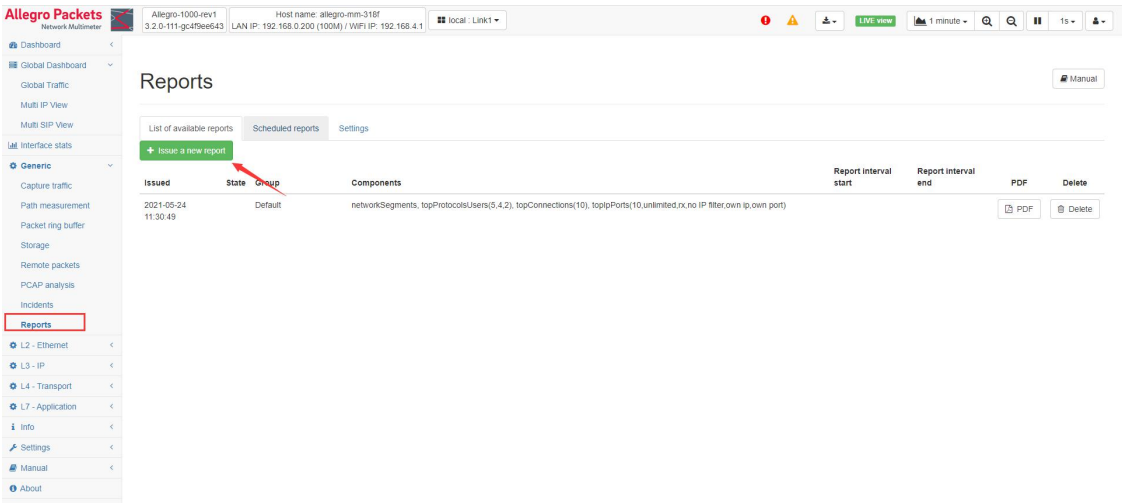
4.5 事件告警

自定义告警规则，统计告警事件。



4.6 报告生成

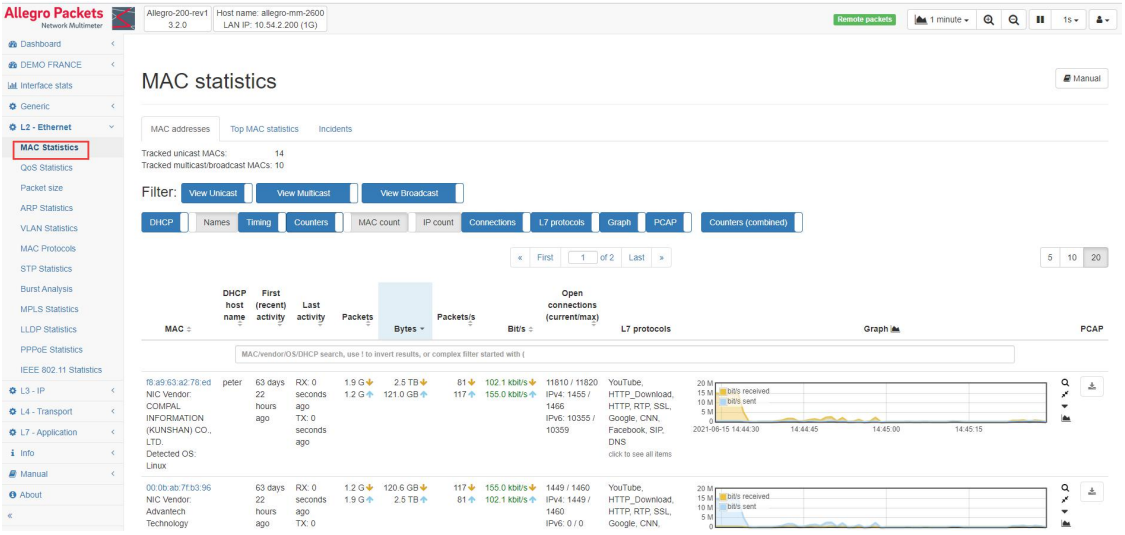
可自定义生成 PDF 格式报告。



5. 数据链路层监控

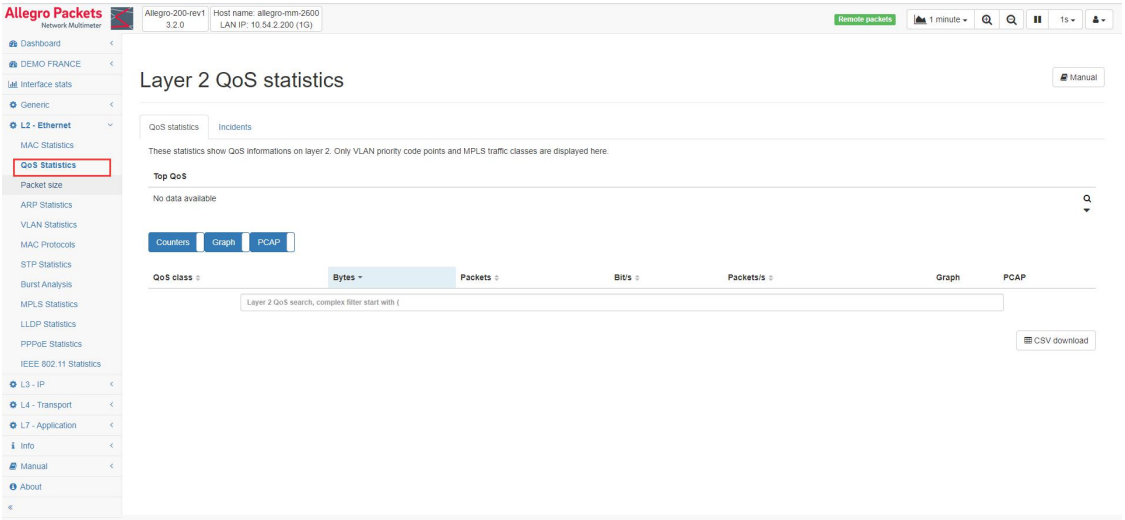
5.1 MAC 统计

监控所有 MAC 统计信息。



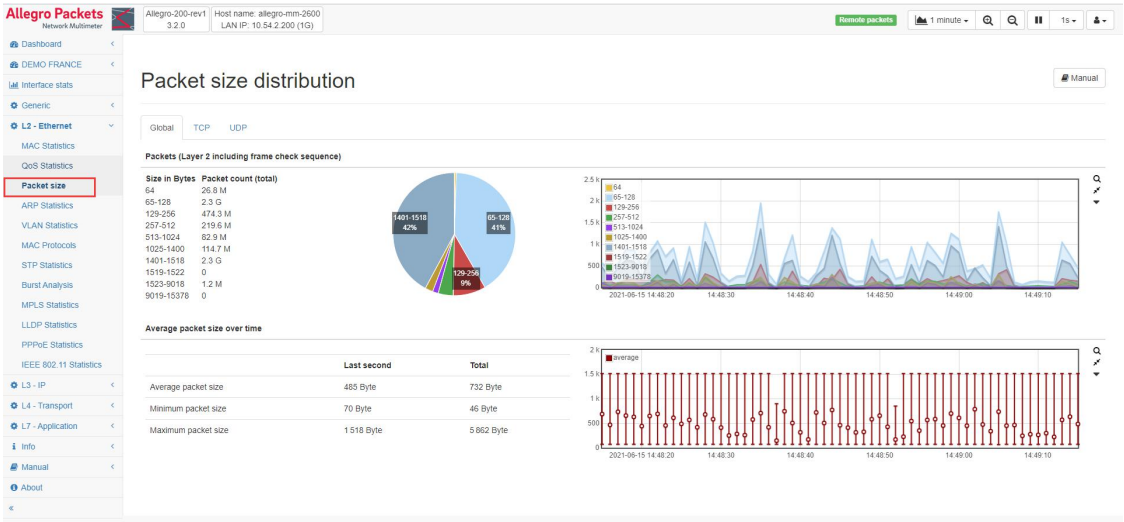
5.2 QoS 统计

显示了第 2 层的 QoS 信息。



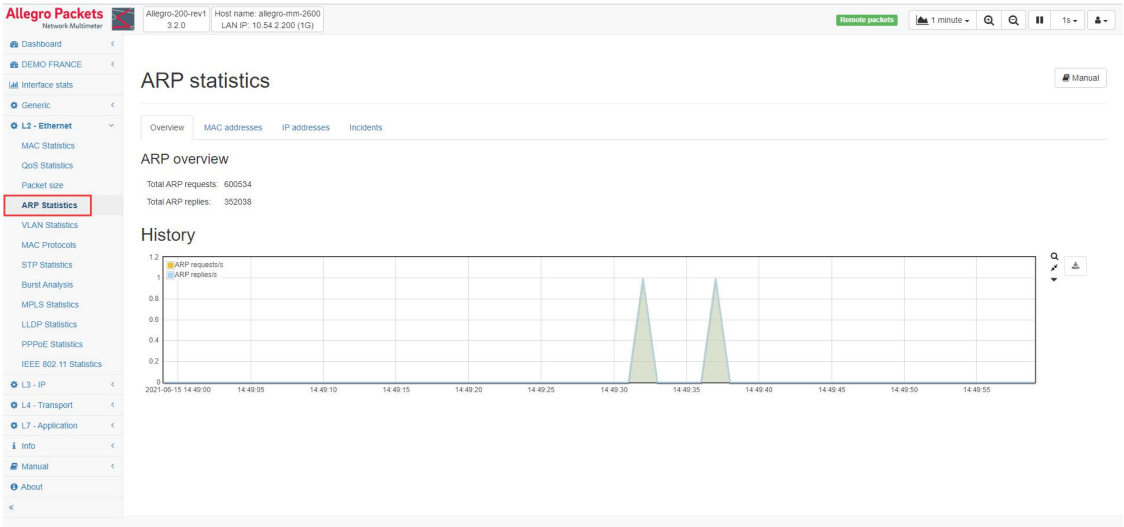
5.3 数据包大小统计

数据包大小分布详细统计信息。



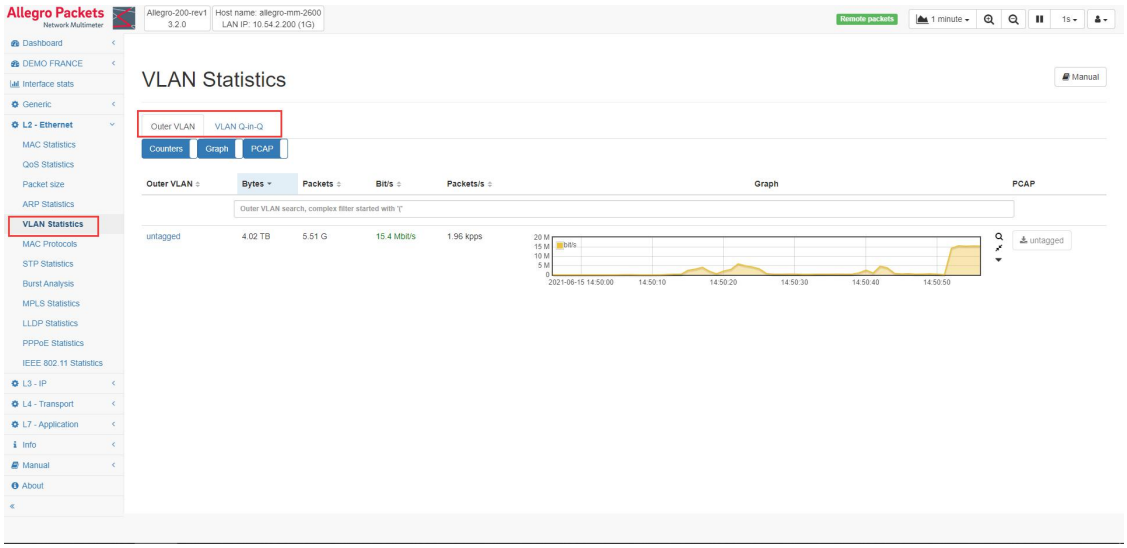
5.4 ARP 统计

址解析协议 (ARP) 用于第 2 层以跟踪哪个硬件（MAC 地址）使用哪个 IP 地址。ARP 模块监控请求和回复，并建立一个包含所有已知 MAC 和 IP 地址及其相关性的数据库。它还考虑了可能的欺骗警报，当某些计算机发送或回复错误的 MAC 地址，或多台计算机使用相同的 IP 应答时。由于配置错误或攻击，这些事件可能表明网络中存在某些问题。



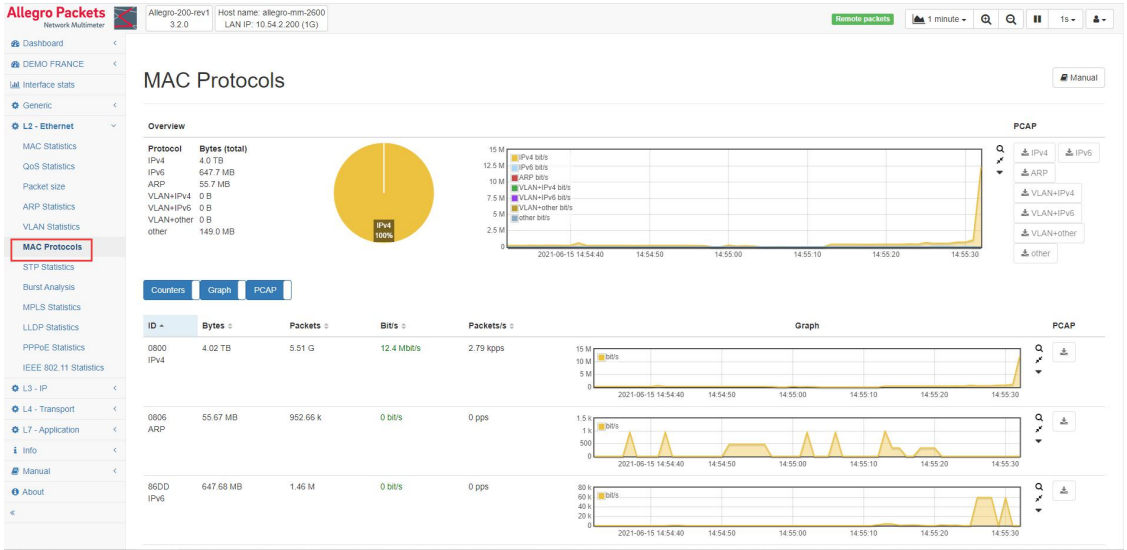
5.5 VLAN 统计

VLAN 统计信息显示有关所有可见 VLAN 的信息。支持 IEEE 802.1Q VLAN 和 IEEE 802.1ad Q-in-Q。该模块显示网络上看到的每个 VLAN 的流量统计。此外，始终显示有关没有任何 VLAN 标记的流量的统计信息。



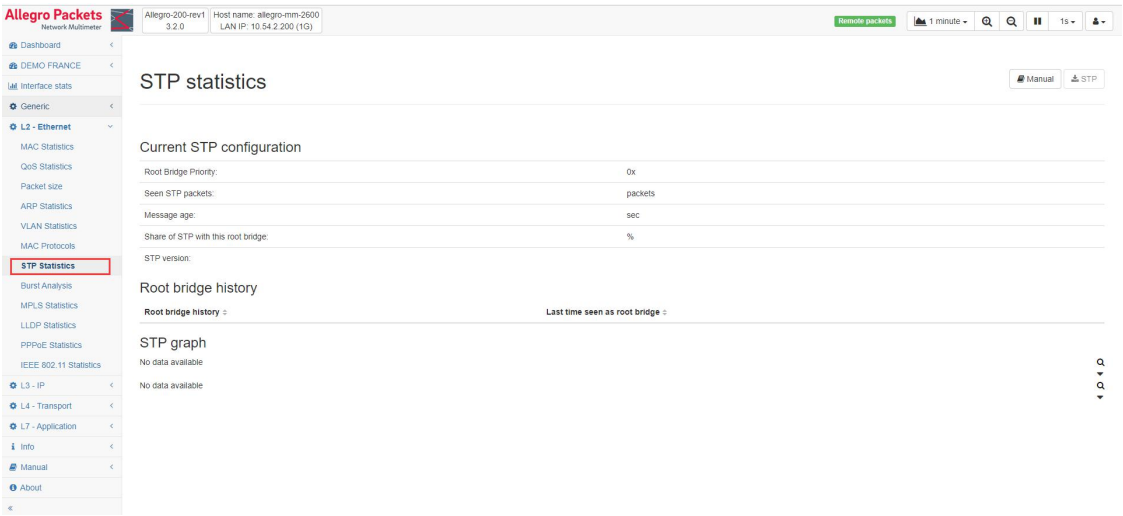
5.6 MAC 协议

MAC 协议模块在网络堆栈的第 2 层上运行。它存储有关所有 MAC 协议的信息。对于每个协议，都会考虑相应的网络流量。



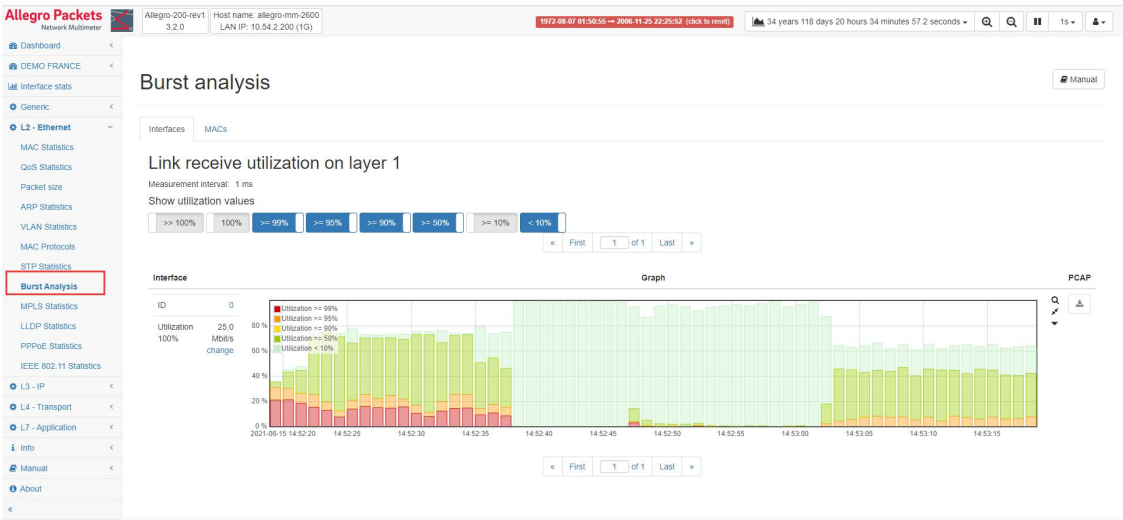
5.7 STP 状态

STP 模块处理 STP 流量并存储所有检测到的根桥的历史记录，包括有关这些的信息。



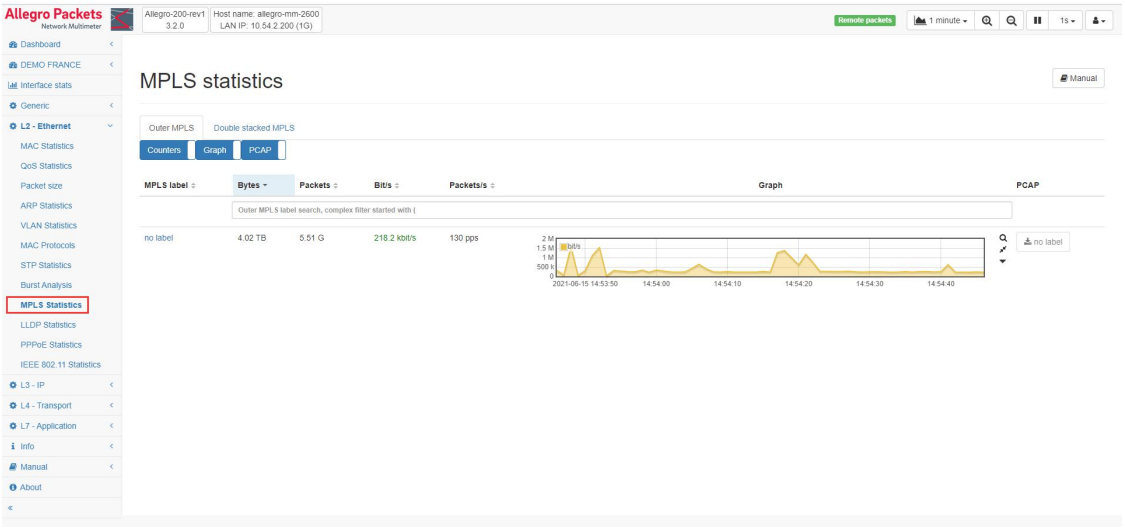
5.8 网络利用率分析

网络利用分析模块测量每个接口或 MAC 地址的吞吐量并显示利用率图。



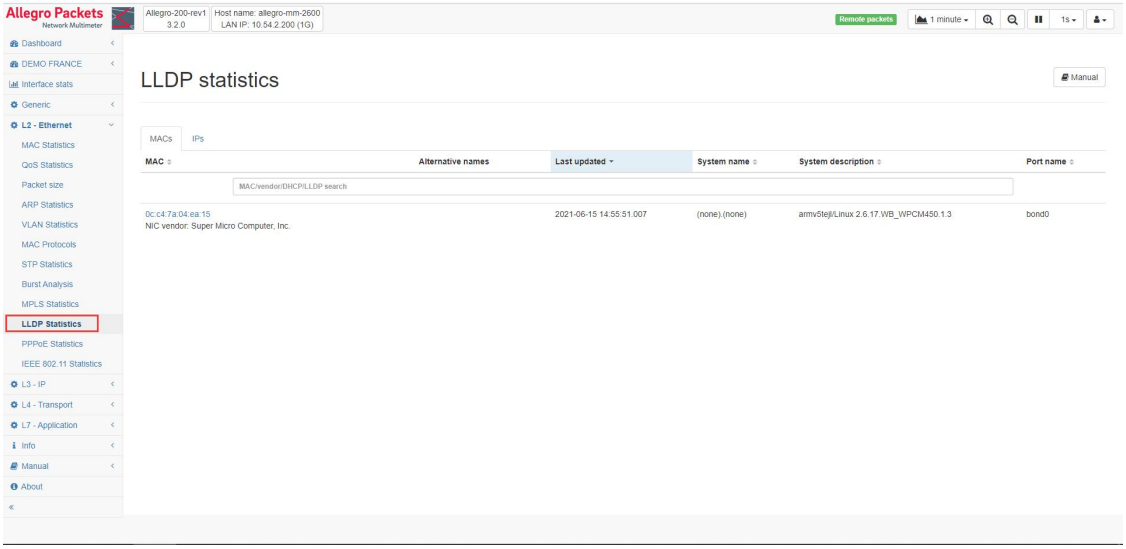
5.9 MPLS 统计

MPLS 模块显示有关所有看到的 MPLS 标签（单标签和双堆叠）的信息。



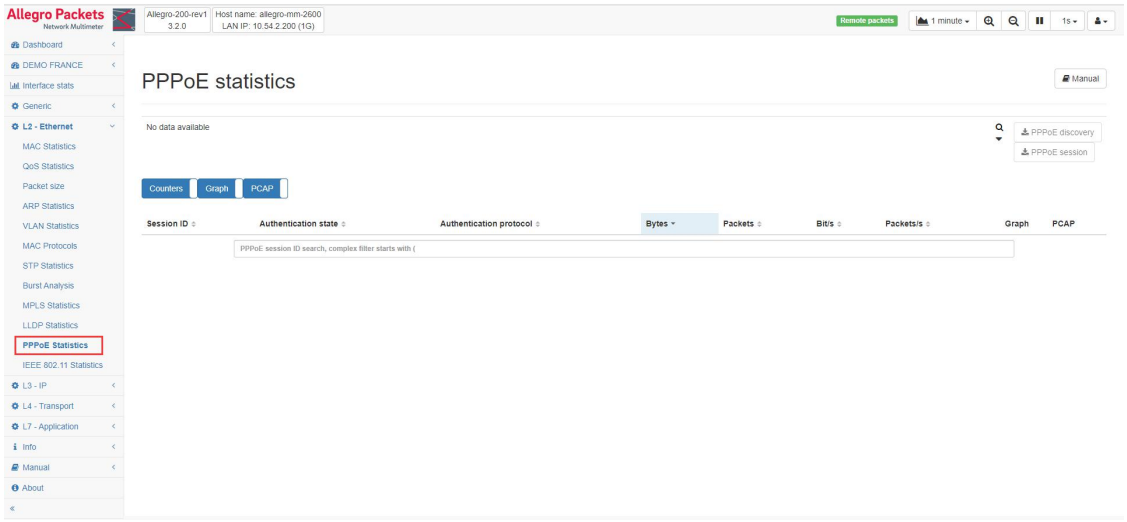
5.10 LLDP 统计

LLDP 模块从 LLDP 消息（链路层发现协议）中提取信息，并将此信息与各自的 MAC 和 IP 地址相关联。



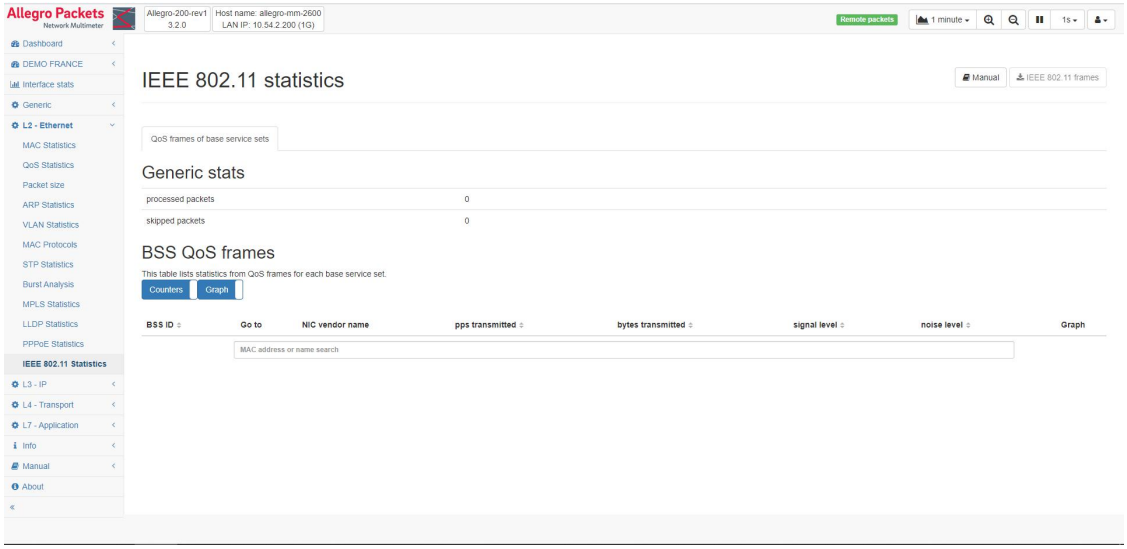
5.11 PPPOE 统计

PPPoE 模块显示某个会话内的所有 PPPoE 会话和流量。



5.12 IEEE 802.11 统计

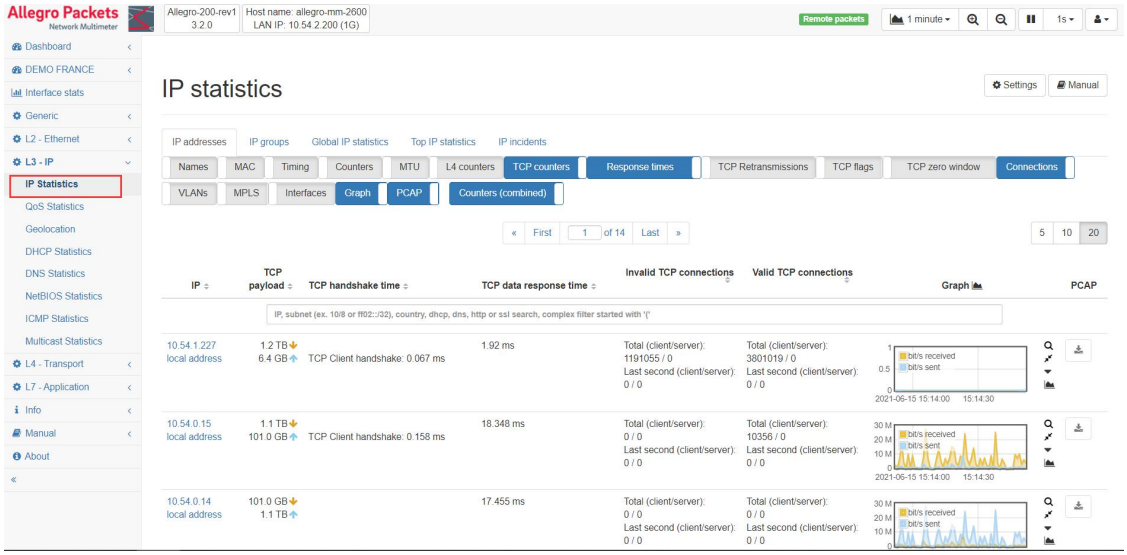
该模块分析封装在特殊数据包中的 IEEE 802.11 帧。在当前版本中，仅处理带有 QoS 数据的 IEEE802.11 数据帧，以显示有关接入点和参与者及其质量的统计信息。跳过所有其他 IEEE802.11 帧。



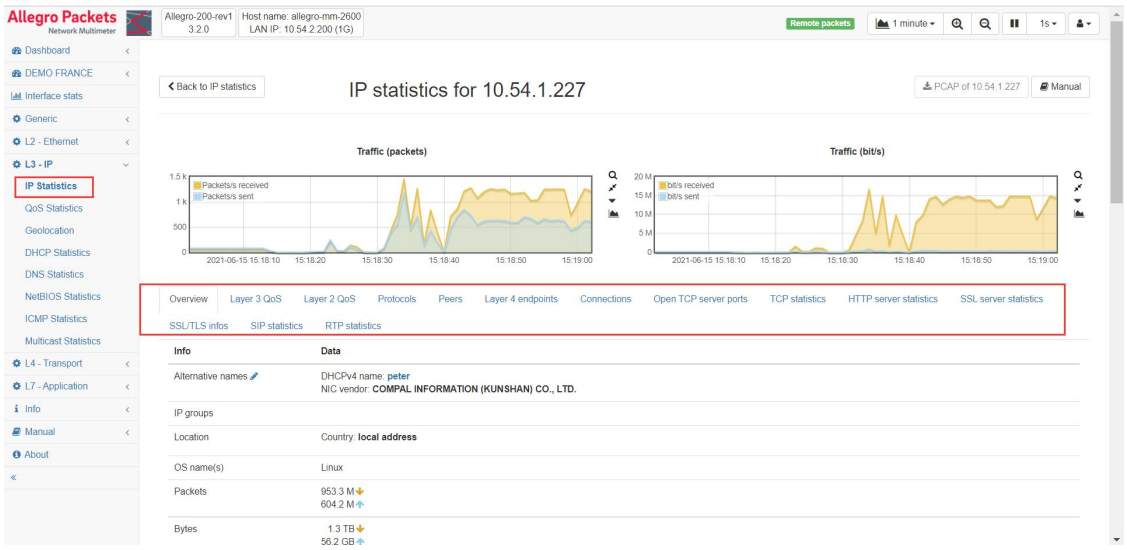
6. 网络层监控

6.1 IP 统计

生成详细的 IP 统计信息，Top IP,TCP 信息，吞吐量，历史图表等等可选，每个 IP 都可以点击进入进行详细分析。

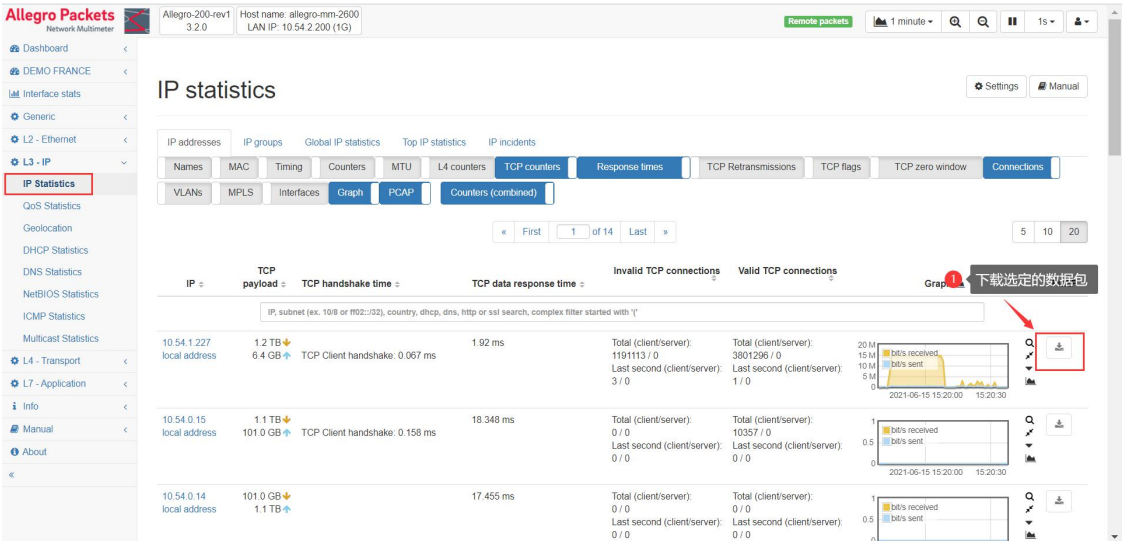


单个 IP 详细分析：

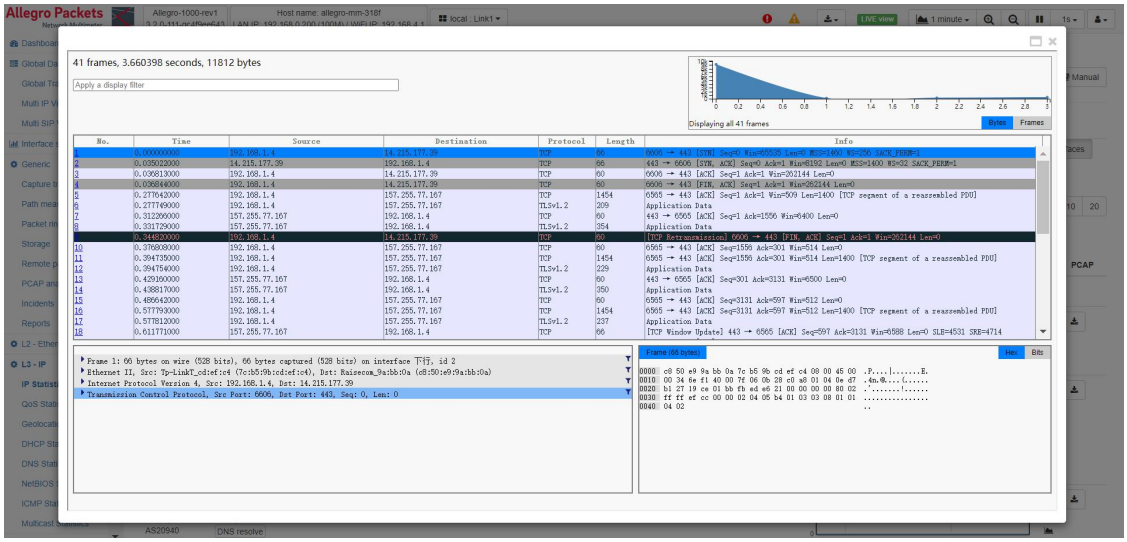


6.2 数据包下载

大部分的页面都有下载数据包的功能，点击下载按钮就能下载选定的流量原始 PCAP 数据到本地，使用 wireshark，Omnipeek 等数据包分析器进行详细分析。

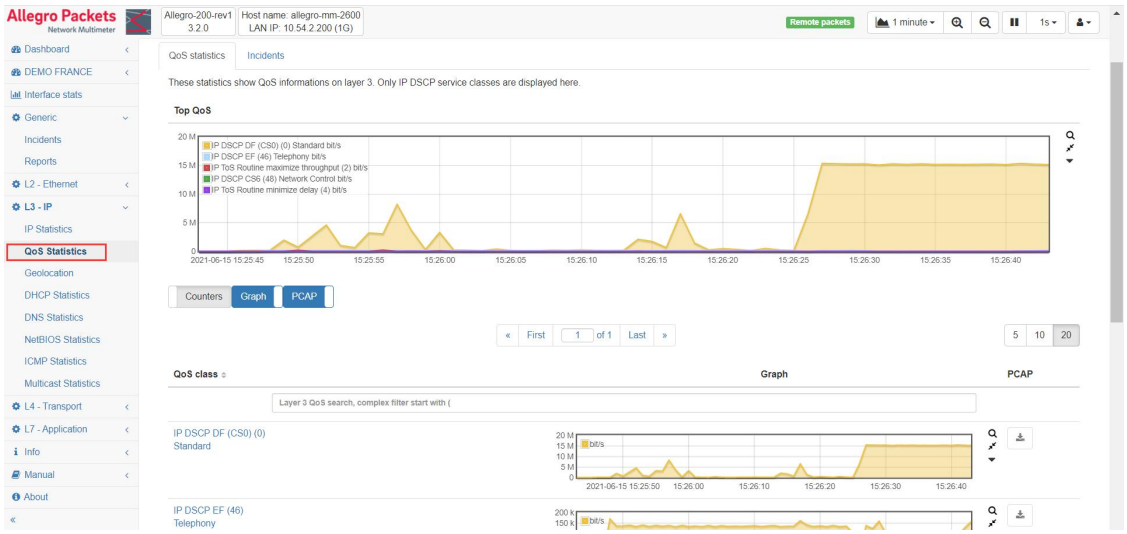


也可以直接使用 Allegro 预安装的 webshark 进行详细分析。



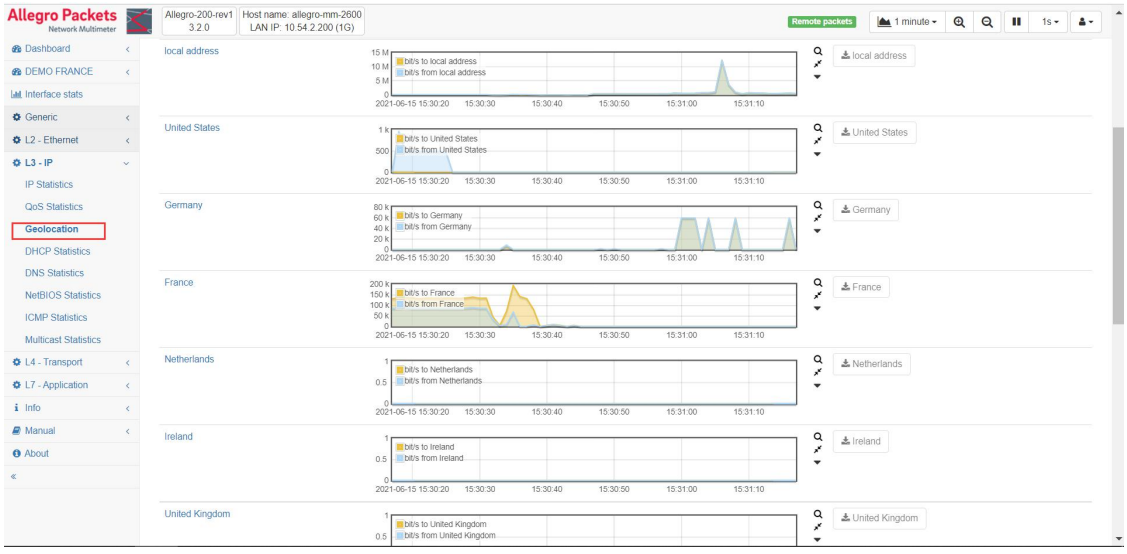
6.3 QoS 状态

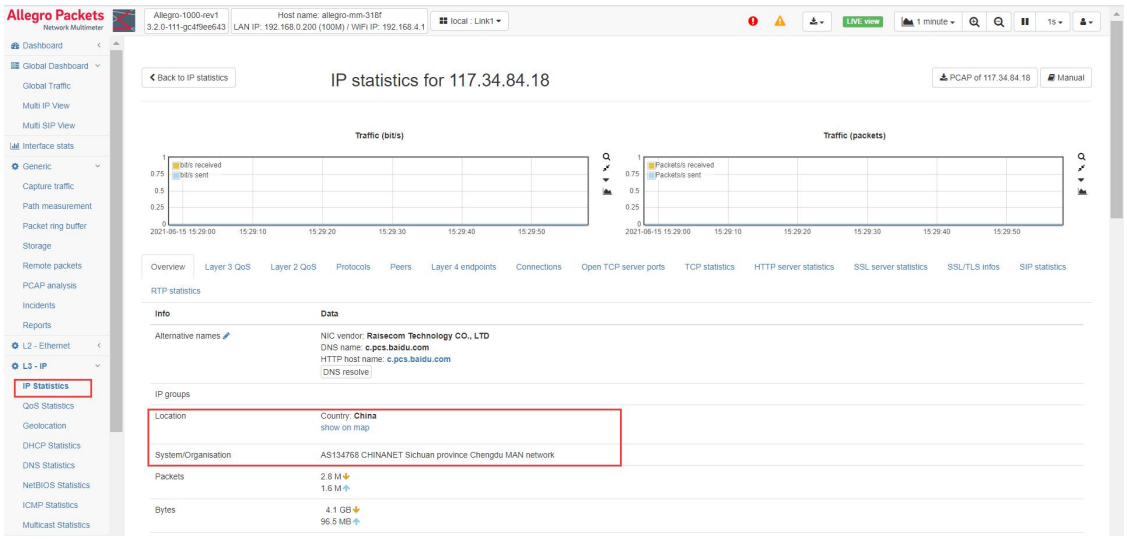
对于第 3 层 IP，显示 DSCP 流量计数器、流量随时间变化的历史图表和该特定 DSCP 值的 PCAP 按钮下载按钮。此外，如果不使用 DSCP，则会显示 RFC791 和 RFC1349 定义的旧式服务类型值。考虑遵循 DSCP 和服务类型兼容性映射。



6.4 地理位置信息统计

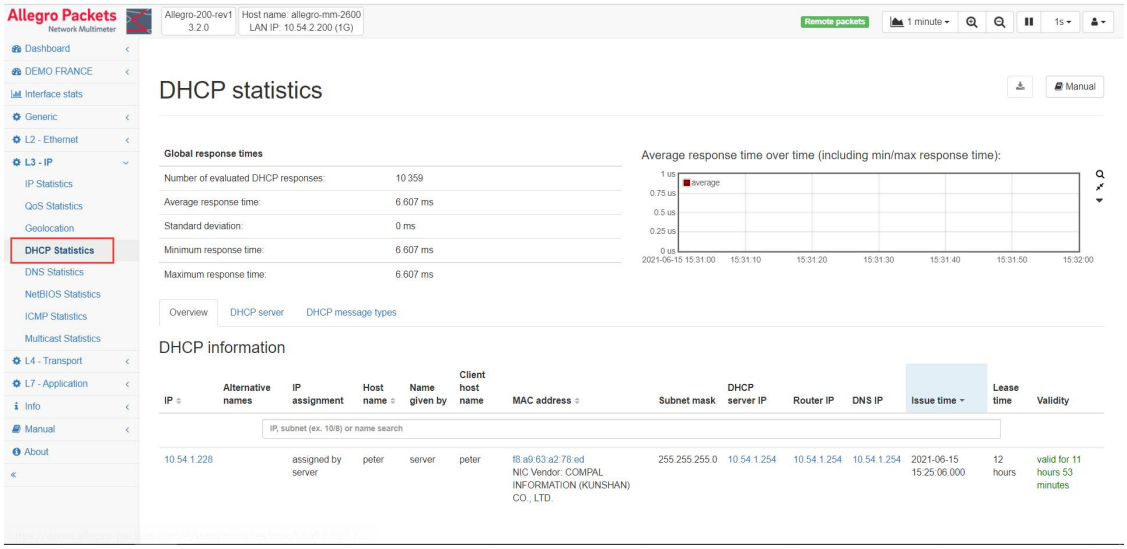
提供国家、城市级精度的 GeoIP 信息。





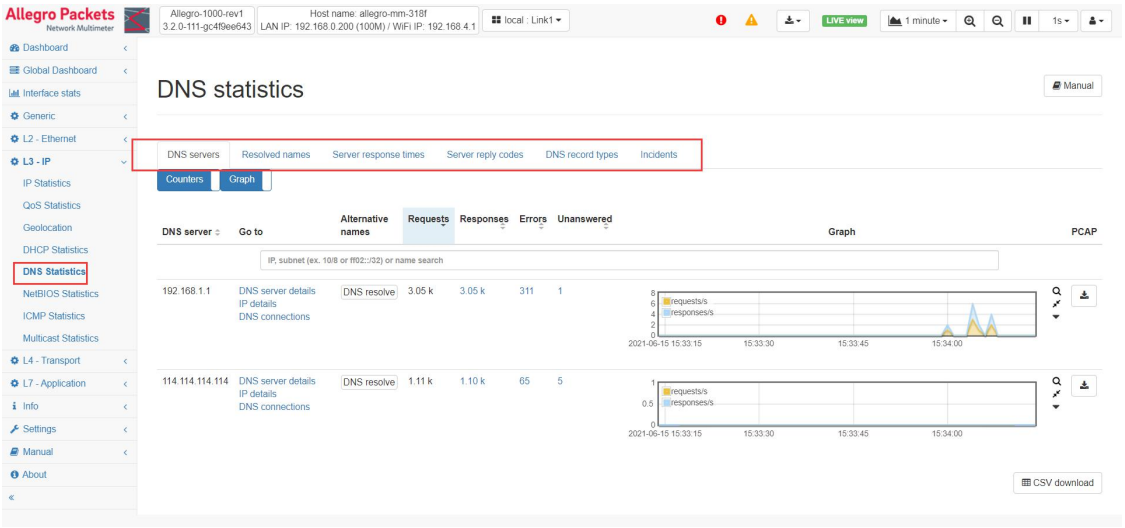
6.5 DHCP 统计

DHCP 模块跟踪网络中动态 IP 分配的请求和应答。这允许将自行宣告的系统名称解析为实际的 IP 地址。此外，该模块还提供了有关在网络中运行 DHCP 服务器的概述，从而可以识别 IP 分配问题。



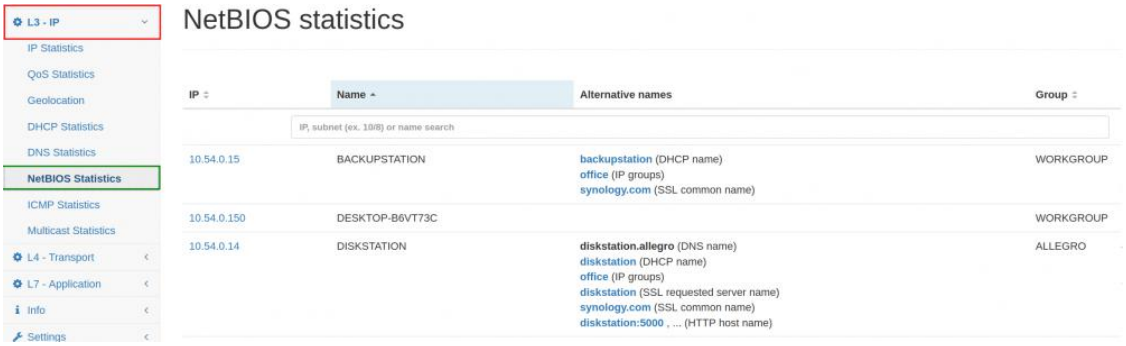
6.6 DNS 统计

DNS 模块跟踪名称查找请求和响应，以便能够在不进行主动查找的情况下显示 IP 地址的名称。DNS 模块为每个域名存储已宣布的最后一个 IP。由于内容交付网络（或其他设置）和虚拟主机中的负载平衡机制，一个名称可能会解析为多个 IP 地址，或者单个 IP 地址使用多个名称。Web 前端将始终显示在网络上看到的最新信息。



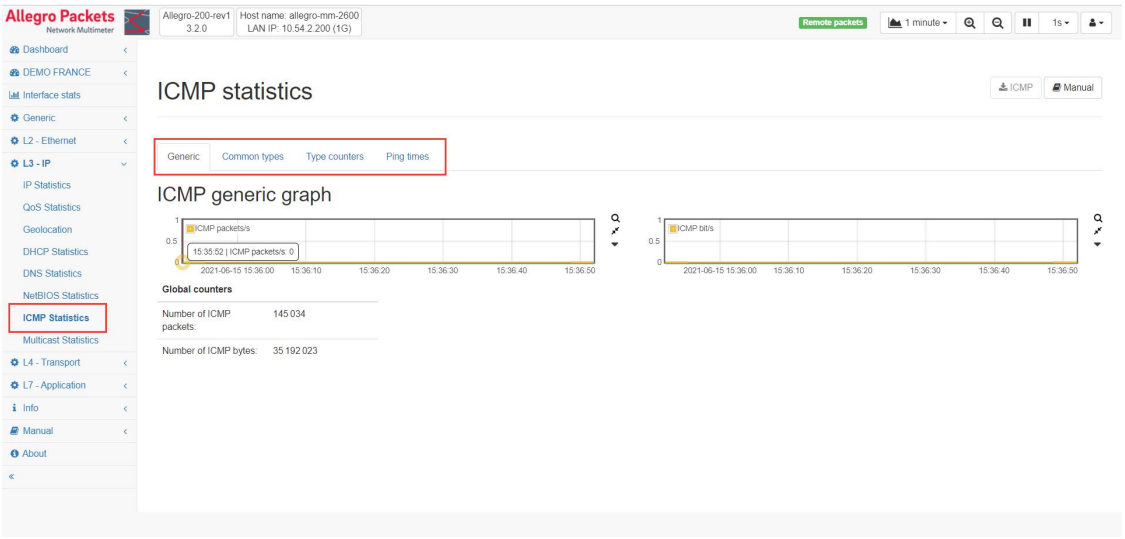
6.7 NetBIOS 统计

NetBIOS 经常在 Window 环境中用于多种用途。此模块跟踪特定的 NetBIOS 数据包以进行名称解析。如果 DNS 或 DHCP 等其他来源错过了此类信息，它可以提示 IP 地址的名称。NetBIOS 的相关协议和同义词是 SMB、Samba、CIFS 或 WINS。



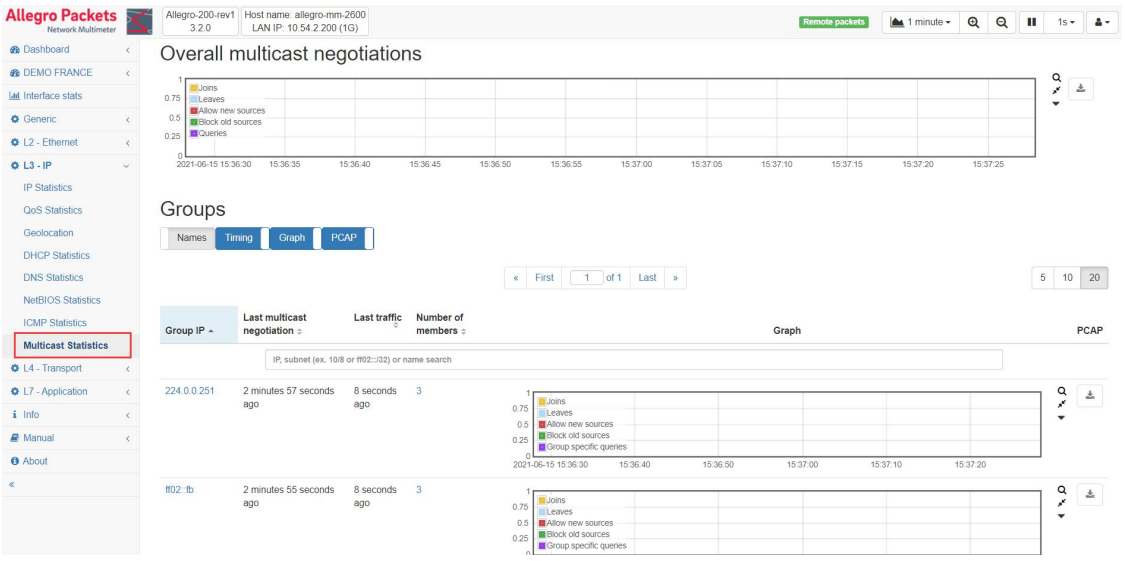
6.8 ICMP 统计

ICMP 模块处理 ICMP 流量。它存储 ICMP 流量并提取有关类型的信息。



6.9 组播统计

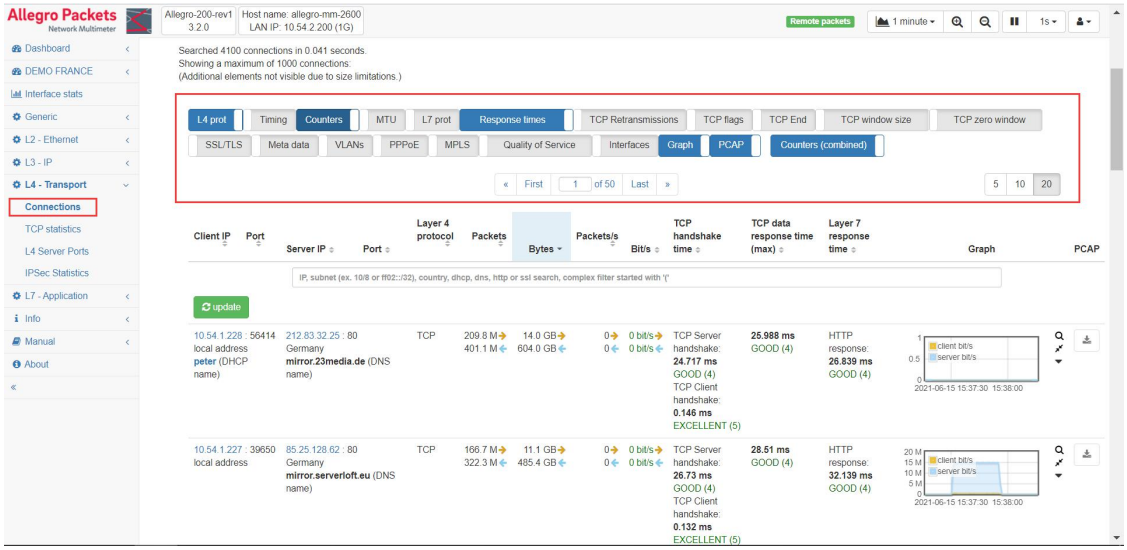
组播模块分析 IGMP 和 MLD 组播管理数据包，并显示有关组播组及其成员的详细信息。支持用于 IPv4 的 IGMPv1、v2、v3 和用于 IPv6 的 ICMPv6 子协议 MLDv1 和 v2。



7. 传输层监控

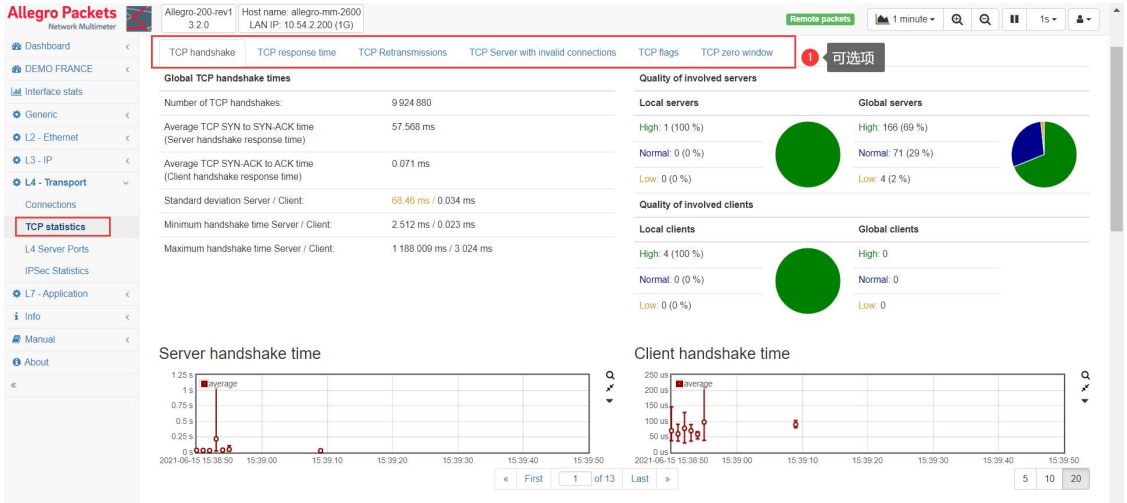
7.1 会话

连接模块显示来自系统内所有 IP 地址的连接。该模块遍历所有 IP 连接列表，并根据活动的排序和过滤参数收集前 1000 个元素。该列表始终最多只包含 1000 个连接，但可以使用过滤器来查看不可见的部分。



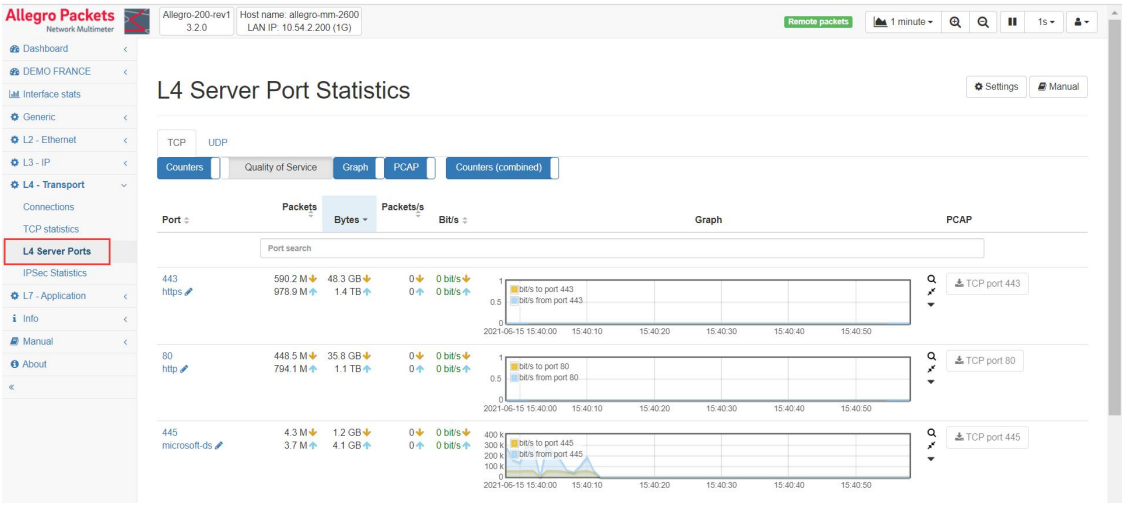
7.2 TCP 状态统计

TCP 模块测量接所有 TCP 数据包，计算往返时间，响应时间，重传，无效连接，零窗口等所有 TCP 参数。



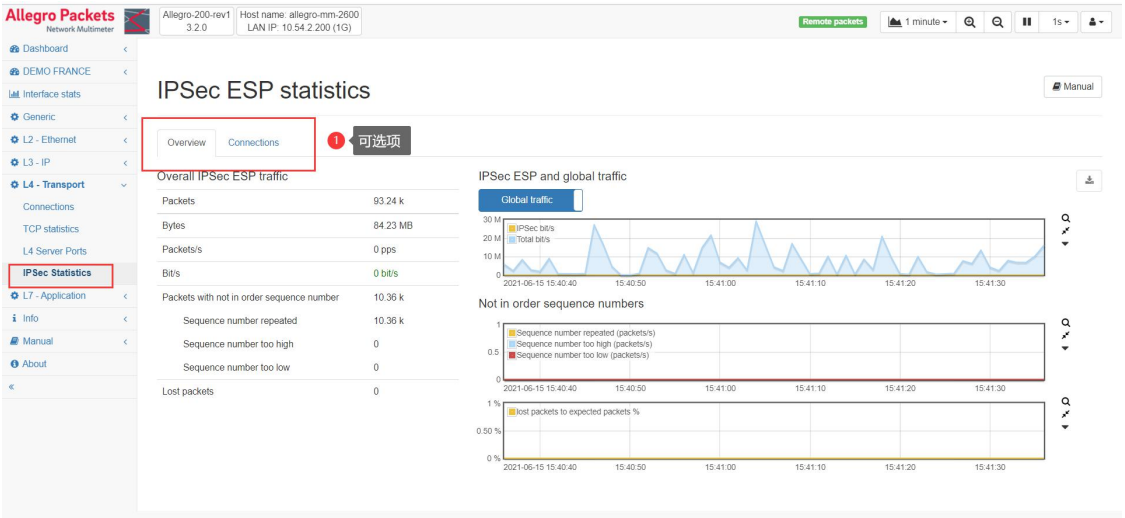
7.3 端口

第 4 层服务器端口统计信息包括网络上每个 TCP 和 UDP 服务器端口的流量计数器。



7.4 IPSec 统计

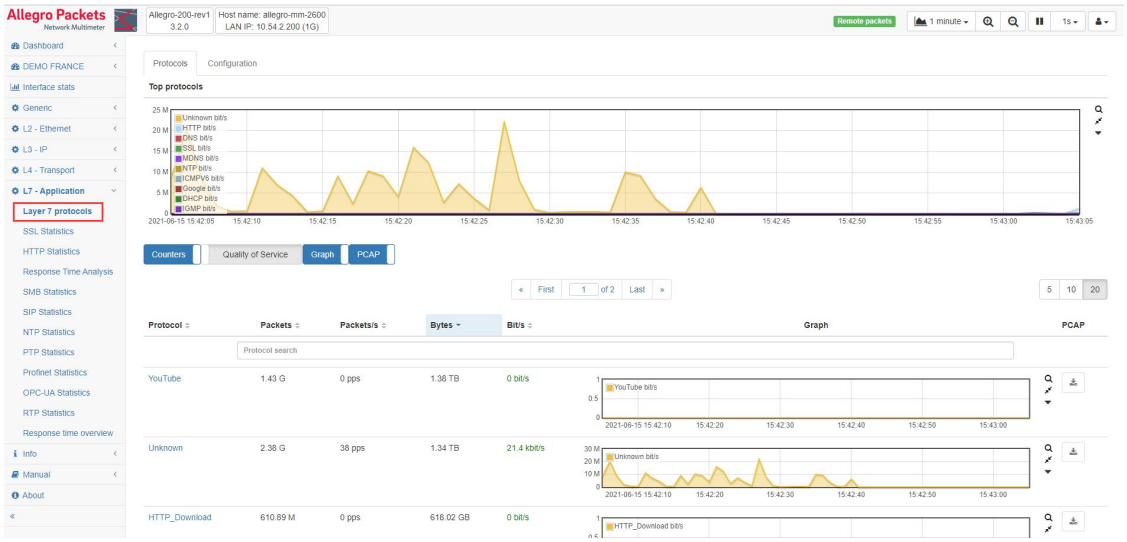
IPSec 模块显示有关 IPSec ESP 流量和序列计数器正确性的信息。



8. 应用层监控

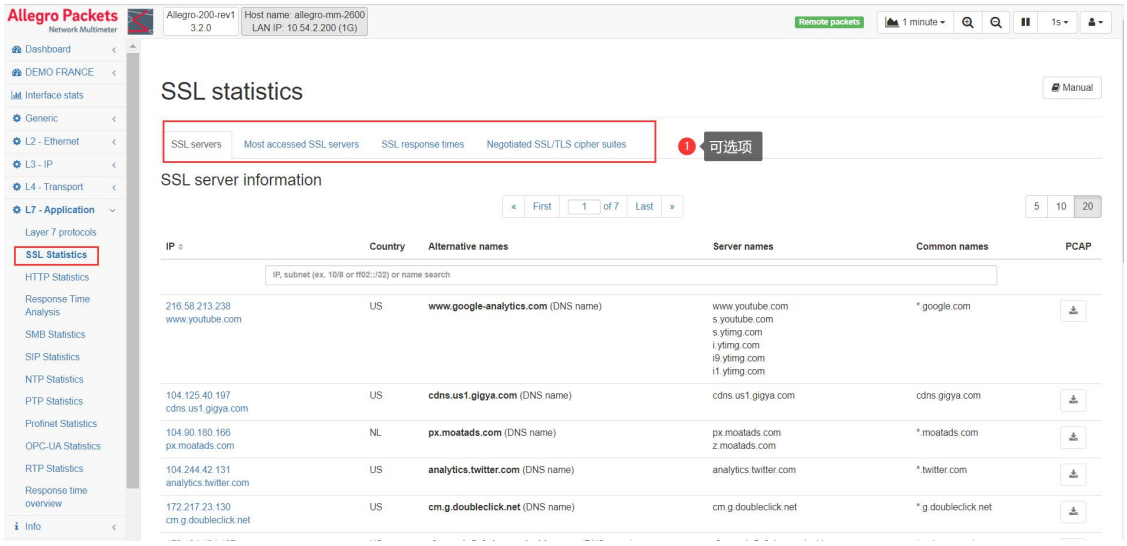
8.1 应用协议统计

L7 模块对第 7 层协议分类引擎提供的结果进行操作。这包括有关每个 IPv4 和 IPv6 地址使用的每个协议的流量的信息。对于每个协议，相应的网络流量都会被计算在内，并且可以使用看到该协议的 IP 地址列表。还可以通过基于 IP 地址或端口配置自定义协议来扩展第 7 层协议列表。



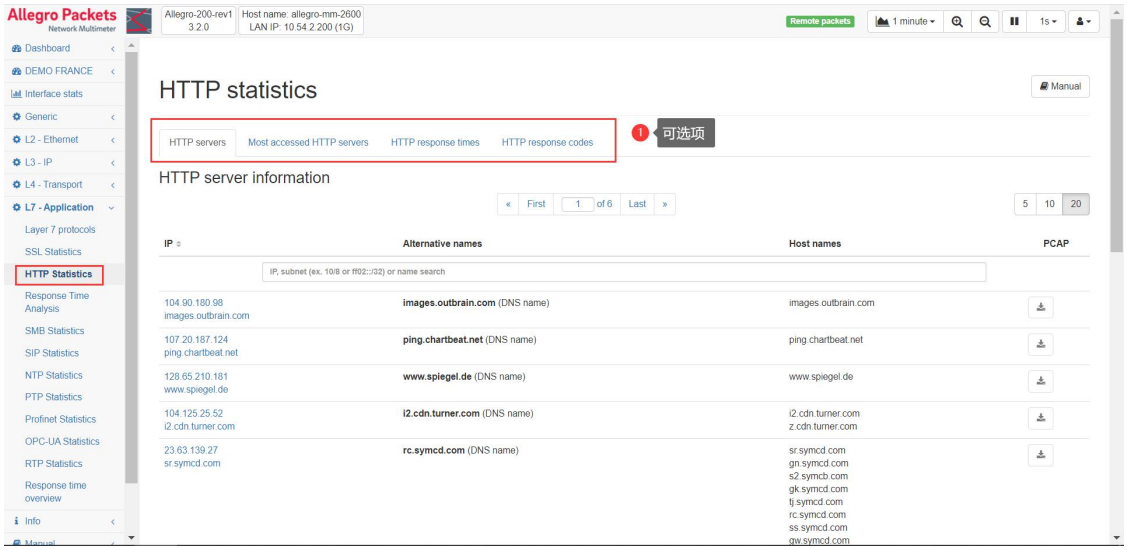
8.2 SSL 统计

SSL 模块处理加密的 SSL/TLS 流量并在内部存储 SSL 服务器的可见名称以供交叉引用，这样即使 IP 没有看到 DNS 名称，也可以对其进行名称查找。由于服务器可能会处理多个加密服务实例，因此对于一个 IP，也可以看到多个名称。SSL 模块存储每个 IP 的所有名称，这有助于查看网络中的哪些服务器处理哪些特定服务。此外，还会测量服务器对初始 SSL 握手和第一次数据传输的响应时间，以量化 SSL 连接的质量。



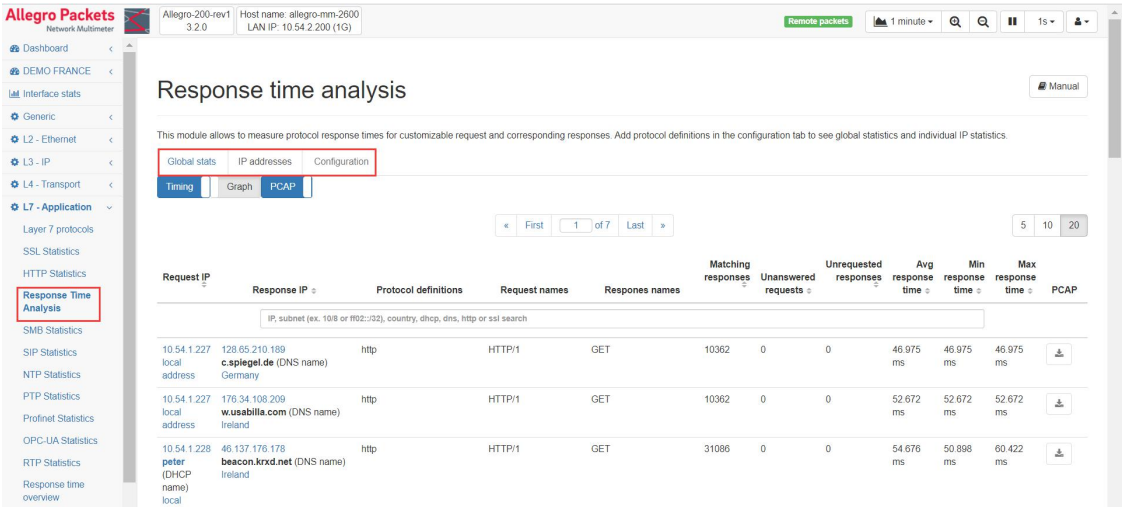
8.3 HTTP 统计

HTTP 模块处理 HTTP 流量并在内部存储 HTTP 请求的请求主机名以供交叉引用，这样即使没有看到 IP 的 DNS 名称，也可以对其进行名称查找。由于一个服务器可能处理多个所谓的虚拟主机，因此一个 IP 也可以看到多个名称。HTTP 模块存储每个 IP 的所有名称，这有助于查看网络中的哪些服务器处理哪些特定服务。



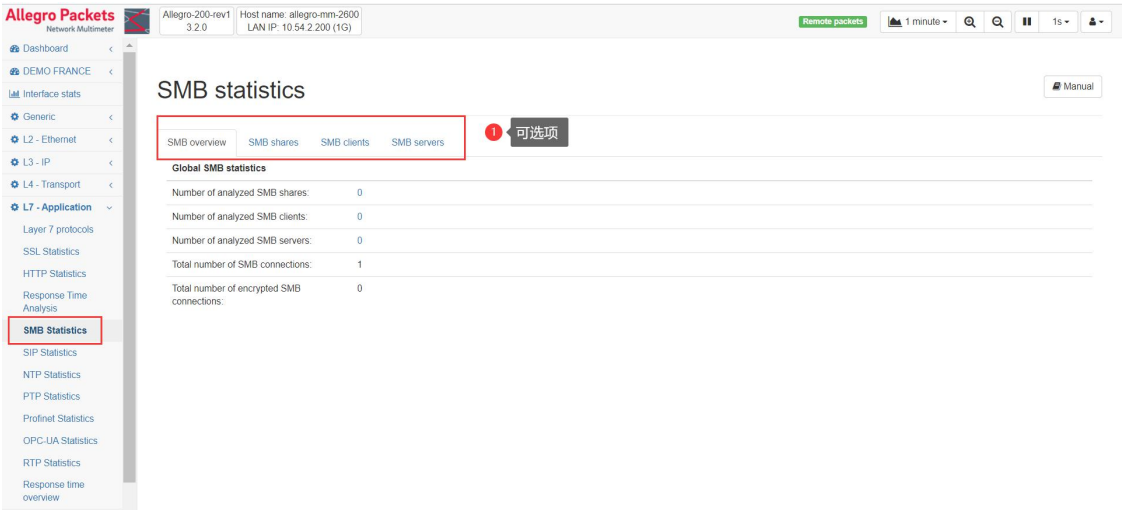
8.4 响应时间分析

响应时间分析允许跟踪几乎任何网络协议中的协议请求和响应。可以添加具有任意数量的不同请求和不同响应的协议定义。系统分析流量并根据配置的模式搜索请求或响应。每当请求发生时，系统都会对事件进行计数并存储数据包的时间，当发生响应时，系统会存储响应时间。



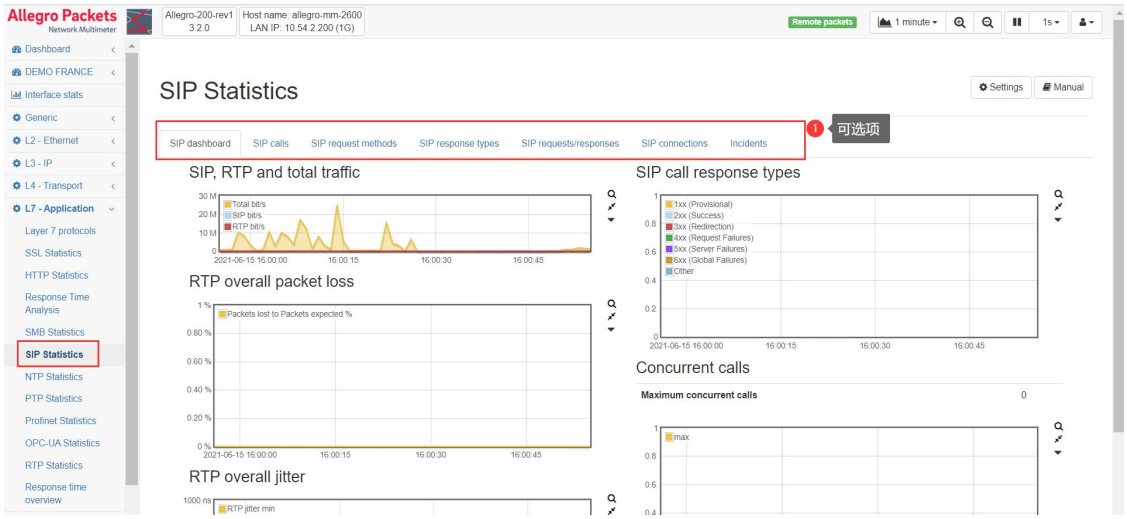
8.5 SMB 统计

SMB 统计信息显示有关 SMB/CIFS 文件传输的信息。它显示未加密 SMB 流量的详细信息和加密 SMB 流量的基本信息。支持旧的 SMB1 和新的 SMB2/3 版本。



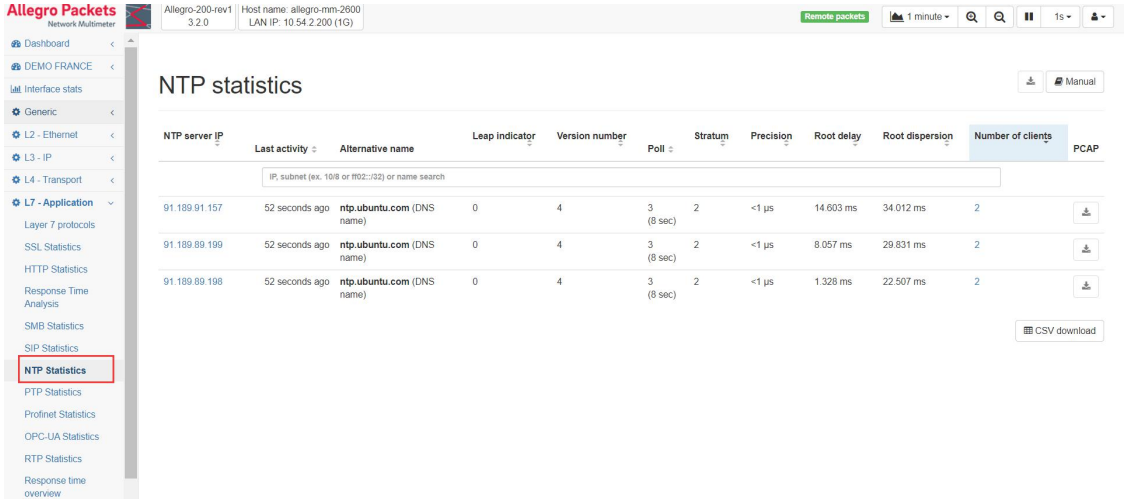
8.6 SIP 统计信息

SIP 统计信息包括所有 SIP 呼叫及其关联的元数据。



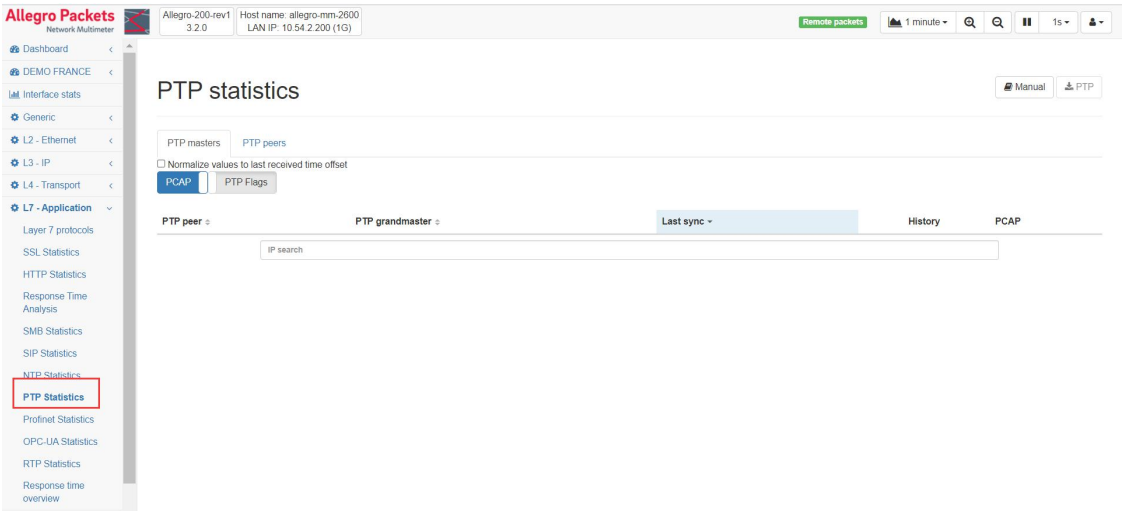
8.7 NTP 统计

NTP 模块处理 NTP 流量。它存储 NTP 服务器，包括它们的客户端，以及更多的 NTP 相关信息。



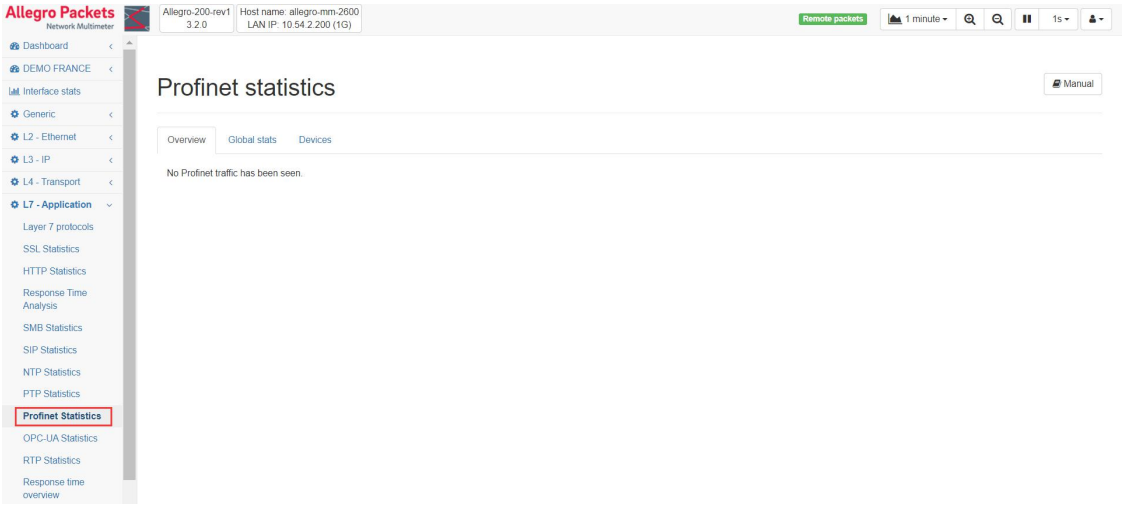
8.8 PTP 统计

PTP 模块处理 PTP 流量并存储 MAC（加上 IP，如果可用）和 PTP 成员的进一步 PTP 元数据。



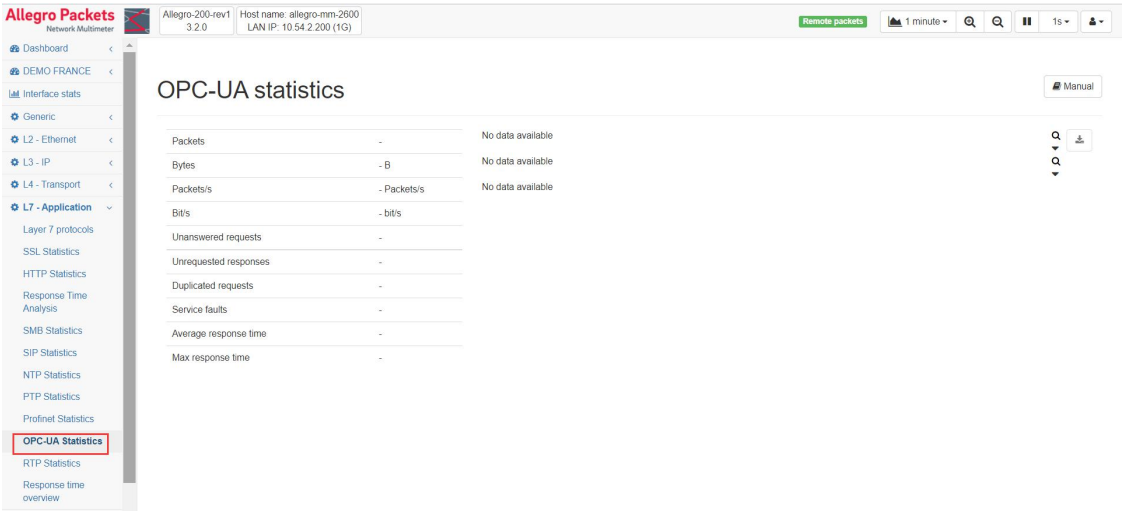
8.9 Profinet 统计

虹科 Allegr 有助于实时和及时进行高度精细的 PROFINET 监控和 PROFINET 故障排除。基于数据包的分析和统计可用于通信关系、最大通话者、带宽消耗、抖动、帧、PROFINET 错误和警报（PN-RT、PN-RTA 和 PNIO-CM）。



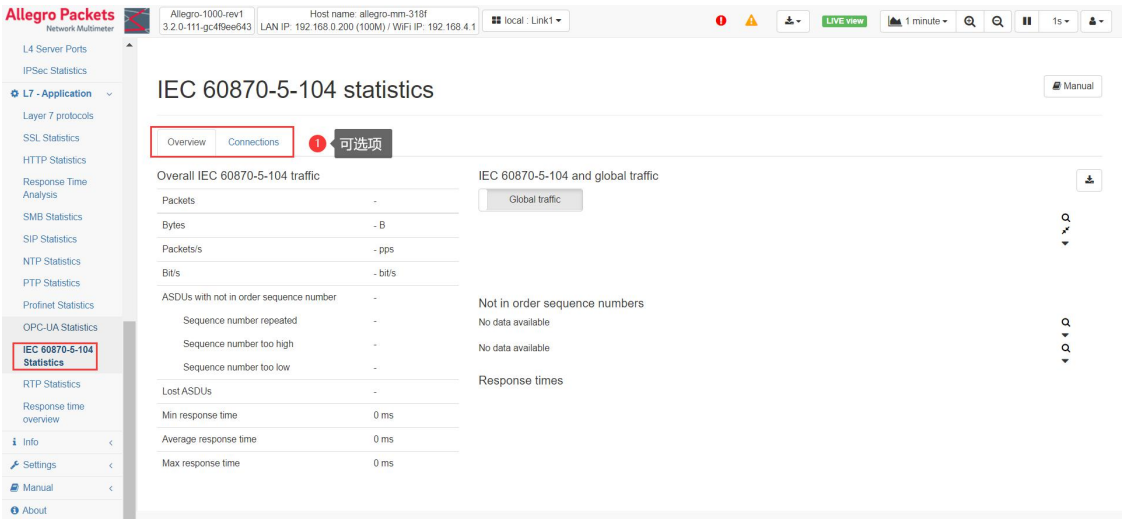
8.10 OPC UA 统计

OPC-UA 模块在第 7 层显示有关 OPC-UA 二进制协议流量的信息，并执行相关请求和响应的响应时间测量。PCAP 按钮允许捕获 OPC-UA 二进制协议流量。统计表显示了所有 OPC-UA 二进制协议包的流量计数器。流量图显示了未加密和加密的流量。



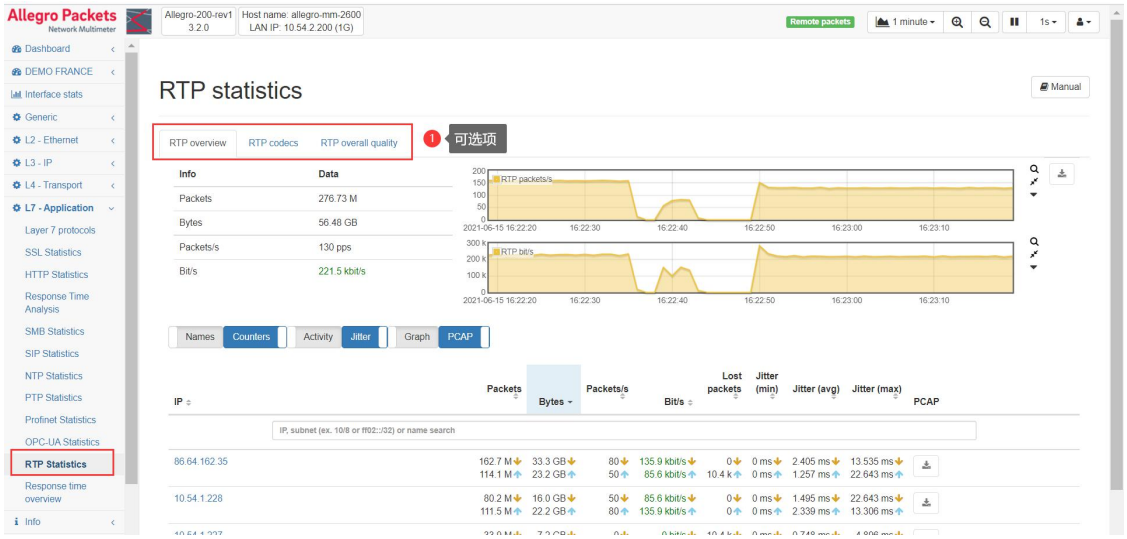
8.11 IEC 60870-5-104 统计

IEC 60870-5-104 模块显示有关 IEC 60870-5-104 流量、序列计数器正确性和响应时间的信息。



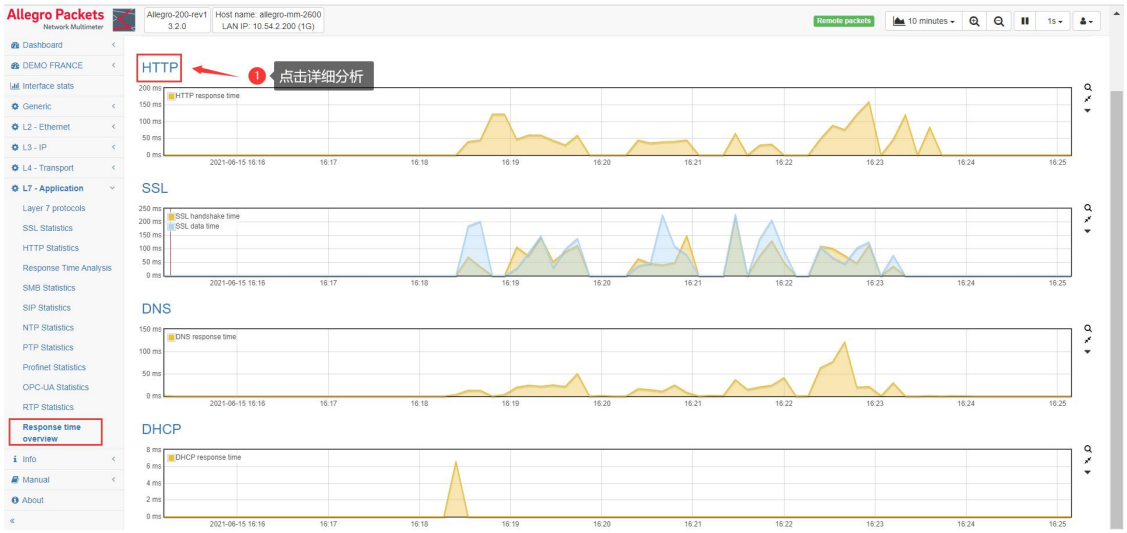
8.12 RTP 统计

RTP 统计数据显示了所有 RTP 流量的完整列表和所用编解码器的分布。



8.13 响应时间概览

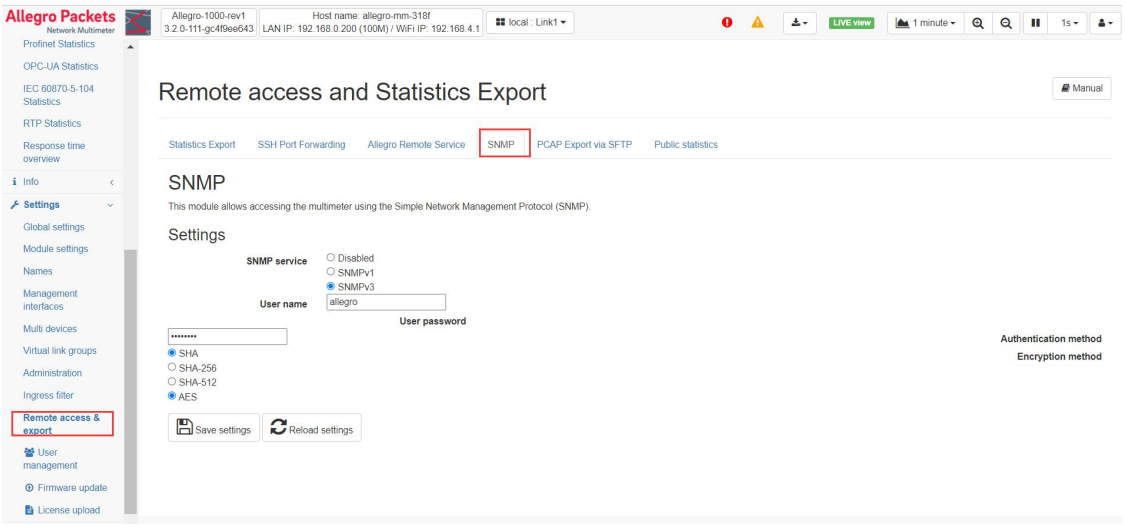
提供详细 HTTP，SSL，DNS，DHCP 响应时间概述。



9. 其他功能

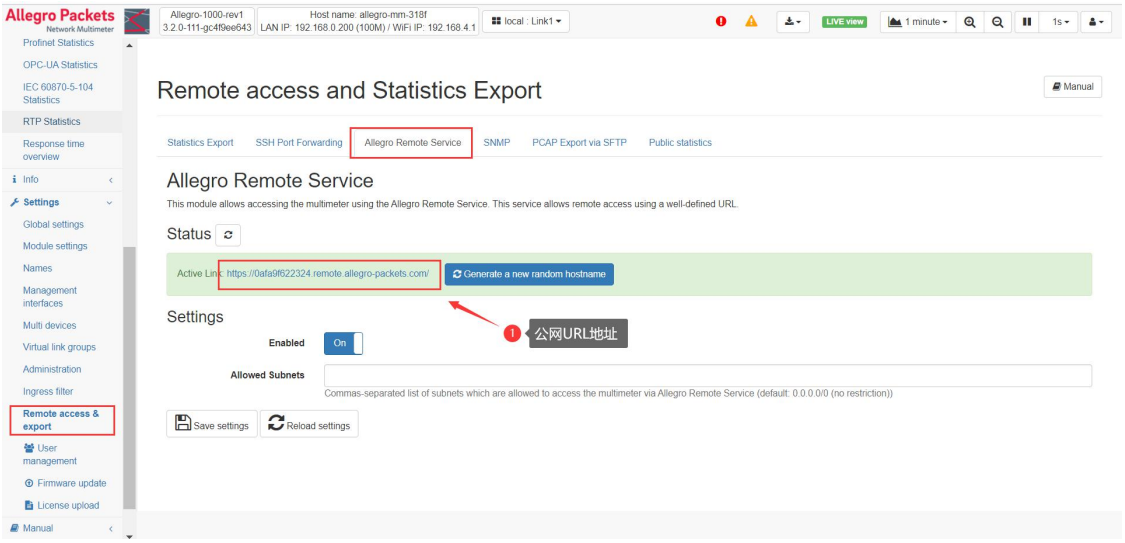
9.1 SNMP 管理

提供 SNMP 管理功能，支持 SNMP v1,v3



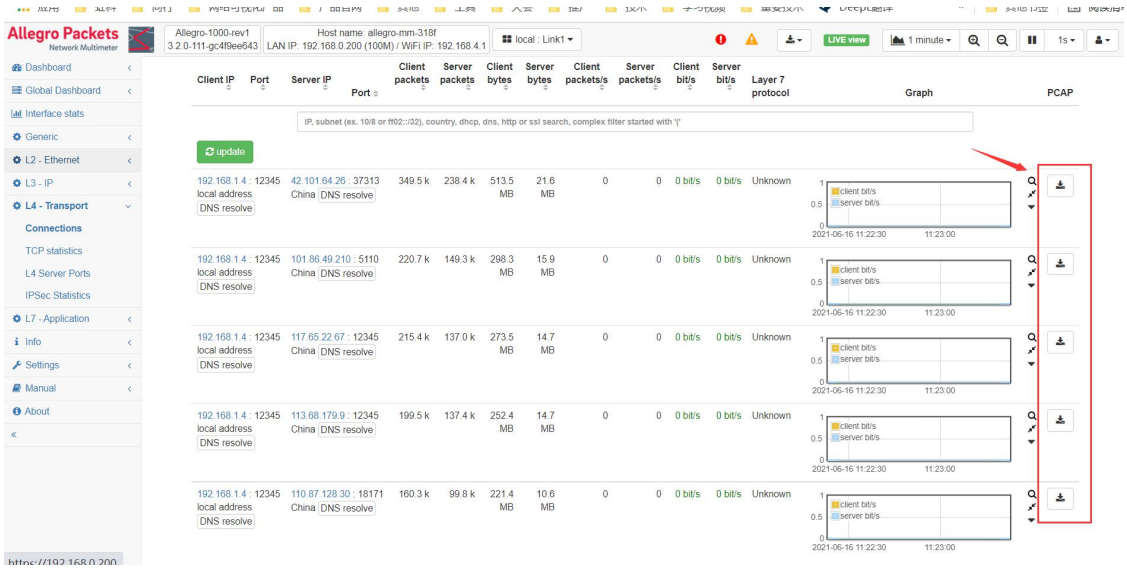
9.2 远程访问

启动远程访问服务，生成远程访问 URL，可跨公网访问 Allegro。



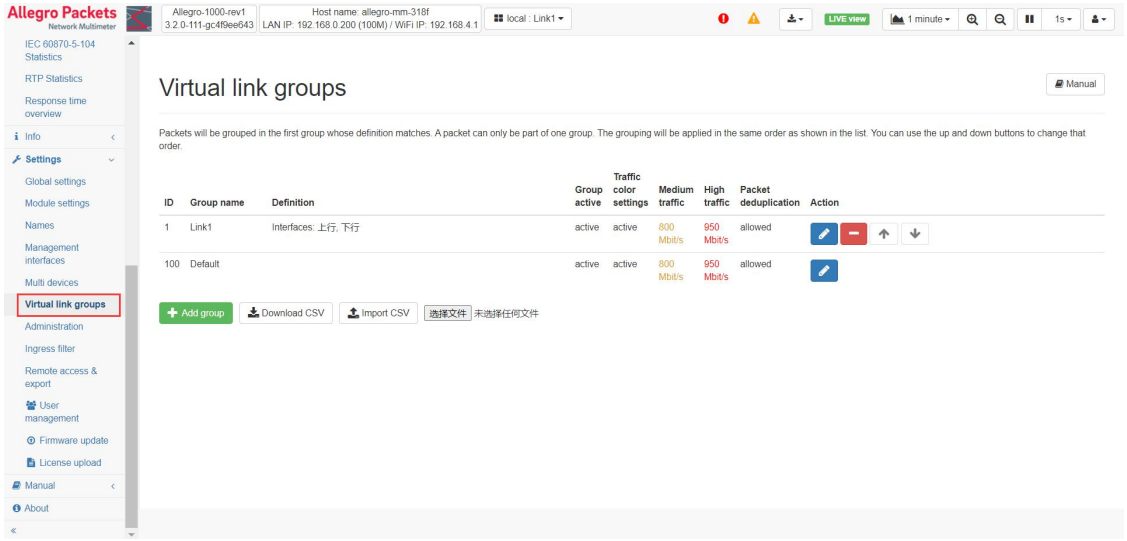
9.3 历史流量 PCAP 下载

Allegro 提供了随时随地下载历史 PCAP 数据包的功能，对于存储在环形缓冲区中的数据包，你可以轻松提取你感兴趣的流量，**PCAP 下载功能几乎在任意流量分析界面可用**。



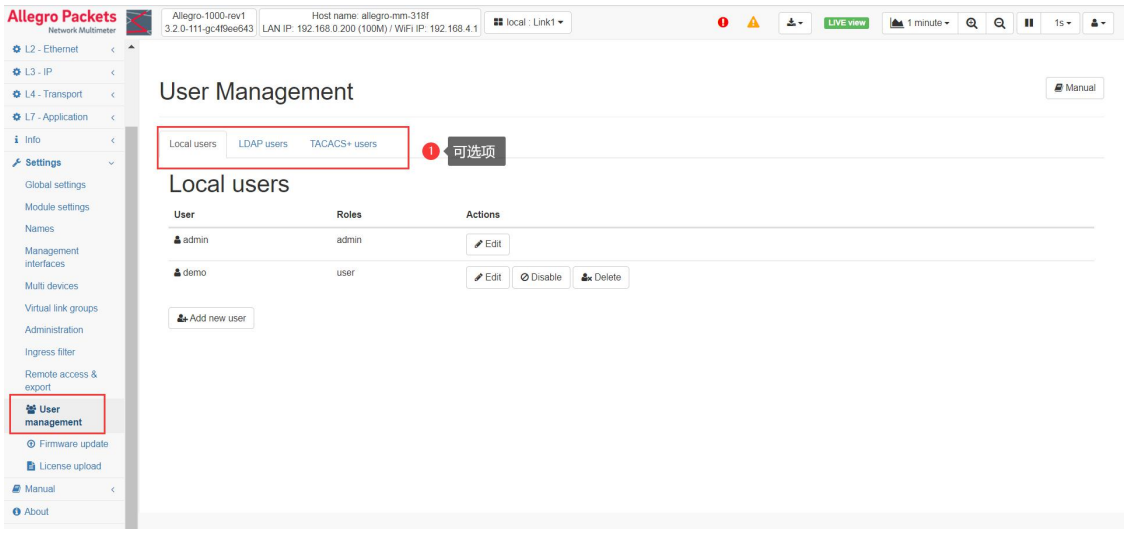
9.4 自定义虚拟链路

可根据接口，VLAN，MPLS，ERSPAN ID 等划分虚拟链路，并在全局流量统计图表中查看各个虚拟链路的流量统计信息。



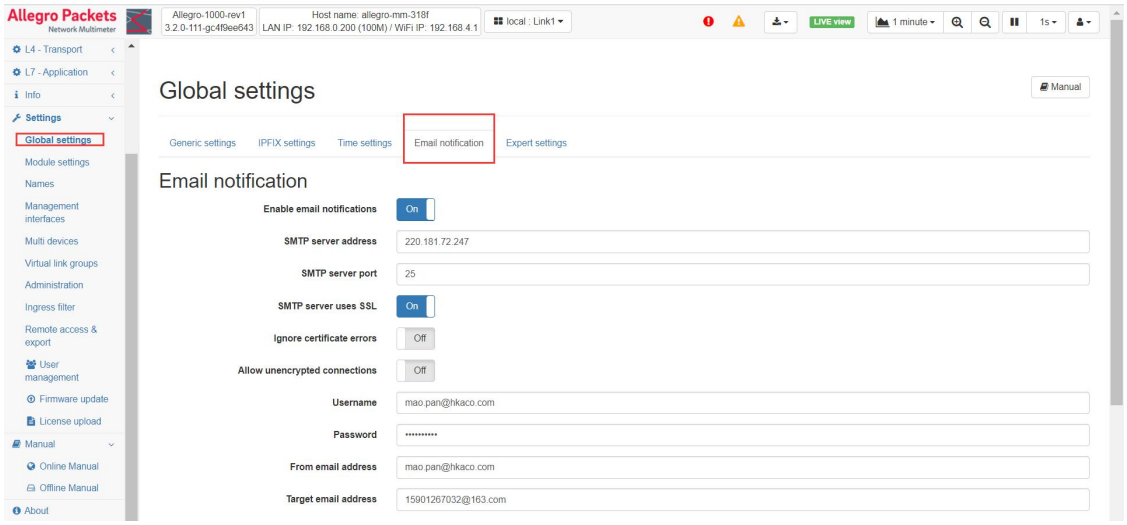
9.5 多用户管理

可自定义具有不同权限的多个用户。



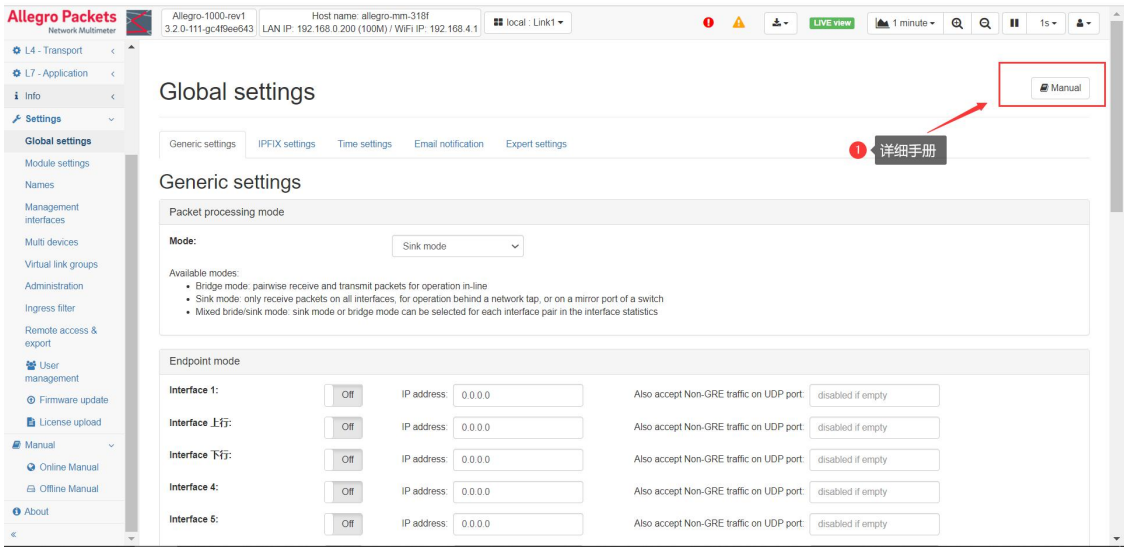
9.6 邮件警告

启用邮件警告功能，系统和自定义警报信息将通过邮件发送到管理员。



9.7 便携手册

任意界面点击右上角 Manual 将跳转到页面的对应详细手册。



10. 关于我们

www.hkaco.com 广州| 深圳| 武汉| 成都| 上海| 西安| 北京|台湾|香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233