itbigtec
艾体宝

# IOTA 1G

## 用户操作指南


PROFITAP

# 目录

# 产品概览

## 1.1 硬件概览

IOTA是一个多功能的无源网络探头，具有集成的流量捕获和分析功能。IOTA设计为安全灵活的分析解决方案，是获取工业或企业级网络访问和可视性的重要资产 。

网络工程师和IT分析师使用Profitap IOTA快速清晰地了解网络传输情况。这意味着可以快速执行全面分析，帮助工程师只需点击一下即可找到根本原因。

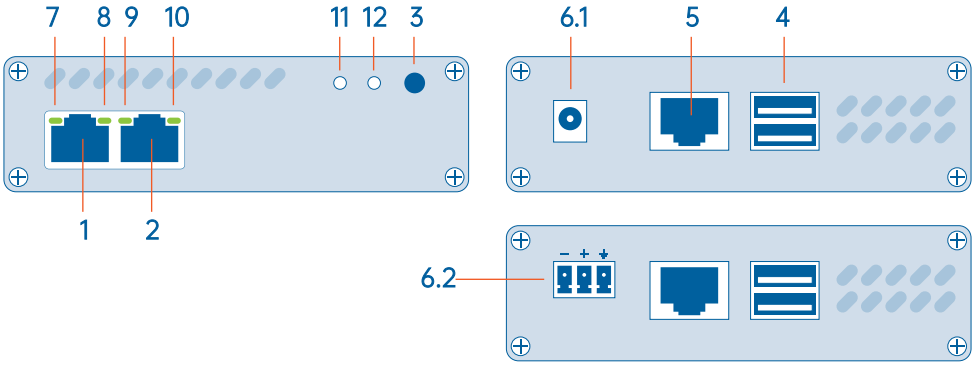
该设备可以部署为专用探头，也可以编程进行自主分析，无需现场网络专家。

# 1.2 技术规格

| | | |
|---|---|---|
| 内联模式 | | Yes |
| 内联延迟 | | 1G: 380 ± 8 ns<br>100M: 720 ± 24 ns<br>10M: 7600 ± 25 ns |
| 内联抖动 | | 20 ns |
| 双SPAN输入模式 | | Yes |
| FAIL-SAFE | | Yes |
| 捕获性能 | | 3.2 Gbps / 3.2 Mpps |
| 数据包处理器 | | Yes, 2 Gbps / 3.2 Mpps |
| 硬件时间戳 | | Yes: 8 ns, NTP synchronized |
| 内存 | | 1 TB |
| 电源输入 | 12V 模式 | 12 VDC |
| | | PoE (management RJ45) |
| | 24V 模式 | 24–48 VDC |
| | | PoE (management RJ45) |
| 功耗 | | 12 W |
| 管理 | 接口 | 10/100/1000 Ethernet |
| | | 2 x USB 3.0 |
| | 服务 | HTTPS (server), UPnP/VPN |

# 1.3 接口 & LED指示

## IOTA 1G 接口




1, 2 Ethernet port A, B

3 START/STOP/RESET按钮

4 2 x USB 3.0 port type A

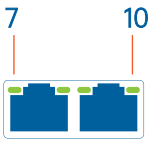
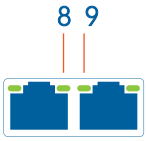
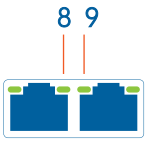
5 RJ45 管理端口 (PoE)

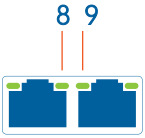
6.1 12 VDC电源输入

6.2 24-48 VDC电源输入 7,

8, 9, 10, 11, 12 活动 LEDs

## IOTA 1G LED指示

| LEDs | 状态 | 含义 |
|---|---|---|
|  | 7 和/或 10<br>稳定绿色 | 端口已链接 |
| | 7 和/或10<br>闪烁绿色 | 端口已链接并具有RX/TX活动(流量正在通过)。 |
|  | 8 稳定绿色<br>9 关闭 | 捕获接口以10 Mbps的速度运行。 |
| | 8 闪烁绿色<br>9 关闭 | 捕获接口正在初始化。 |
|  | 8 关闭<br>9 稳定绿色 | 捕获接口以100 Mbps的速度运行。 |
| | 8 关闭<br>9 闪烁绿色 | 捕获接口固件已损坏。 |

| LEDs | 状态 | 含义 |
| --- | --- | --- |
|  | 8+9稳定绿色 | 捕获接口以1 Gbps的速度运行。 |
| | 8+9闪烁绿色 | 端口已链接并具有RX/TX活动(流量正在通过)。 |
| | 8+9交替闪烁 | 捕获接口无法在连接的设备之间找到共同的速度。 |

| LEDs | LED 11 状态 | LED 12 状态 | 含义 |
| --- | --- | --- | --- |
|  | 橙色闪烁 | OFF | 启动 |
| | 绿色 | 绿色 | 运行 |
| | 绿色 | 绿色闪烁 | 捕获 |
| | 绿色 | 橙色闪烁 | 捕获警告 |
| | 绿色 | 红色 | 磁盘满了 |
| | 橙色绿色闪烁 | 橙色绿色闪烁 | 更新中 |
| | 红色闪烁 | 红色闪烁 | 硬件故障 |
| | 橙色闪烁 | 橙色闪烁 | 出厂重置 |
| | 绿色闪烁 | OFF | 关机中 |
| | OFF | OFF | 完成关机 |

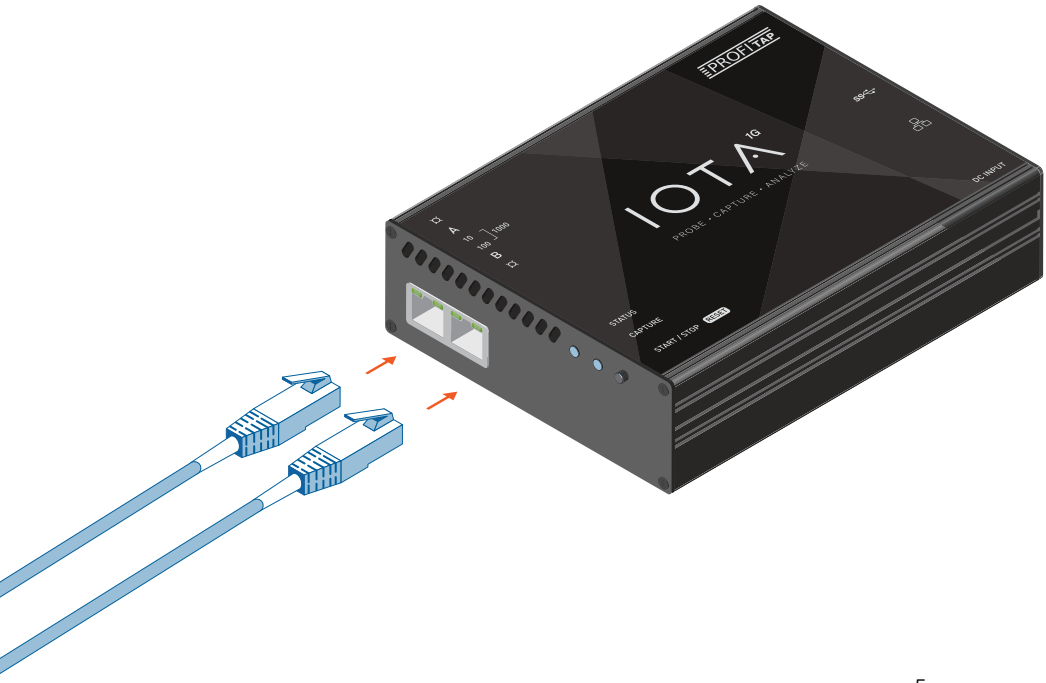
# 入门指南

## 2.1 部署IOTA

### IOTA 1G

将您要监控的线路的以太网电缆插入IOTA的RJ45端口A和B，使用5类UTP电缆 ，额定为千兆操作。

> ► 注意：当在线部署IOTA时，为了充分利用其故障安全功能，请在通电前将其连接到网络。这一步对于验证故障切换时内联路径的可用性至关重要。



## *IOTA 1G 机架式型号*

机架式型号可以使用 Profitap 机架式机箱套件（单独出售；参考：ARKB-1U）安装在标准的 19" 机架上。使用提供的螺钉将机箱固定在机架上，然后插入IOTA并使用设备前面板上的拇指螺钉将其固定在机箱上。

## 2.2 设备供电

根据IOTA型号，连接12V/2.5A直流电源或24-48VDC端子板。另外，也可以通过PoE，通过管理端口为设备供电。同时连接电源端口和PoE管理端口，以实现冗余供电，确保在任何一个端口被断开或无法提供电源的情况下继续运行。

IOTA在建立电源连接后自动启动。它的状态可以通过活动LED灯来观察。

► 注意：初始启动可能需要一些时间来完成。当Status和Capture LED指示灯均为绿色时，说明IOTA已经完成了启动序列。

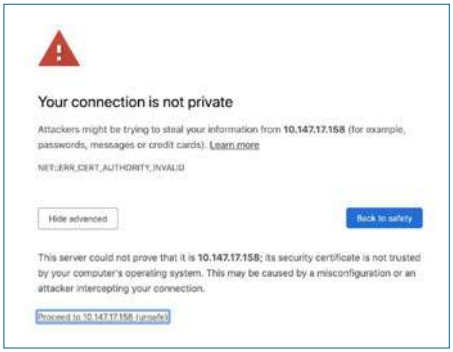
一旦上电，内联故障切换电路就会被禁用，从而有效地将设备置于内联状态。

## 2.3 通过网络访问IOTA

要通过网络访问IOTA，请通过浏览IOTA的设备IP，包括端口号，连接到HTTPS接口。
完整的URL应该是：https://x.x.x.x:3000
默认情况下，DHCP模式是启用的，如果没有给IOTA分配IP，默认的后备IP是169.254.1.1

初次登录时，请使用以下凭证：
默认username: admin
默认password: admin

► 注意：如果您的浏览器显示'Your connection is not private'警告，请点击底部的advanced > proceed to... 网址进入到IOTA页面



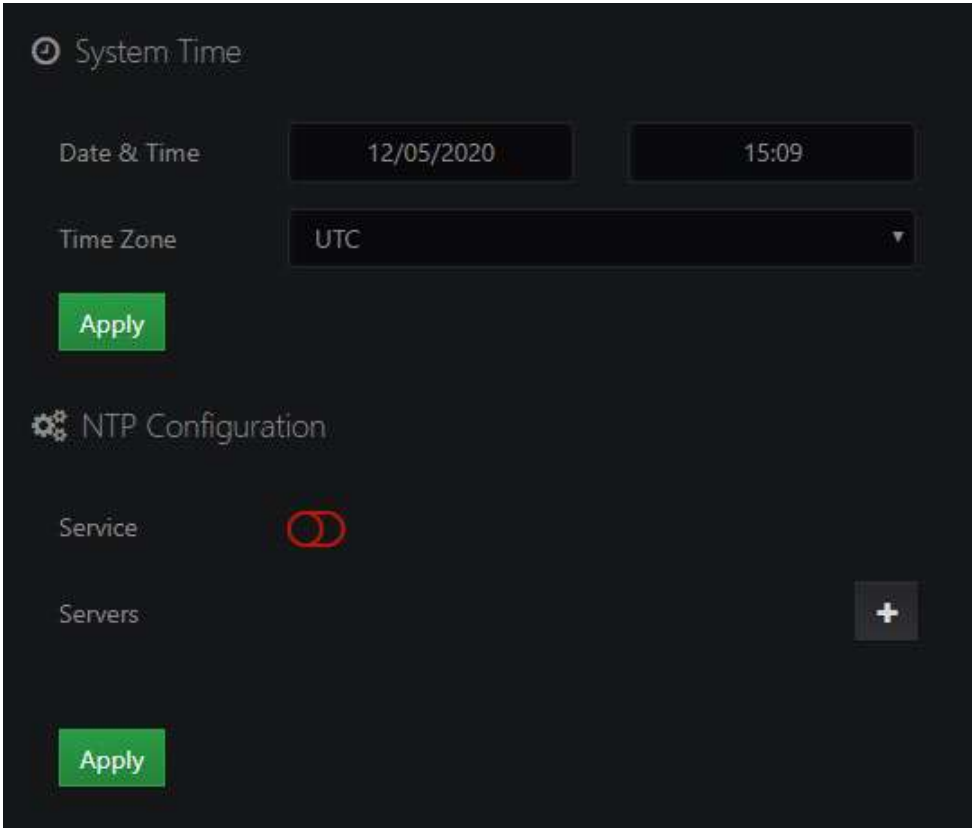

# 2.4 IOTA配置

## System Time系统时间

NTP服务默认启用：如果IOTA有互联网接入，则不需要额外的配置。系统时间也可以手动调整。
系统时间可用于：

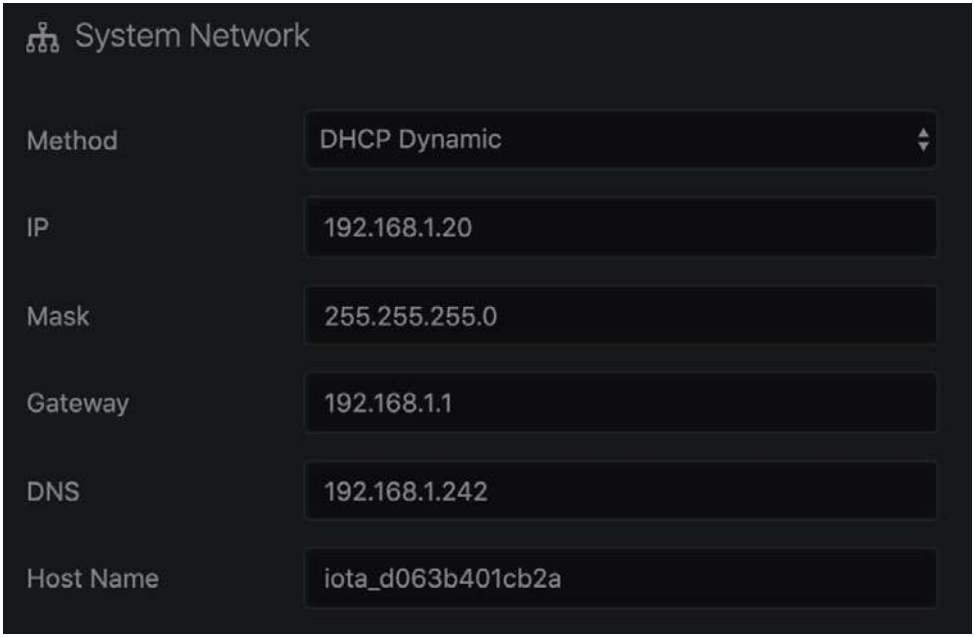
- 嵌入式操作系统，
- 捕获接口，以不断约束硬件时间戳计数器。

改变时间可能需要重新启动捕获界面才能生效。



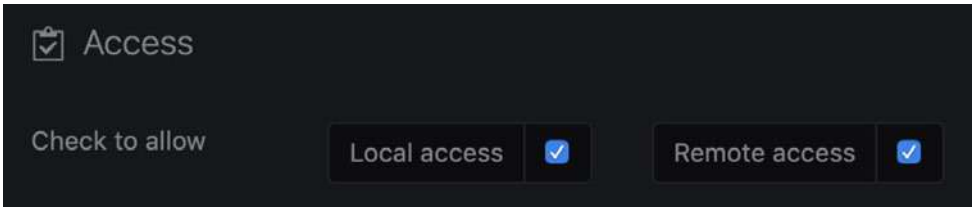
## *System Network系统网络*

导航到IOTA设置/配置以更改默认网络设置，如IP、掩码、网关、DNS和主机名。



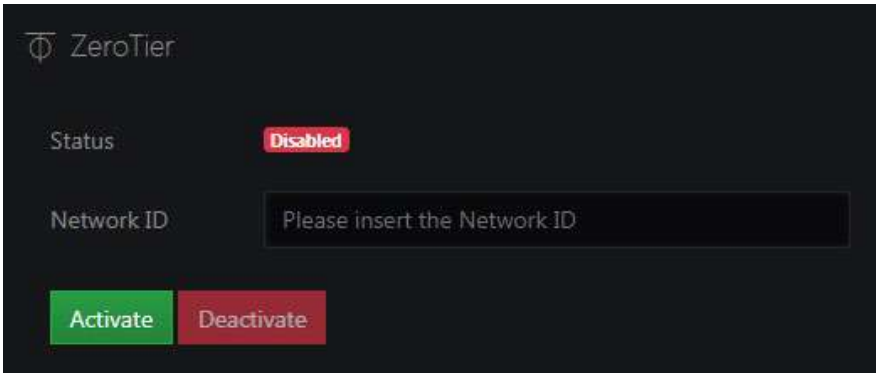

## *Access / Internal Firewall访问/内部防火墙*

用于限制来自本地客户端(LAN子网)和/或远程客户端(WAN、ZeroTier)的访问。



## *ZeroTier*

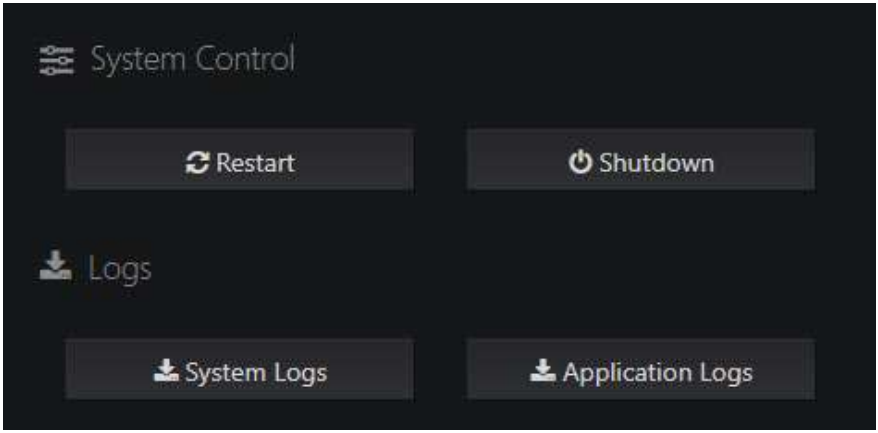
ZeroTier提供了一种简单的方式，通过P2P VPN远程访问设备，并在云应用上管理虚拟网络。(更多信息：www.zerotier.com )




## *System Control & Logs*

按 'Restart' 或 'Shutdown' 按钮原厂重启或关闭您的IOTA。

按'System Logs' 或'Application Logs' 按钮下载系统日志和应用程序日志。



## *System Updates*

*IOTA Settings > System Updates*页面提供了关于当前IOTA软件版本，最新可用版本和更新日志信息。如果IOTA能够访问互联网，则会自动获取最新更新版本号和变更日志，并通过 'Update' 按钮更新IOTA软件。如果设备无法访问互联网，可以下载最新的IOTA软件，并通过'Select a file' 按钮进行更新。

# 捕获指南

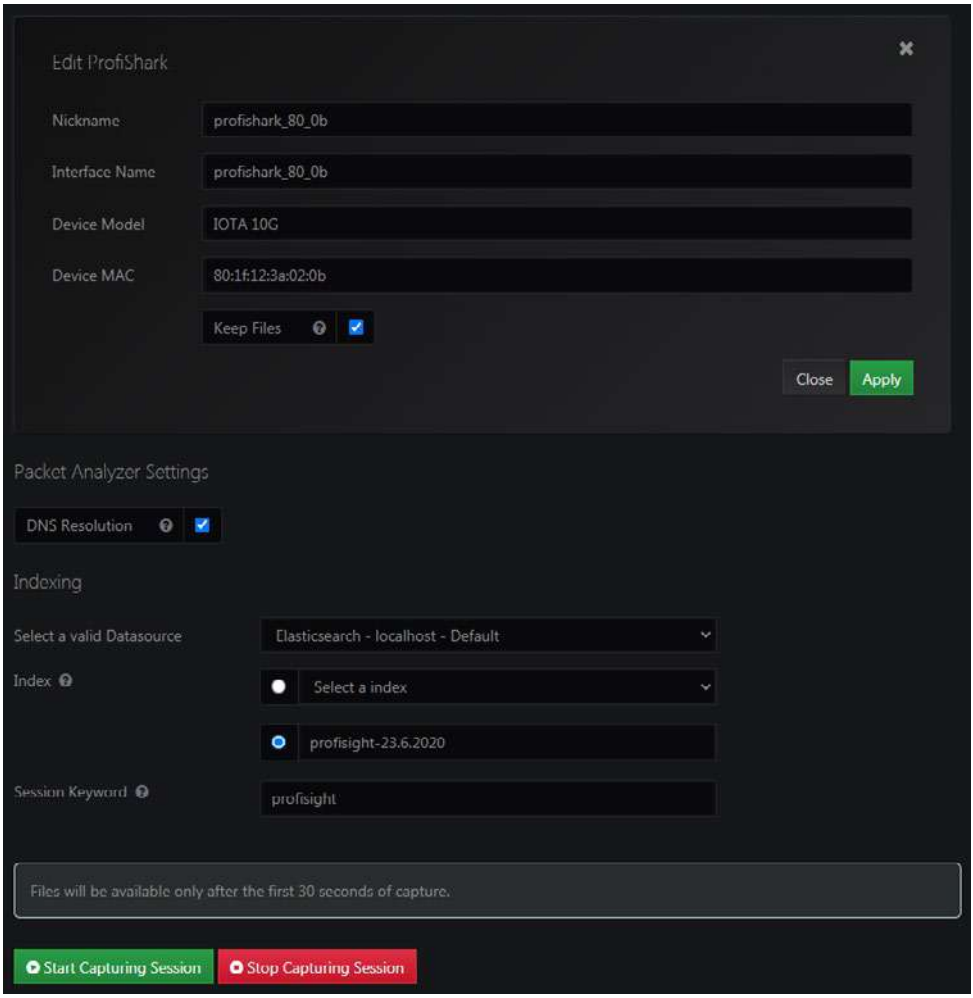
## 3.1 CAPTURE CONTROL捕获控制

*Capture > Capture Control*界面包含了捕获流量和对捕获流量进行索引的选项。当捕获进行时，流量会自动在指定的数据源中进行索引。如果在捕获界面的设置中启用了'Keep Files' 选项，捕获的流量将会保存在磁盘上，每30秒或当当前文件的大小达到4GB时，将自动创建新的文件。

► 注意：捕获文件会自动分析和索引。如果启用了'keep file' 选项，则可以从仪表盘中检索完整的跟踪文件、部分跟踪文件，或者过滤后的副本。如果禁用了 'keep file'选项，则仪表盘只显示索引数据，无法检索原始跟踪文件。

*Indexing*选项定义了将在其中索引捕获的数据的数据库和索引。默认数据源时IOTA设备上已存在的数据库。如果已在Configuration > Data Sources中设置了其他数据源，则可以选择这些数据源。

*Index*子选项定义了捕获的数据将被保存到哪个索引中。选择所选数据库上已经存在的索引，或者通过选择第二个选项并输入名词（必须以 'profisight'开头）创建一个新的索引。


Edit ProfiShark
Nickname
profishark_80_0b
Interface Name
profishark_80_0b
Device Model
IOTA 10G
Device MAC
80:1f:12:3a:02:0b
Keep Files
Close
Apply
Packet Analyzer Settings
DNS Resolution
Indexing
Select a valid Datasource
Elasticsearch - localhost - Default
Index
Select a index
profisight-23.6.2020
Session Keyword
profisight
Files will be available only after the first 30 seconds of capture.
Start Capturing Session
Stop Capturing Session

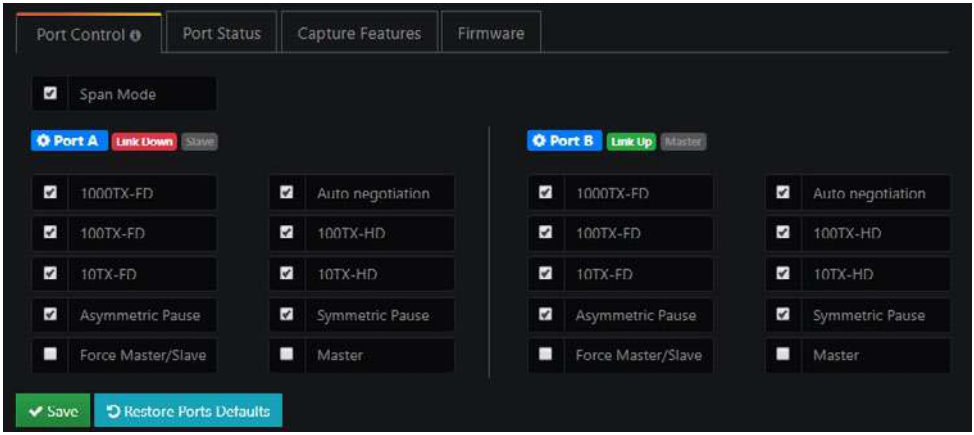
# 3.2 INTERFACE CONFIGURATION接口配置

Capture > Interface Configuration屏幕上提供了连接设备、捕获统计和设备信息的概述。要更改接口设备，有几个标签可供选择：

## Port Control端口控制

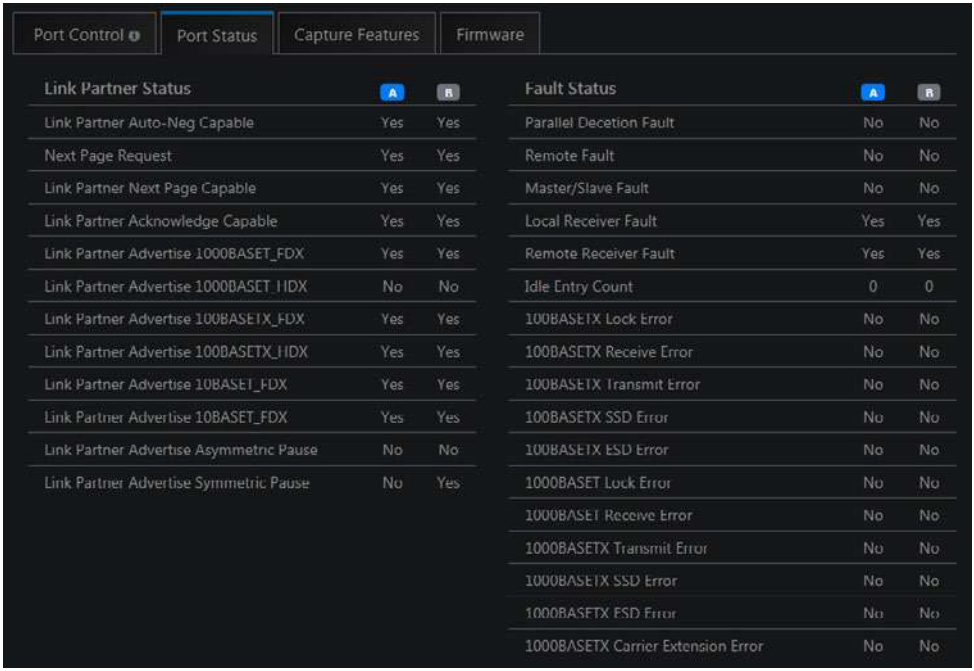
如果IOTA计划内联使用，必须设置适当的配置。'In-Line mode'是默认模式('Span Mode'复选框未勾选)。通过勾选'Span Mode'复选框，IOTA可以设置为SPAN模式。

端口速度和行为可以在这个屏幕，包括端口 A 和端口 B 。

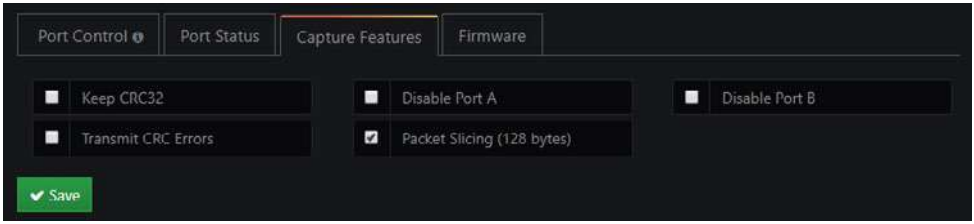



## Port Status端口状态

该选项卡提供了端口 A 和 B 的链路伙伴状态和故障状态的概览。




## *Capture Features捕获功能*



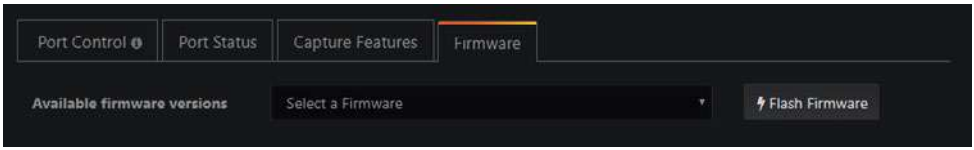

通过该选项卡可以配置以下捕获设置：

- Transmit CRC Errors
- Keep CRC32
- Packet Slicing (128 bytes)
- Disable Port A
- Disable Port B

可以通过勾选或取消勾选相关复选框来启用和禁用功能。

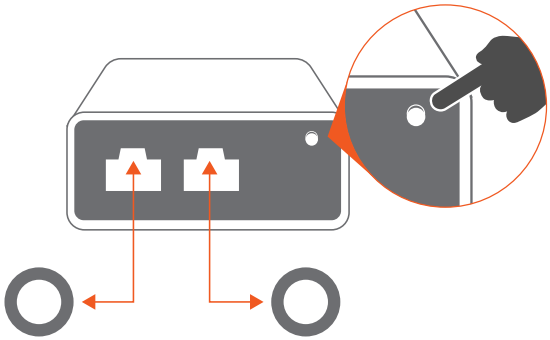
### *Firmware固件*

从下拉菜单中选择一个固件版本，然后点击 "Flash Firmware "按钮，即可对固件进行刷新。




## *3.3 AUTONOMOUS CAPTURE自主捕获*

为了能够在不允许或不可能通过网络远程访问的网络中捕获流量，您可以通过按下物理的START/STOP按钮来启动IOTA的自主捕获功能。



START：开始捕获。IOTA 将使用捕获控制中的最新设置。

STOP：停止捕获

FACTORY RESET：断开IOTA的电源。长按START/STOP按钮然后在保持的同时，重新连接电源并保持20秒。当LED灯为绿色时，FACTORY RESET完成。

RESET：长按START/STOP按钮和保持20秒。当LED等绿色时，RESET完成。 这将重置密码和网络参数。

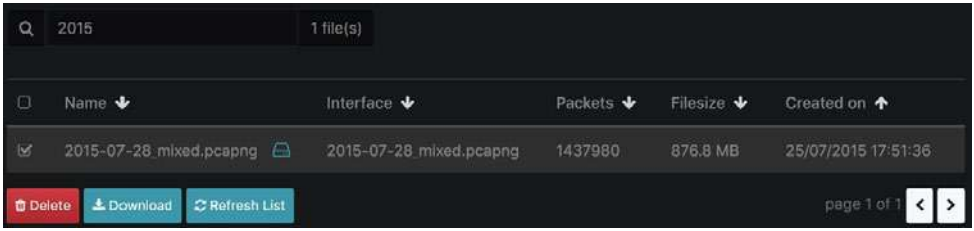
SHUTDOWN：按住10秒，设备安全关机。这将停止捕获并卸载内部磁盘，以结束捕获会话。

> 注意：在您要分析的网络中部署IOTA之前，请确保在'Interface Configuration' 中应用了适当的配置。

# 3.4 DATA VAULT

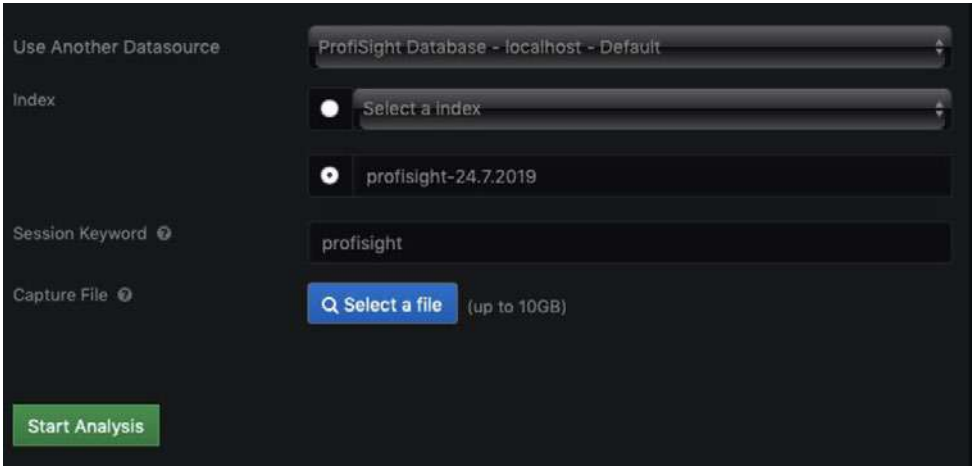
## Captured Files捕获文件

导航到Data Vault > Captured Files下载或删除原始PCAP-NG文件。选择一个或多个文件，然后点击'Download'按钮下载所选文件的.zip文档，或单击'Delete'按钮删除它们。




## Import a PCAP-NG（导入PCAP-NG）

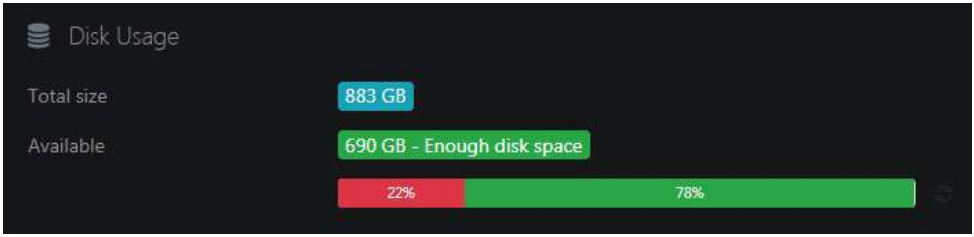
导入PCAP-NG或PCAP文件到IOTA可以通过点击'Select a file'按钮，选择文件，然后点击'Start Analysis'按钮。上传后，将仪表盘的时间范围设置为文件的时间范围，以确保图形显示正确的数据。



# 3.5 DATA MANAGEMENT数据管理

## Disk Usage

导航到Data Management > Capture Machine获得磁盘使用情况的概述，包括总磁盘大小和可用磁盘空间。




一个好的做法是每隔一段时间检查一下剩余的可用存储空间数量，并对是否需要进行清理进行评估，因为捕获和索引存在与可用空间有关的限制：

- 只有在至少5%的磁盘空间可用时，才能开始新的捕获。
- 只有在至少10%的磁盘空间可用时，才能开始数据库索引。如果已经在运行，如果剩余的磁盘空间少于10%，索引将停止。

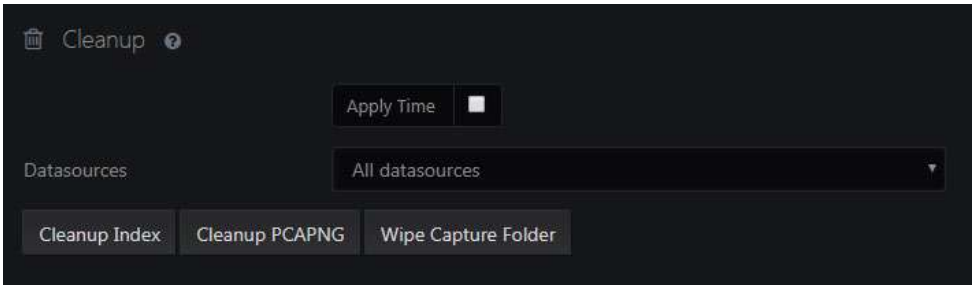
## Schedule a Cleanup安排清理

数据保留管理可在Data Management > Capture Machine > Schedule a Cleanup中使用。超过指定时间范围的捕获文件和索引将被定期删除。

## *Manual Disk Cleanup手动磁盘清理*

通过以下选项可以手动清理捕获文件和索引:

- Selective cleanup based on time
- Selective cleanup based on index
- Cleanup index or PCAP files or both



# 分析指南

## 4.1 DASHBOARD OVERVIEW仪表盘概览

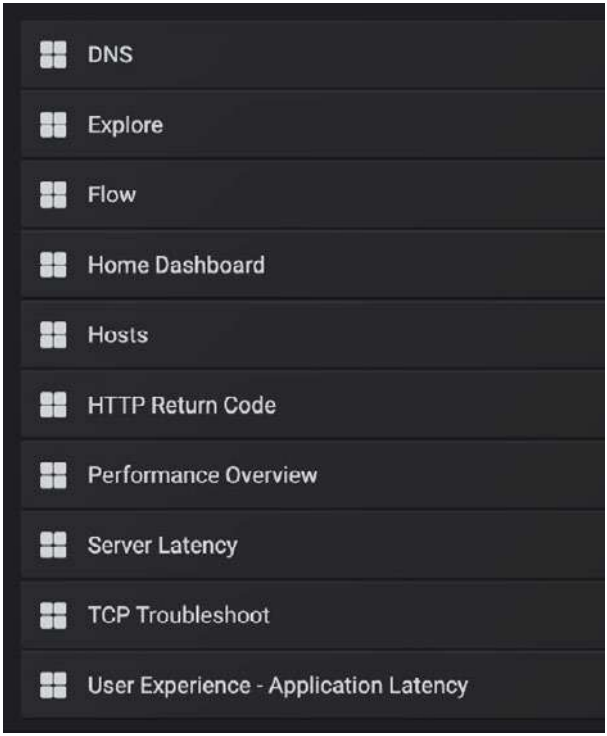

1. 主菜单
2. 登出
3. 主仪表盘选项
4. 时间范围选项
5. 仪表盘区域
6. 显示过滤器
7. PCAP文件下载
8. 带有过滤器和时间选项的仪表盘导航
9. 仪表盘配置

# 4.2 BASIC NAVIGATION基本导航

## Main dashboard selection menu主仪表盘选项菜单

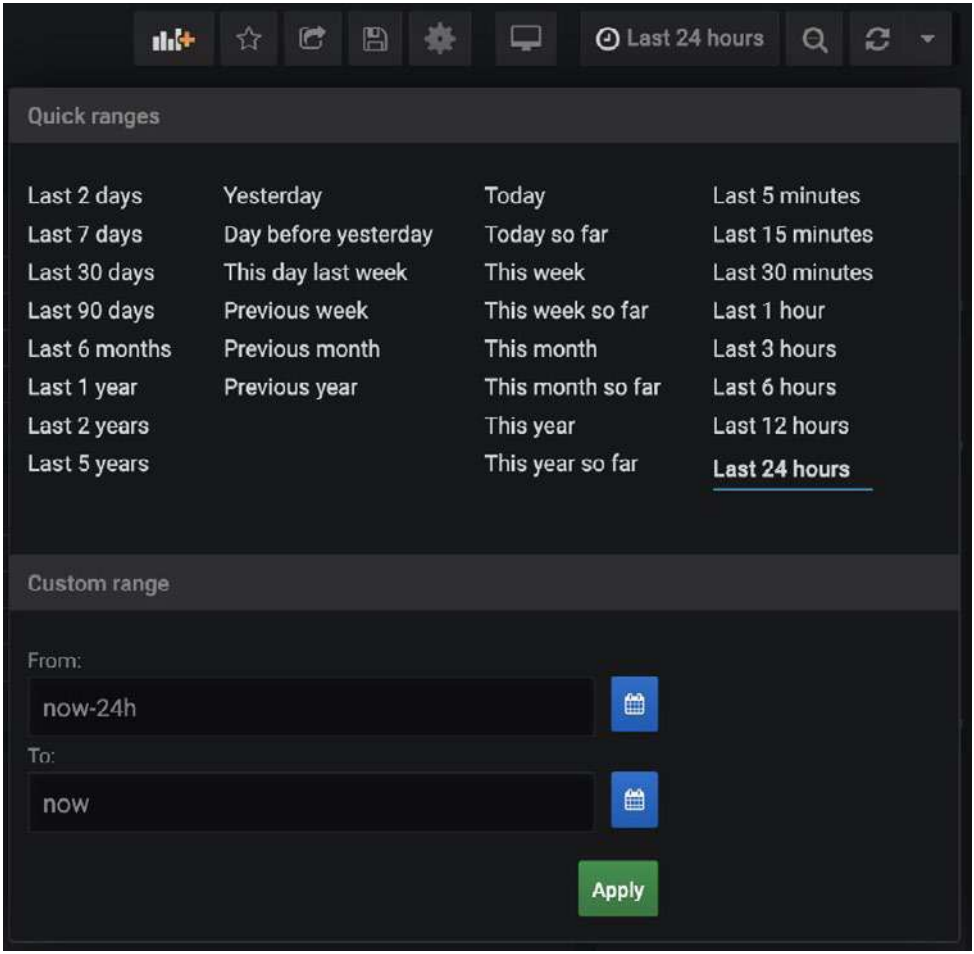
该菜单显示所有可用的仪表盘。仪表盘列表并非详尽无遗，会随着时间的推移而变化，以包括新功能和其他改进。

► 注意：从该菜单访问仪表板会重置当前仪表板中定义的时间选取器时间范围和显示过滤器。要在保持时间范围和过滤器设置的同时在仪表板中导航，请用'Goto >>'仪表板导航。



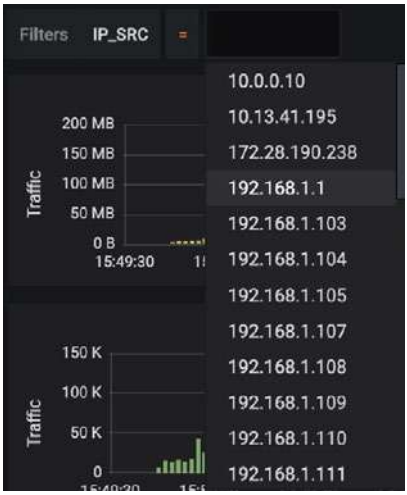
## *Time range selection**时间范围选项***

时间范围和自动刷新率可以在这个菜单设置。

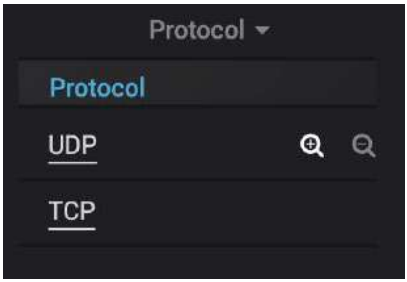


## *Filtering traffic过滤流量*

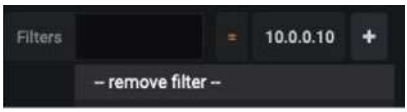
显示过滤器可以手动定义，通过点击Filter框（左上角）旁边的+图标，选择需要过滤的过滤器类型和值。




或者，在仪表板中，可以使用+放大镜图标（包括过滤器）或-放大镜图标（删除过滤器）来快速应用过滤器。

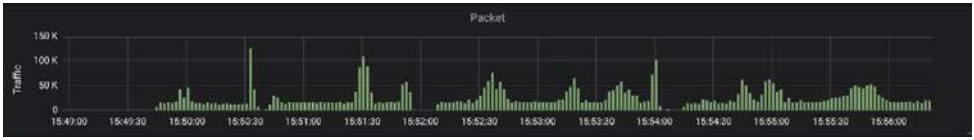



可以通过再次点击过滤器类型并选择'--remove filter--'来删除过滤器。

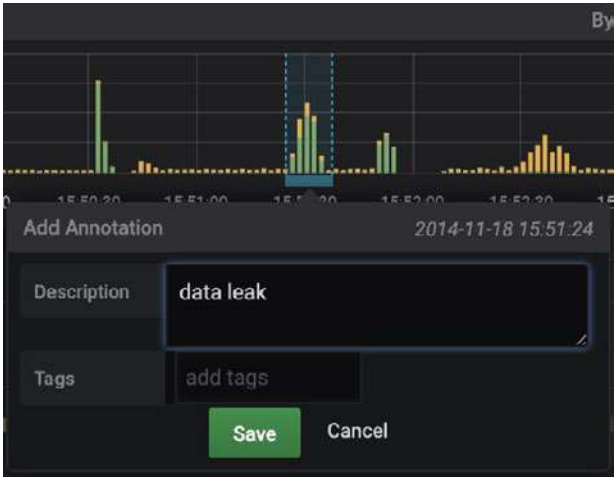


## *Graphs图表*

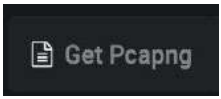
点击并拖动以放大特定的时间范围。




使用 CTRL/CMD + 鼠标拖动来给图形添加注释。



# 4.3 PCAP文件下载




使用任何仪表板右上角的 'Get Pcapng'按钮下载PCAPNG文件。

下载的PCAP文件的时间范围与时间选择器菜单中选择的时间范围一致。

以下过滤器也将适用于下载的PCAPNG文件：

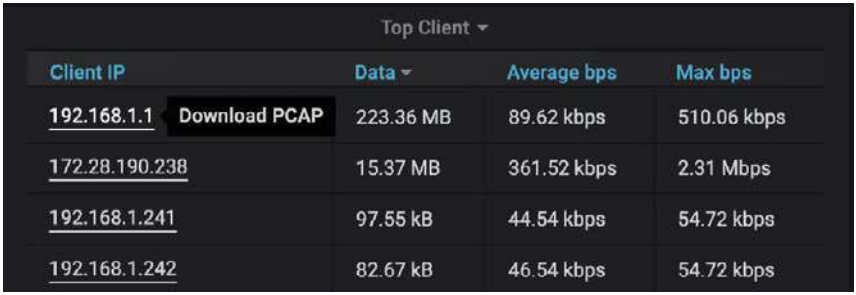
- IP address
- MAC address
- VLAN ID
- Protocol
- Port


如果选择了MAC地址、IP地址或端口，则过滤器会同时影响源和目的地。

下载PCAP文件的其他方法：

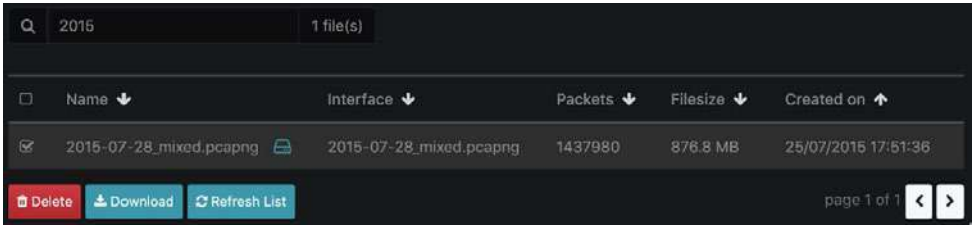
*1 - Use the direct download link使用直接下载链接*

点击任何链接都会启动PCAP文件传输，只用值过滤。此方法会忽略过滤器。



*2 - 从列表中下载原始PCAP-NG文件(Data Vault > Captured Files)*

文件或文件组以.zip存档的方式下载。





艾体宝科技有限公司

www.itbigtec.com
sales@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T (+86)400-999-3848

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港 | 日本 | 韩国



*版本：V1.0 - 22/11/14*


网络安全与监控方向
*(T: 135 3349 1614)*

*网络安全交流2群*

获取更多资料

itbigtec.com