虹科 Allegro 一体化网络监控方案

目录

1、简介

虹科 Allegro 网络万用表是用于网络分析的诊断工具和故障排除工具。目前已被世界各地的网络管理员部署，以实时分析网络流量，无论是当前事件还是过去的事件。它能提供高粒度和详细的分析。因此，可以快速识别网络问题、性能瓶颈和数据包丢失。。

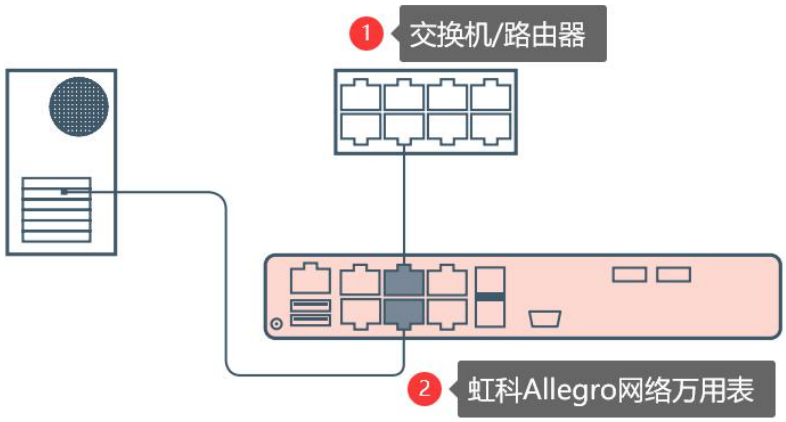
Allegro 网络万用表使用高性能、强大的软件算法来分析负载峰值和干扰。同时，它们作为强大的网络监测工具，确保高网络质量。

Allegro 网络万用表的超便携型号体积小、重量轻，不需要配置。对于我们所有的设备，分析数据可以通过我们的 Web 界面在浏览器中访问。只需点击几下，就能检测到网络问题。可以随时下载 PCAP 文件，以便进一步分析。

2、安装部署

2.1、内联部署

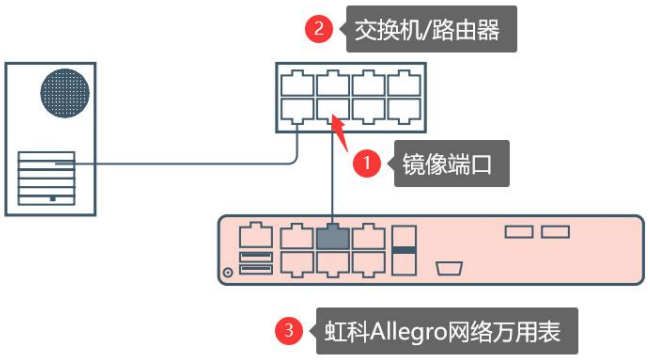
桥接模式下，每一对接口建立一个二层网桥（引入 50us 延迟），将所有进入的流量发送到相对应的接口。每一对垂直的接口构成一个桥接。内联模式可以添加 bypass 功能，当 Allegro 设备断电，两端网络任然能正常通信。



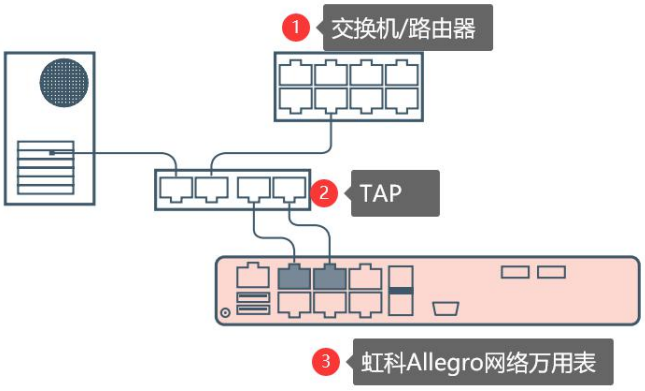
2.2、SPAN/TAP

sink 模式下接收到的数据包将被处理，但不会被转发。将两个 TAP 端口连接到设备上。或者，将交换机或路由器的镜像端口连接到任意一个网络万用表的网络接口。

连接镜像端口（SPAN）：



连接 TAP：



3、网络分析功能

主要功能	详细内容
全局视图	Top 用户 质量分析 三重播放（Triple play） 自定义仪表盘 回溯分析
全局流量统计信息	自定义虚拟链路 全局流量统计
常用功能	流量捕获 路径测量 全流量存储 离线数据包分析 事件告警 报告生成
数据链路层监控	MAC 统计 QoS 统计 数据包大小统计 ARP 统计 VLAN 统计 MAC 协议 STP 状态 网络利用率分析 MPLS 统计 LLDP 统计 PPPOE 统计 IEEE802.11 统计
网络层监控	IP 统计 数据包下载 QoS 状态 地理位置信息统计 DHCP 统计 DNS 统计 NetBIOS 统计 ICMP 统计 组播统计
传输层监控	会话 TCP 状态统计

主要功能	详细内容
	端口 IPSec 统计
应用层监控	应用协议统计 SSL 统计 HTTP 统计 响应时间分析 SMB 统计 SIP 统计 NTP 统计 PTP 统计 Profinet 统计 OPC UA 统计 IEC 60870-5-104 统计 RTP 统计 响应时间概览
其他功能	SNMP 管理 远程访问 历史流量 PCAP 下载 自定义虚拟链路 多用户管理 邮件警告

4、选型

https://hongwangle.com/allegro/overview-appliances/

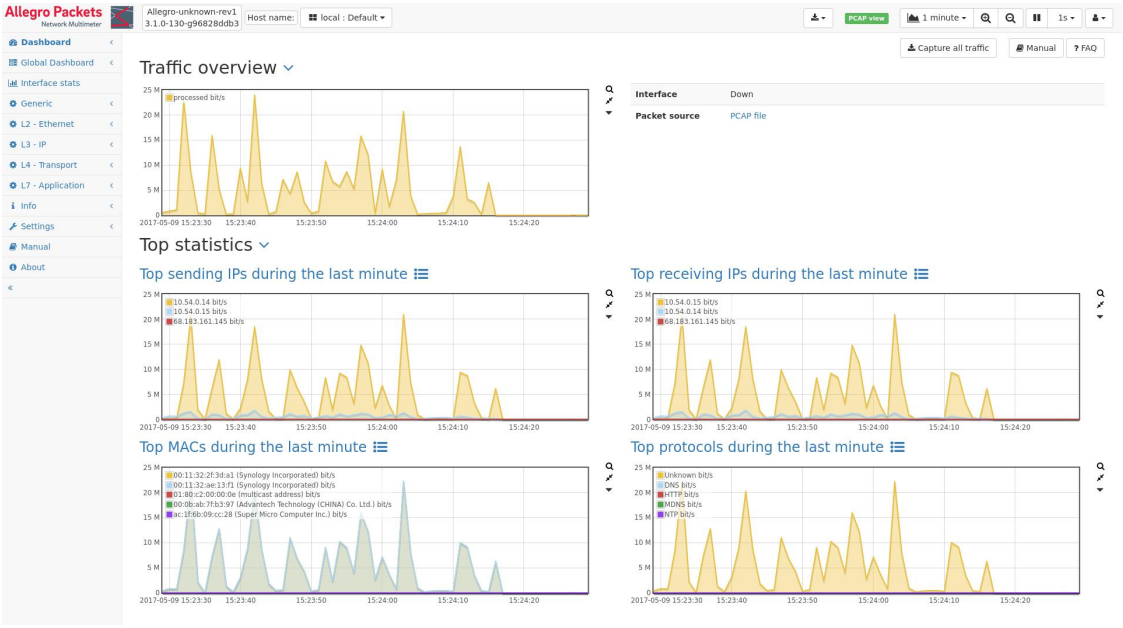
5、分析网络负载用例

5.1、问题

如何使用虹科 Allegro 网络万用表快速轻松地检查网络负载？让我们举一个实际的例子：上午 9 点到 10 点之间，许多个用户抱怨他们的网络连接有时很慢。

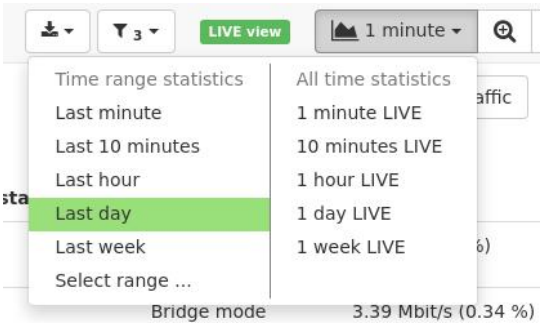
5.2、仪表盘

首先，我们从仪表板中的概述开始。通过浏览器打开网络界面。



5.3、选择时间间隔

接下来在右上角选择一个时间视图，选择一个比要检查的间隔更长的时间范围：

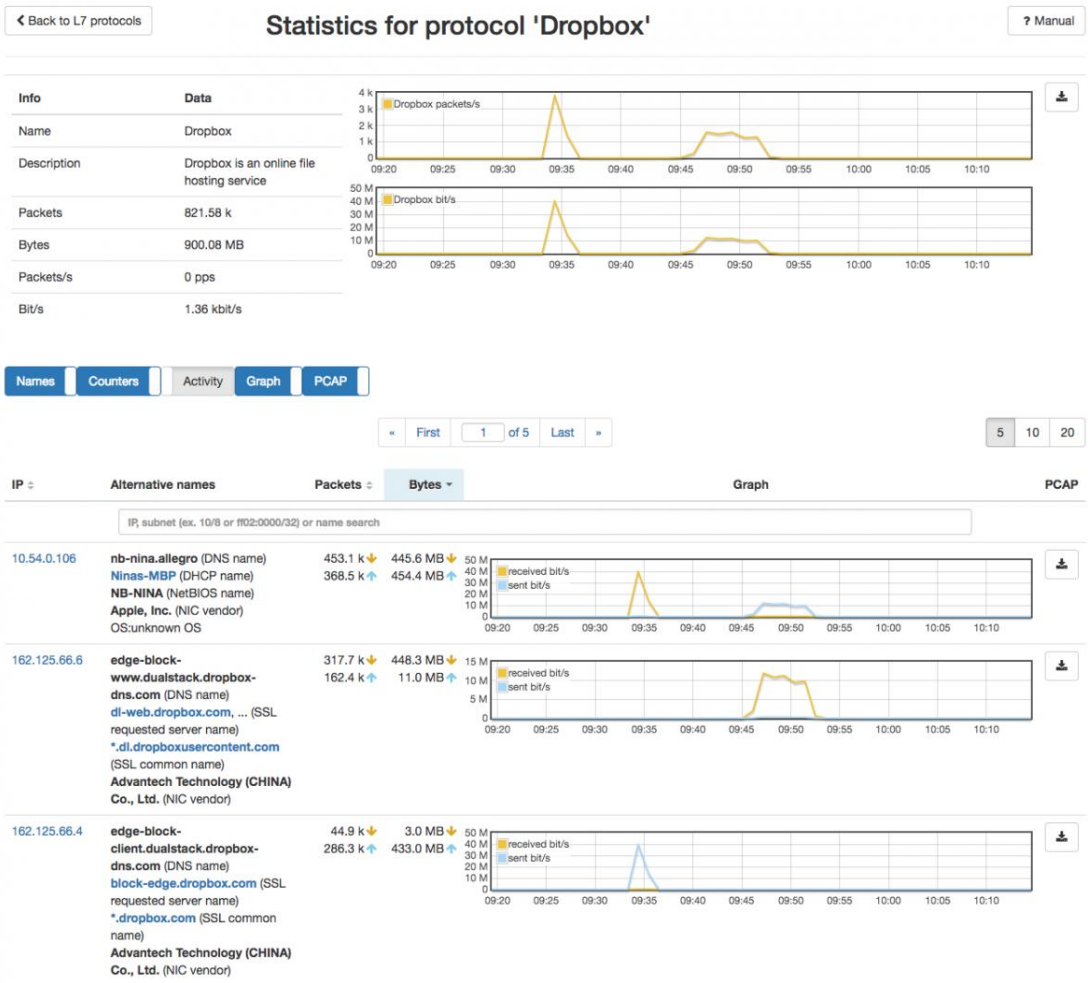


在这种情况下，为了寻找今天早上的事件，选择了最新一天的视图。现在通过使用鼠标选择（单击“拖动”）以下部分来选择用户报告问题的时间段：

Allegro 的内部数据库现在在选定的时间间隔内工作，因此您可以调查存在哪些问题。以下几点很容易在仪表板上使用：

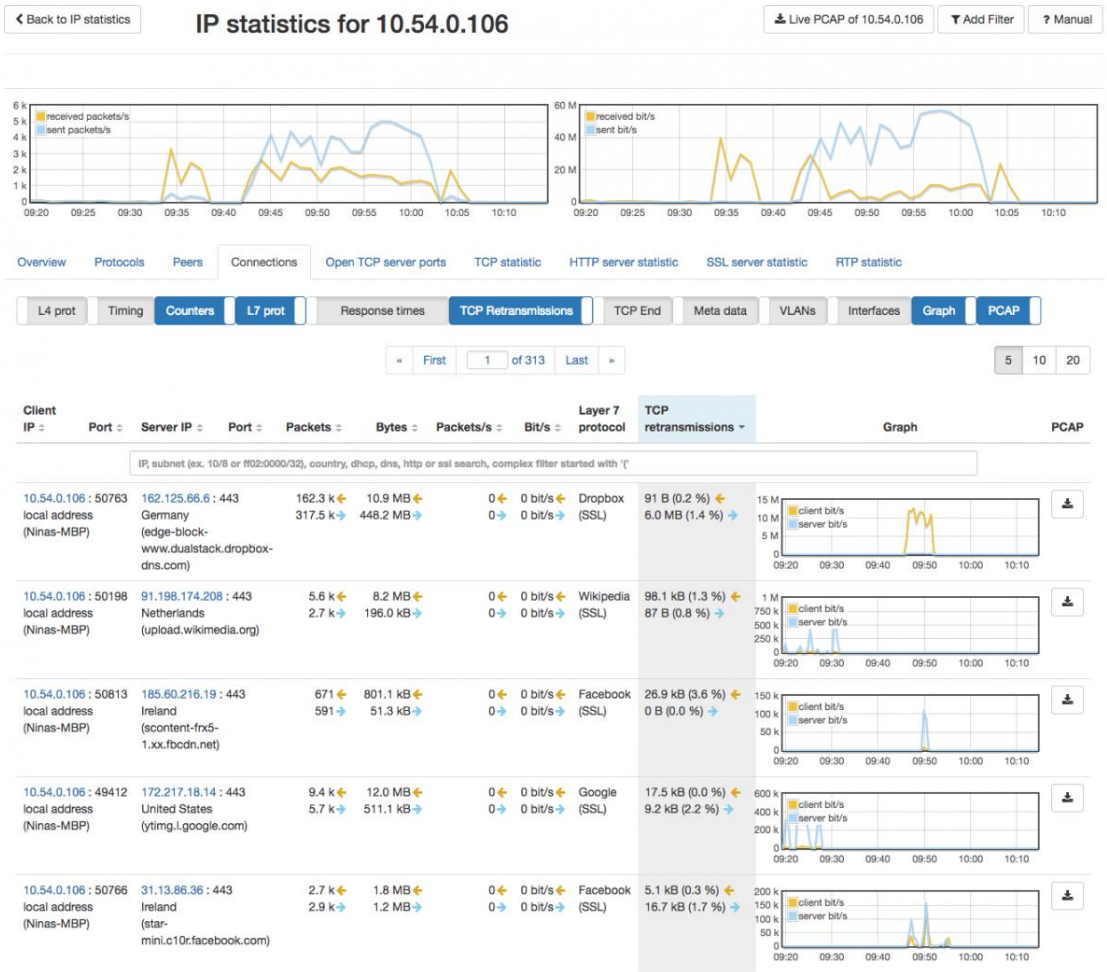
- **Top 协议：**网络中的端点可能会遇到增加的意外流量，例如大型 Windows 更新。通过单击协议，您可以查看哪些 IP 生成了此流量。
- **Top IP：**例如，可能有多个备份同时运行，这会给链路和内部服务器带来负担。
- **Top MAC 地址：**例如，如果此处出现大量多播或广播流量；这可能表明存在环路或类似问题，并且数据包风暴会给网络带来沉重负担。
- **高 TCP 重传率：**这可以指示网段过载，例如来自 WLAN 或终端设备。
- **低网络流量或没有网络流量：**这可能表示链路问题，例如没有连接到 Internet 或另一个网络节点。

在我们的示例中，Dropbox 显示总共 900 MB 的数据传输。通过单击“Dropbox”，我可以轻松查看谁触发了此流量的概览：



在这里，计算机“nb-nina.allegro”以高达 40 MBit/s 的速率生成到 Dropbox 的上传和下载。这可能会因上传和下载而导致用户中断。

通过单击 IP 地址，然后在“会话”选项卡上，您可以通过 TCP 重新传输对连接进行排序：



您可以使用重传次数来估计 Allegro 和接收方之间是否存在瓶颈，以及是否需要重传更多数据包。在我们的示例中，大约有 1.4%（448,2MB 中的 6MB）重传。12 MBit/s（上传）到 Dropbox。可能此时上行链路繁忙并丢弃了几个 TCP 数据包。

如果您需要更详细的分析，您可以使用 pcap 按钮来提取会话数据包。

6、查找 Profinet 问题用例

6.1、挑战

使用虹科 Allegro 网络万用表可以快速轻松地检查 Profinet 设备网络并发现问题吗？

6.2、准备

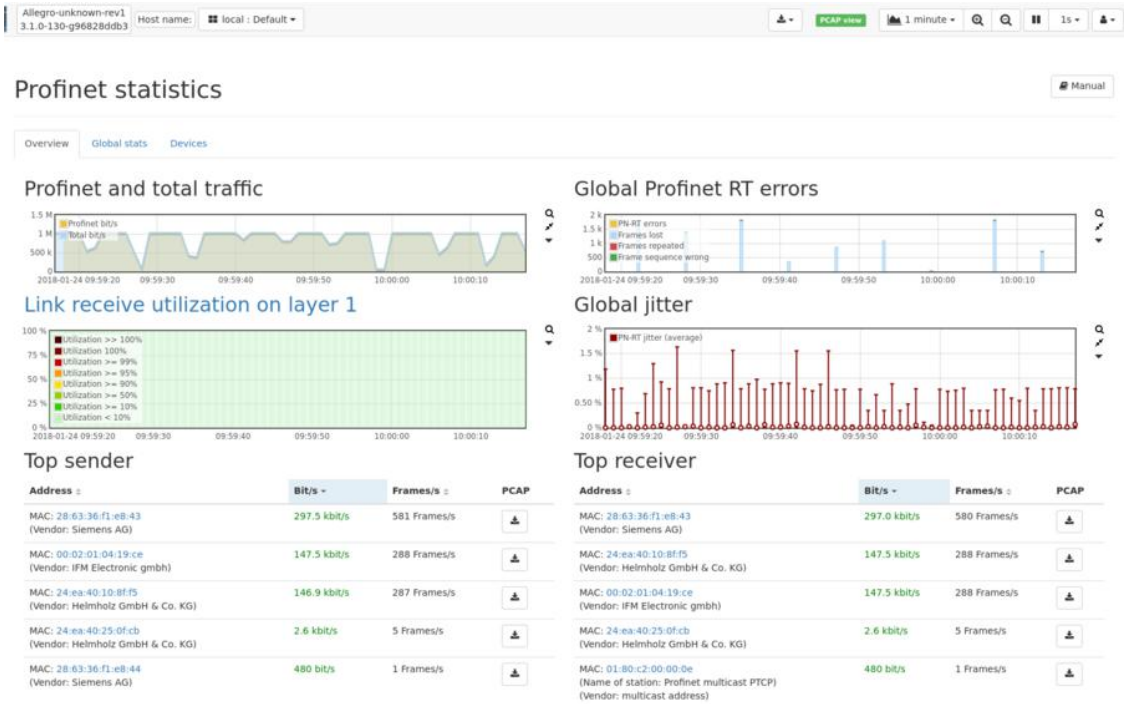
将虹科 Allegro 网络万用表连接到支持 Profinet 的交换机的镜像端口或使用 Tap。放置在那里后，万用表将分析所有数据包并收集实时和回溯的 Profinet 统计数据。

我们不建议在 Profinet 实时网络中以桥接模式在线安装 Allegro 网络万用表，因为这会导致大约 50 微秒的额外延迟。而应该使用网络 Tap 来保持可靠的网络连接。

我们建议使用 Allegro 数据包环形缓冲区功能，因为它允许提取历史特定数据包。

6.3、概述

首先，我们首先概述 Profinet 主设备以及与主设备或彼此通信的所有 Profinet 设备。使用浏览器打开 Web 界面，然后转到“应用程序”->“Profinet 统计信息”。



在此页面上，显示了整个 Profinet 通信的概览。在这里，流量以恒定的 250 kbit/s 运行，然后停止。您可以在 14:11:53 左右看到警报。错误将以同样的方式呈现。当实时帧的时序出现偏差时，带有最小值、平均值和最大值的抖动图一目了然。大约在发送警报的同时，抖动显着增加。

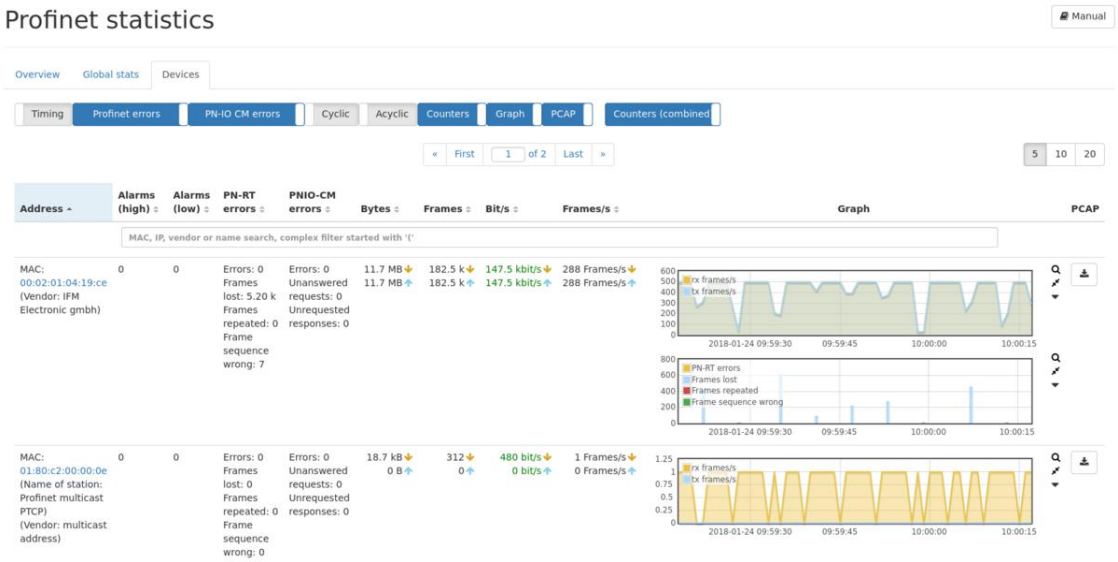
pcap 按钮允许您捕获与 Profinet 相关的整个流量。

如果您希望查看该网络点同时发生的情况，请使用鼠标放大时间范围，然后导航到仪表板。它将显示此时间间隔内整个流量的概览。这有助于识别与非 Profinet 流量相关的 Profinet 问题，例如可能干扰 Profinet 设置的更新或流。

6.4、Profinet 设备

在“设备”选项卡中可以看到所有 Profinet 设备的概览。

显示所有重要信息，例如字节数和所选时间跨度内的帧数。为了快速识别报警和错误，您可以通过单击相关列标题对设备表进行排序。可以通过在过滤器字段中键入其站点名、供应商、MAC 或 IP 地址来过滤特定设备。

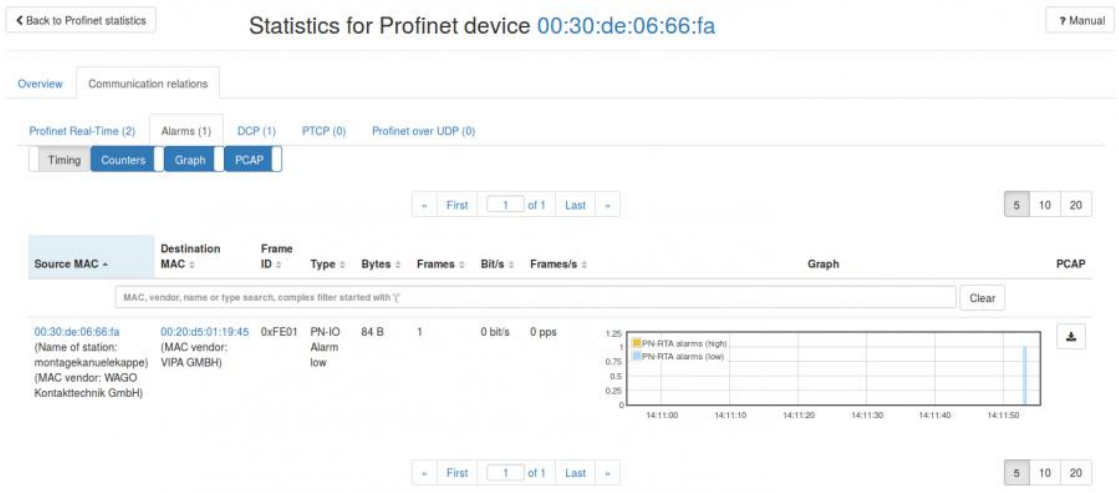


为每个 Profinet 设备显示 MAC 地址。看到相关帧后，将立即显示所有设备的 IP 地址和 Profinet 站名称。

Profinet 统计页面上的两个警报已从 WAGO 设备 00:30:de:06:66:a5 和 WAGO 设备 00:30de:06:66:fa 发出，站点名称为“montagekanuelekappe”。

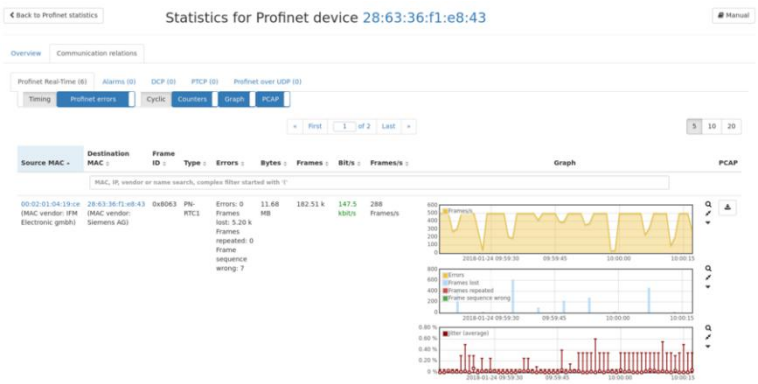
通过单击 MAC 地址，您可以查看特定 Profinet 设备的详细统计信息。设备的统计信息包括传入和传出流量、抖动以及传出警报和错误的数量。pcap 按钮使您能够为该特定 Profinet 设备创建所有传入和传出流量的捕获。

“通信关系”选项卡列出了来自该设备的所有传入和传出帧组。源和目的地都显示，因此可以轻松识别方向。



“警报”选项卡显示此设备已发送的所有警报。此处，WAGO 设备 00:30:de:06:66:fa 站名为“montagekanuelekappe”，向 VIPA 设备 00:20:d5:01:19:45 发送了低优先级警报。

您是否有兴趣在选定的时间范围内捕获数据以进行进一步分析？只需单击右侧的 pcap 按钮即可。



在“Profinet 实时”选项卡中，您将看到所有实时通信并检查抖动值是否不佳。

抖动是如何计算的？两个相邻帧的时钟周期是使用周期计数器计算的。然后将其与这两个帧之间的测量时间进行比较。良好的抖动值应为零，这意味着所有帧都在同一时钟周期内无偏差地到达。差的抖动值将等于甚至大于周期时间。

设备是否有发送帧的问题，它是唯一一个抖动值很差甚至丢帧的设备吗？或者是网络中的交换机导致了问题？检查通过同一交换机通信的其他 Profinet 设备的抖动值和错误。或者，将 Allegro 网络万用表连接到另一个交换机，看看抖动和错误是否减少。

7、捕获分析用例

7.1 介绍

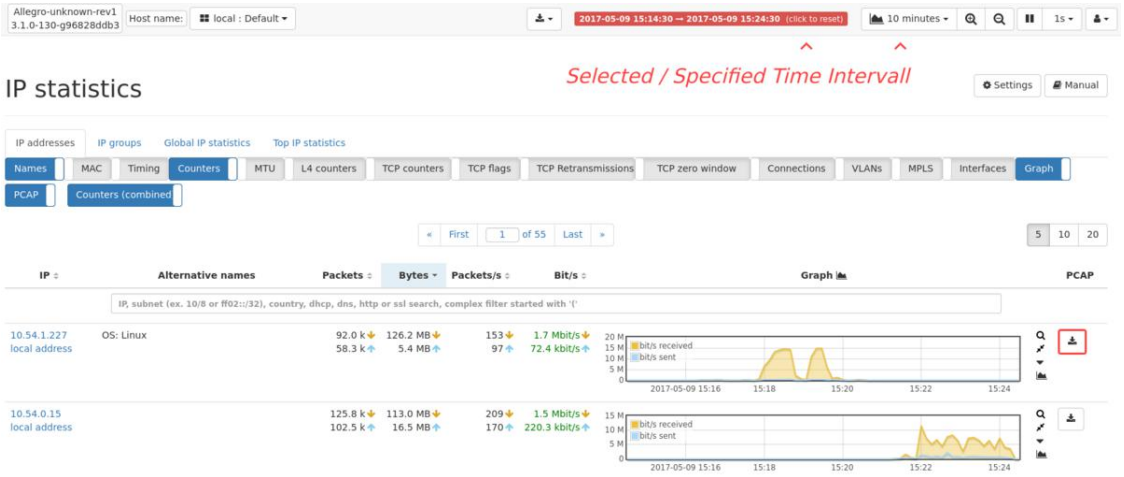
使用 Allegro 网络万用表，可以很容易地以 pcap 格式启动和检索非常具体的网络数据包捕获。然后可以使用 Allegro 内置的 Webshark 或 Wireshark 之类的工具轻松调查此类预过滤的 pcap 文件。

7.2 创建特定 IP 或 MAC 地址的 pcap

所有 Allegro 网络万用表 L2-L7 分析模块在整个仪表板中都具有专用的 pcap 按钮，以非常简单的方式非常具体地捕获大多数流量类型。

例如; 要捕获特定的 IP 地址，请在左侧菜单中导航至“L3 - IP”->“IP”统计信息。然后，通过排序和/或过滤搜索轻松找到所需的 IP 地址，然后单击捕获按钮 -  。

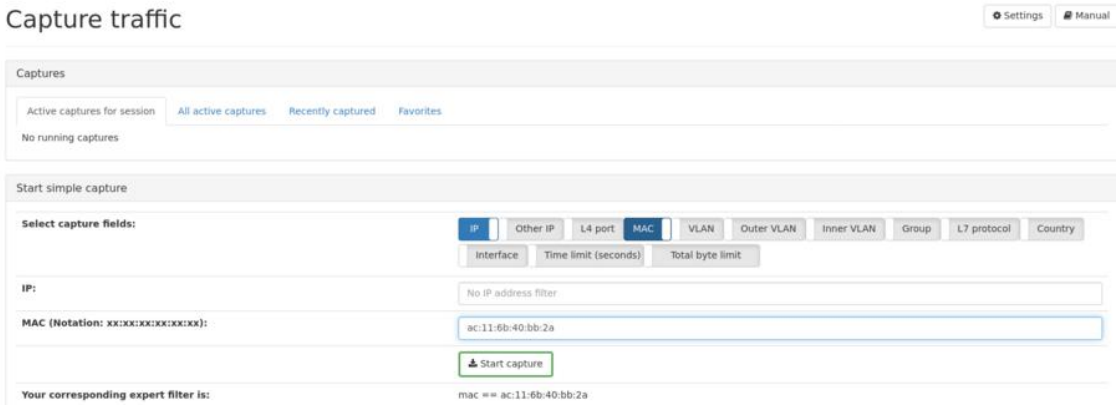
当仪表板中显示特定时间间隔时，仅提取该时间间隔内的有效负载。



要快速查找 IP 地址，您可以通过几乎每一列对 IP 表进行排序。搜索栏/过滤器栏提供了一种将表格内容缩减为您心中的内容的快速方法。这可以通过输入 IP 地址（片段）、DNS 名称（片段）或输入“复杂”过滤器来完成。

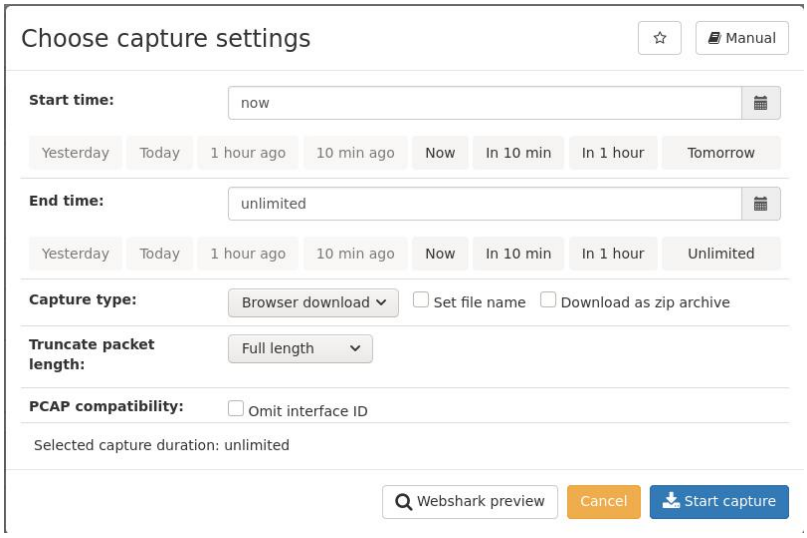
创建特定地址的 pcap 的另一种快速方法是使用 Allegro 的简单捕获功能。

在菜单中转到“通用”->“捕获流量”。现在，在“开始简单捕获”部分，切换所需的捕获字段（例如 MAC、IP），输入地址，然后单击“开始捕获”按钮。



7.3、捕获设置

单击捕获按钮后，将显示“选择捕获设置”对话框。在这里您可以限制捕获的开始和结束时间，并选择是将 pcap 文件直接下载到您的计算机还是将其存储在万用表连接的存储设备上。如果您不需要完整的数据包并且只想要一个在 Wireshark 中打开速度更快的小 pcap 文件，您可以将捕获的数据包限制为给定的长度。



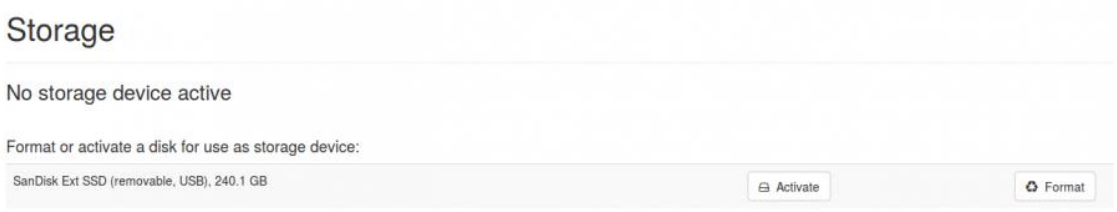
单击“保存捕获”按钮开始配置的捕获。

单击“Webshark 预览”将在 Allegro 网络界面中打开一个基于网络的 Wireshark 窗口。

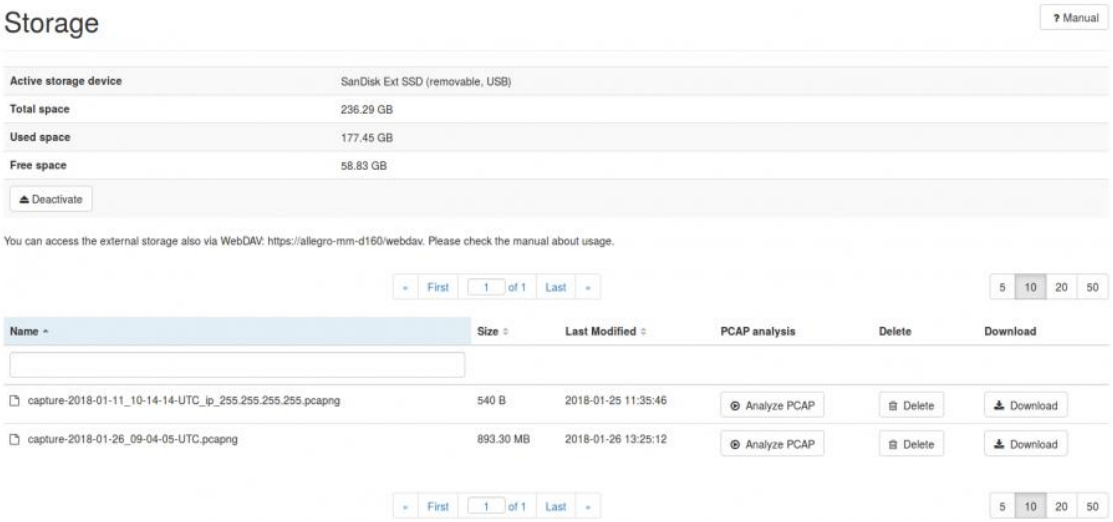
7.4、历史流量提取

使用 Allegro 网络万用表数据包环形缓冲区，可以将过去的流量提取为 pcap 文件。数据包环形缓冲区存储在 Allegro 网络万用表（如果您的型号配备）的内部存储设备上，或存储在外部连接的 USB 存储设备上。建议使用支持 USB3.x 的快速 SSD。也可以使用 U 盘，但如果 U 盘写入速度太慢，可能会丢失一些突发数据包。

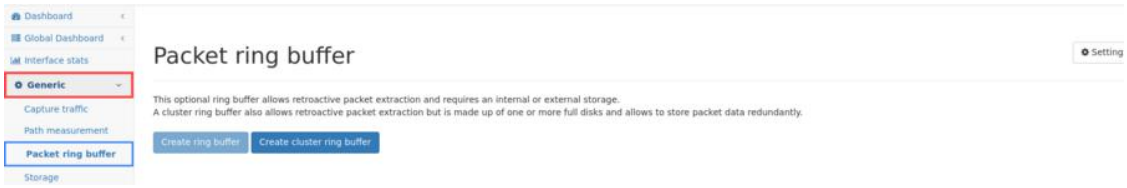
您可以在“通用”->“存储”下查看有关可用于 Allegro 万用表的所有存储设备的概述。



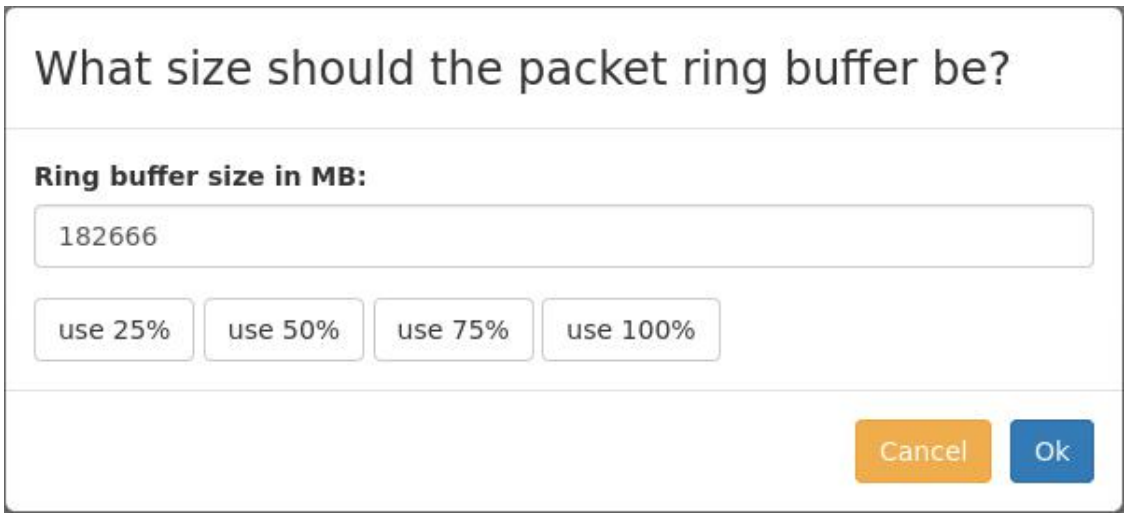
外部 SSD 连接到 USB 端口，但尚未激活。单击“激活”按钮，以便可以使用设备。如果磁盘的文件系统不适合环形缓冲区，则会弹出警告提示您格式化磁盘。格式化或激活后，存储页面将显示有关磁盘使用情况的信息以及磁盘上所有文件的概览。



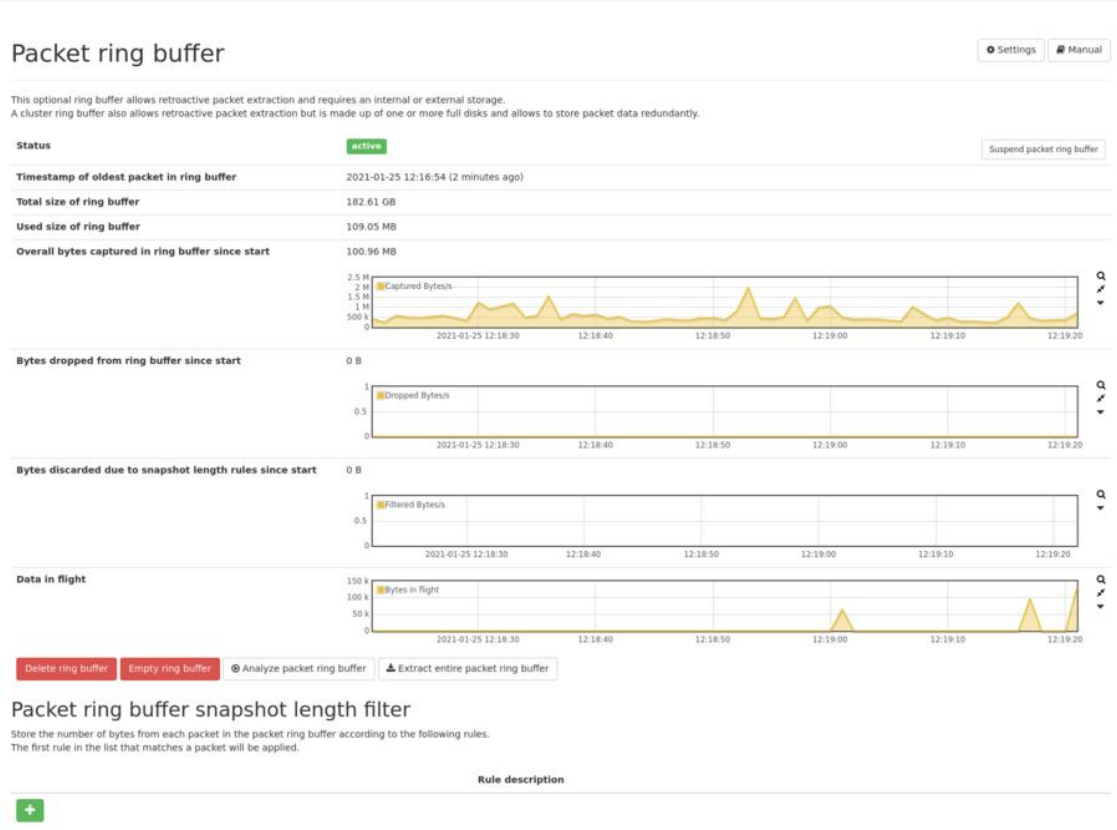
现在存储处于活动状态，如果在格式化期间尚未准备好，则必须创建环形缓冲区。这可以在“通用”->“数据包环缓冲区”中实现。单击“创建环形缓冲区”按钮。



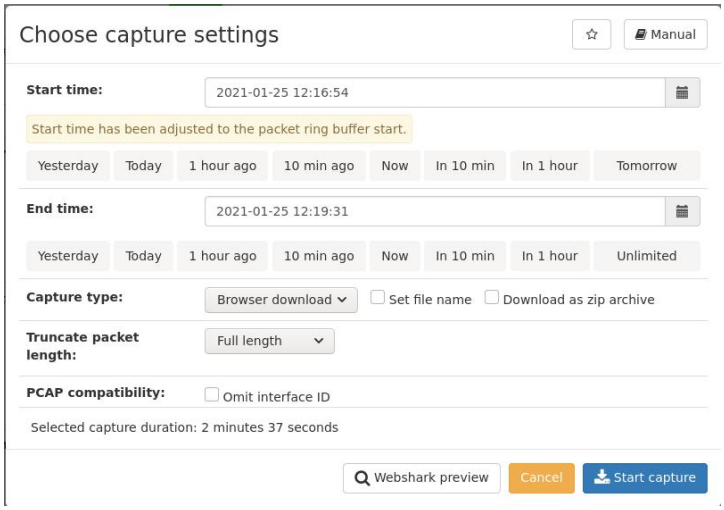
必须指定环形缓冲区的大小。如果存储设备上不需要 pcap，则环形缓冲区将使用 100% 的存储设备容量。



当包环缓冲区创建并运行时，“数据包环缓冲区”统计页面会显示有关环缓冲区使用情况的信息，并且还会显示一些恢复或过滤流量的图表。可以应用过滤器来确定哪些数据包存储在环形缓冲区中。



当数据包环形缓冲区启动并运行时，可以利用任何捕获来提取过去的流量。通过用鼠标左键单击在用户界面的任何图形中选择时间跨度，然后单击 pcap 按钮。选定的时间跨度将显示在“选择捕获设置”对话框的开始和结束时间字段中。



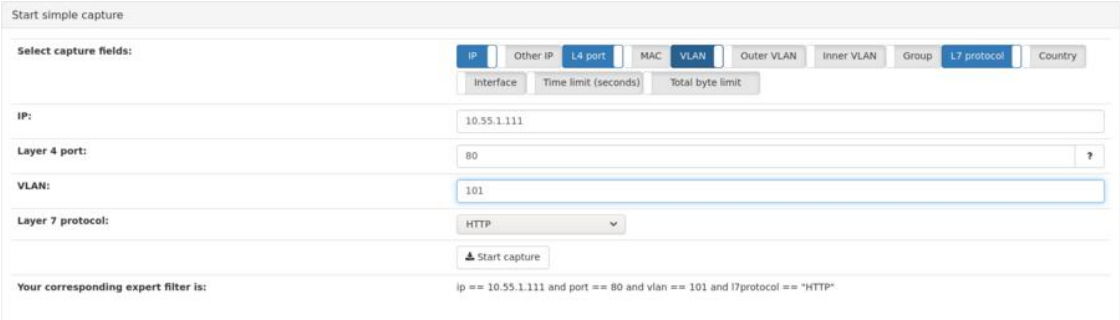
在选择时间字段或单击常用时间的专用按钮时，可以使用日期和时间弹出窗口更改开始和结束时间。如果开始时间早于包环缓冲区的开始时间，则将其调整为开始时间并显示提示。

7.5、创建具有多个条件的复杂捕获

捕获可以使用复杂的过滤器表达式开始，用于特定捕获，例如 IP 地址或第 7 层协议。

要查看基本概述，请从任何模块开始捕获。您可以在 Web 界面顶部栏的捕获按钮上查看所有正在运行的活动捕获。

在“开始简单捕获”页面上，可以轻松访问所有常用的过滤器表达式。结果表达式如下所示。



该表达式可以在专家过滤器字段中使用和编辑。所有过滤器都可以与“and”/“&&”或“or”/“||”组合。括号可用于指示优先级。

8、VoIP 分析用例

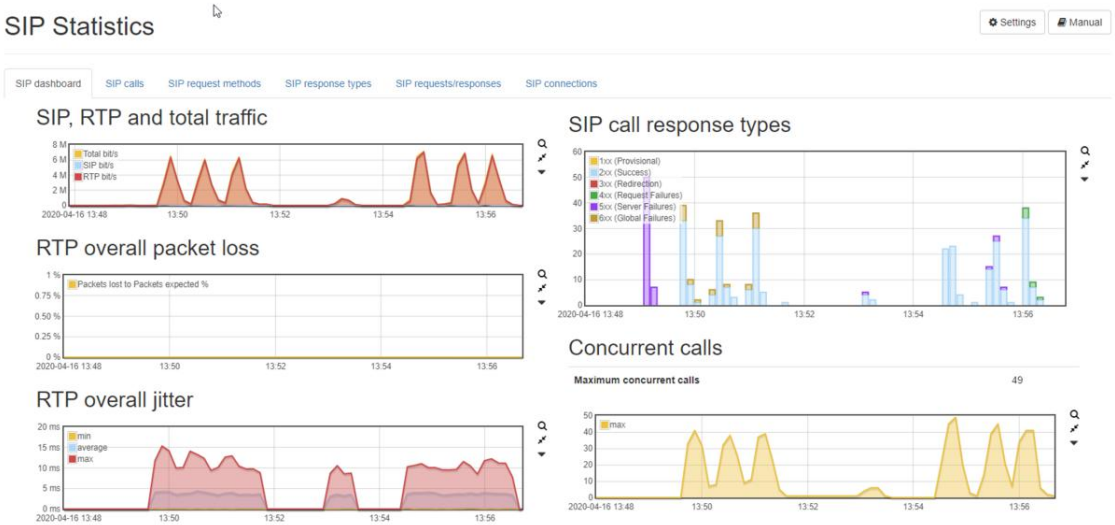
8.1、介绍

如今，大多数公司的电话系统都基于 IP 语音.....简称 VoIP。虽然 VoIP 比“传统”电话基础设施有很多优势，但 VoIP 也给负责维护良好网络的网络管理员和工程师带来了新的挑战。通常情况下，VoIP 服务和流量通过同样处理常规服务器/端点通信的基础设施组件。幸运的是，VoIP 是一种带宽相当低的通信类型（例如编解码器 G.711 = 64 Kbps BR* / 87.2 Kbps NEB*）。然而，另一方面，管理者最好对他们的网络的整体质量保持警惕，因为 VoIP 需要低延迟和低数据包丢失量。

- BR = 比特率 / NEB = 标称以太网带宽（单向）

虹科 Allegro 网络万用表通过提供对 VoIP 通信的全面可见性以及高级 VoIP 故障排除功能来帮助网络管理员和工程师。使用 Allegro 网络万用表进行的 VoIP 监控和分析可以实时和回溯进行。

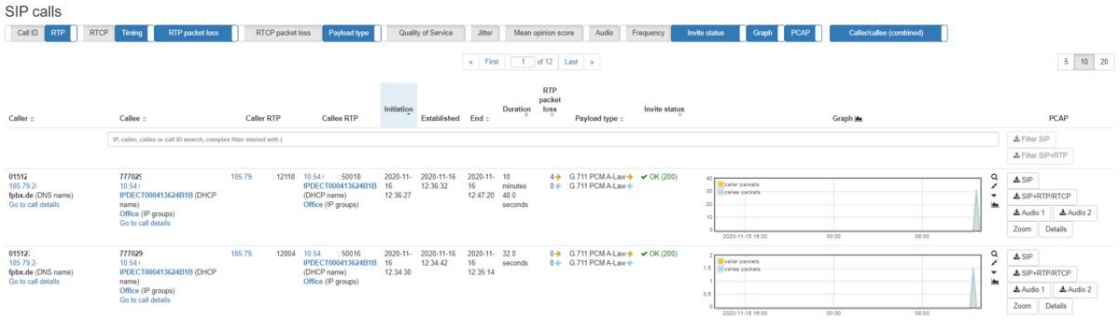
8.2、全局 SIP 统计



虹科 Allegro 网络万用表中的 VoIP 分析和调试，可以通过左侧菜单 L7 - 应用程序 -> SIP 统计信息到达。整个 SIP 统计仪表板，如上图所示，将呈现给用户。此页面旨在“回溯”，并使管理员能够查看一段时间内的统计数据和事件。过去 4 天内是否有异常丢包或高抖动的情况，可能是一个很好的例子。这些图表清晰的描述了流量分布统计信息、数据包丢失和抖动信息、并发呼叫趋势图和围绕 SIP 信令响应类型/代码的统计信息。可以选择所图表的部分，以放大某些时间范围的事件。

8.3、VoIP 呼叫分析

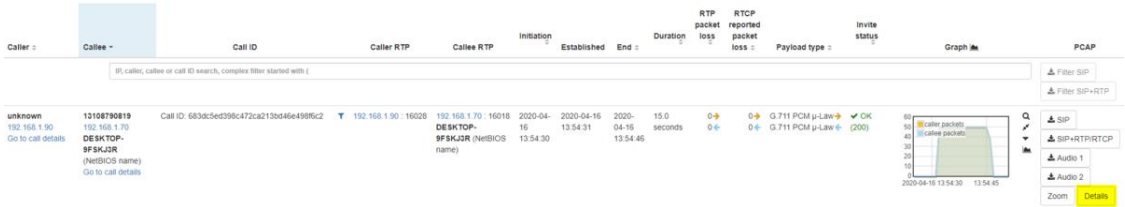
进入第二个选项卡“SIP 呼叫”，用户将看到在选定时间范围内和/或实时显示的所有 VoIP 呼叫列表。多个带有统计信息的表可以由用户自行决定打开或关闭，并且可以对表进行排序。



要调查特定的电话号码，例如来自报告通话（质量）问题的人，只需在搜索栏中输入电话号码并相应地对您感兴趣的表格（例如“开始”时间）进行排序。在 Allegro 网络万用表中，搜索栏还可用于应用复杂的显示过滤器。例如，如果从 100 个或 1000 个索引的 VoIP 呼叫中，您只对不成功的呼叫感兴趣.....（状态代码！=200）将适用。我们已经谈到了 VoIP 对时间的敏感性。有人可能会说，任一呼叫方向上的抖动超过 20 毫秒，就会开始影响和降低呼叫质量。抖动越高，通话质量就越差。对于仅显示受不良抖动影响的呼叫的列表，可以在 SIP 呼叫屏幕的搜索栏中轻松设置过滤器 (avgjitter > 20)。

8.4、单个呼叫的详细报告

在每个特定呼叫旁边，您会发现几个按钮，十分有用。请注意，必须启用列切换“PCAP”。现在我们将进入下面突出显示的“详细信息”按钮。



管理人员和工程师经常发现自己处于对事件历史或详细报告感兴趣的位置。一个页面，讲述了整个故事，并提供了一些图表，以便更容易地翻译给不太懂技术的人谁可能参与。点击一个电话旁边的“详细信息”按钮，你就会看到十分详细的统计信息。

当呼叫详细信息页面打开时，首先单击“缩放”呼叫按钮。这样做时，Allegro 网络万用表中显示的数据将聚焦（或放大）呼叫开始和结束的确切时间和持续时间。您现在将看到围绕呼叫的数据和统计数据很好地集中在各自的图表中。浓缩到一个视图中，您会在屏幕左侧找到有关编解码器和网络的事实和数据，中间是关键质量指标的趋势图，屏幕右侧是捕获按钮。

8.5、数据包、抖动和 MOS

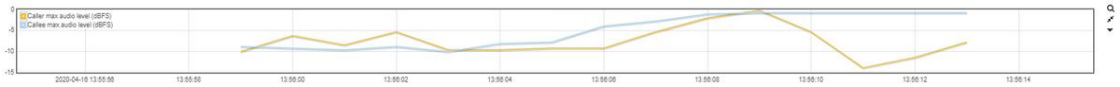
在顶部图表中，您可以看到特定呼叫的数据包流（或数据流）。第二张图保存了所有关于数据包丢失和开销数据包的信息。第三张图显示了非常关键的抖动信息。事实上，网络及其服务的性能和质量取决于多种因素。称为 MOS 的 VoIP 特定评分算法根据多个依赖项（如编解码器、其对丢包的敏感性和网络中的实际丢包率）从 1（差）到 5（最佳）计算呼叫质量等级。

在每个图表中都可以清楚地看到下降或不一致。显示的测量值可用并显示每个单独的 A/B 号码，即呼叫者和被呼叫者。

8.6、音频电平图 (dBFS)

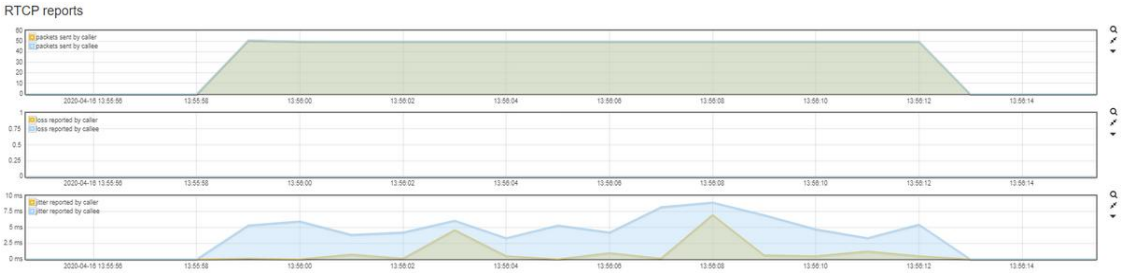
上数第五张图显示了有关来自两个方向的 RTP 音频的音频电平信息。你可能会问这对我有什么帮助。好吧，因为在 Allegro Packets，我们也是网络工程师，并且像一个人一样思考，我们很乐意解释这如何为您提供很多帮助。假设您收到最终用户投诉，描述 - 通话期间质量不佳 。无论如何，您很可能几乎不会收到比这更详细的投诉。但是，作为管理员，您可能已经在考虑语音失真、中断或噼啪声。现在，语音失真、延迟和中断很可能是由数据包丢失和/或不良抖动引起的。因此，导航到

呼叫详细信息屏幕以调查呼叫时数据包丢失和抖动的严重程度，您会立即看到……？ ……没有数据包丢失，非常低的抖动……EUREKA！不是网络。在这种情况下，您可以轻松浏览音频电平图，以便在图形高于 0 时直观确认音频剪辑（失真发生的电平）。



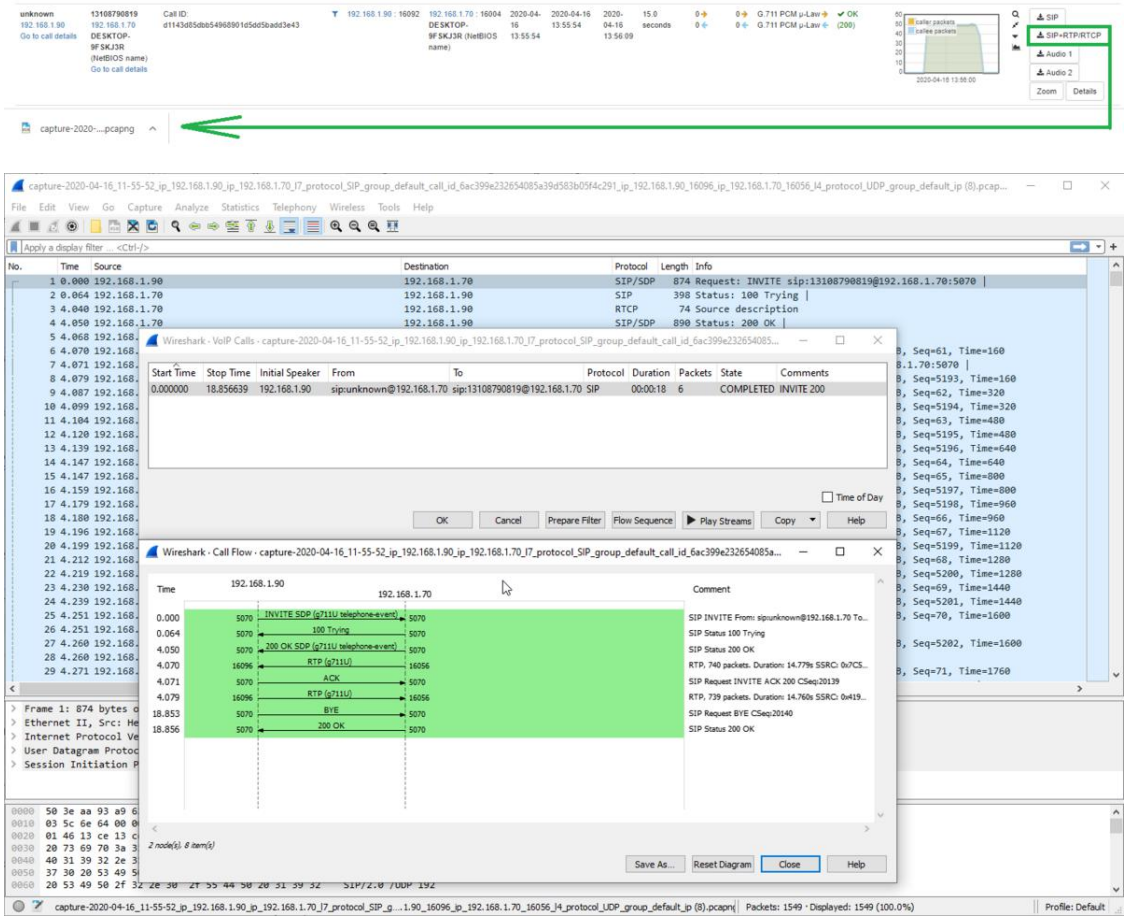
8.7、RTCP 报告

请注意，虹科 Allegro 网络万用表还会解码在手机之间发送的 RTCP 报告。这提供了有关数据包丢失和估计抖动的额外有价值的见解，如呼叫/被呼叫手机（网络外）本身所经历的那样。



8.8、从 SIP、RTP、RTCP 提取 pcap

我们从网络管理员和工程师那里了解到，在 Wireshark 中捕获和查看呼叫的 SIP 及其对应的 RTP 并非易事。特别是在多个呼叫处于活动状态的链接上。然而，这对于 Allegro 网络万用表来说非常容易。在 Voip 呼叫页面（以及呼叫详细信息页面）上的每个单独呼叫旁边，您会找到几个下载按钮。因此，相应的和相关的数据可以很容易地提取和下载为 pcap。无论您是只想查看 Wireshark 中的 SIP 流，还是在一个干净过滤的 PCAP 中检索呼叫的相关 SIP+RTP+RTCP 以进行后期分析。只需在 Allegro 网络万用表中单击 1 次即可。Allegro 网络万用表支持和完全自定义记录的数据包数据切片。例如，



8.9、语音 VoIP 故障排除 (MP3)

噼啪声、回声或低沉的音频很可能不是网络造成的。但是，这些特定的东西也不能从音频电平图中的信息中推导出来。在这种情况下，Allegro 网络万用表提供了下载按钮 Audio1 和 Audio2。在允许或故障排除好处超过隐私限制的情况下，管理员/工程师可能希望将每个方向的呼叫音频下载为 MP3。这有助于解决某些问题，并提供耳机（电缆）、糟糕的车载套件或其他类似东西的声音证据。如上所述..... Allegro 网络万用表支持和完全自定义记录的数据包数据的切片。

9、关注我们

HongKe 虹科

网络安全与可视化

网络可视化，网络监控，时间服务器

400-999-3848

support@hkaco.com

hongwangle.com

广东省广州市高新技术产业开发区科学大道99号科汇金谷三街2号701室