



LINKRUNNER[®] AT 3000 & 4000 用户手册

点击 [点击](#) 直接进入相应章节。
向下滚动以查看完整的内容列表。

NetAlly 网络测试应用程序



自动测试



交换机



缆线测试



Ping/TCP



抓包



发现



路径分析



反射器



iPerf



Link-Live



应用商店

Contents

联系我们	11
介绍	12
如何使用本手册	13
模型之间的差异	16
按键和端口	18
充电和电源	21
PoE充电	21
安全与维护	24
法律通知	26
主页和安卓界面	27
主屏幕	28
导航系统	29
系统状态栏和通知	33
通知面板	33
应用程序屏幕和APP商店	36
设备设置	38
快速设置面板	38
使用Wi-Fi适配器	40
分享	41
分享截图	43
更改语言	44

LRAT 3000-4000设置和工具	46
导航区域	47
关于	47
导出日志	48
测试和管理端口	49
测试端口	49
选择端口	52
测试和端口状态通知	54
测试端口通知	54
管理端口通知	56
发现通知	56
PoE	57
VNC/远程Link-Live	57
LRAT 3000-4000常规设置	58
有线 常规设置	59
管理	60
首选项	63
趋势图	64
常用图标	68
浮动操作按钮 (FAB) 和菜单	69
常用工具	71
网页浏览器/Chromium	71
Telnet/SSH	71

软件管理	73
管理文件	74
文件应用	74
如何移动或复制文件	76
使用USB驱动器	77
弹出存储介质	78
使用 USB Type-C 转 USB 电缆	78
更新软件	81
远程访问	85
使用 VNC	86
使用 Link-Live 远程	86
管理NetAlly应用程序设置	88
重置测试应用程序默认值	88
保存应用程序设置配置	92
导出和导入设置	95
所有应用程序的导入/导出设置 ..	104
重新设置 LRAT 3000-4000 出厂设置	107
LRAT 3000-4000功能控制	109
功能访问简介	110
控制功能可用性	115
更改管理密码	120
LRAT 3000-4000测试应用	123

AutoTest 应用程序和配置文件	124
自动测试概述	126
管理配置文件和配置文件组	128
出厂默认配置文件	128
添加新配置文件	129
配置组	131
创建新的配置文件组	135
导入和导出自动测试配置	137
主自动测试屏幕	139
定期自动测试	141
定期自动测试设置	141
运行定期自动测试	143
DHCP, DNS, 和网关有线测试	146
DHCP 或静态 IP 测试	147
DNS测试	159
网关测试	163
测试目标 有线 测试	168
添加和管理测试目标	169
自动测试 Ping 测试	175
自动测试 TCP 连接测试	182
HTTP 测试	187
FTP测试	197
交换机应用	207

运行交换机	208
缆线测试应用	211
电缆测试设置	212
运行电缆测试	214
音调功能	221
将电缆测试结果上传到 Link-Live ..	225
Ping/TCP 测试应用程序	226
Ping/TCP 设置	227
从另一个应用程序填充 Ping/TCP ..	227
手动配置 Ping/TCP 设置	229
运行 Ping/TCP 测试	232
抓包应用	235
抓包设置	236
运行和查看抓包	240
发现应用	245
发现简介	247
主发现列表页	249
搜索发现列表	252
过滤发现列表	253
排序发现列表	256
安全审计——批量授权	259

刷新发现	264
将发现结果上传到 Link-Live	265
发现详细信息	267
顶部详细信息卡	270
设备详细信息中的下方选项卡 ...	273
问题	275
地址	276
TCP端口扫描	278
VLANs	280
端口	281
SNMP	286
连接的设备	288
资源	289
发现应用程序浮动操作菜单	290
设备类型	294
路由器	295
交换机	296
未知交换机	297
网络服务器	298
虚拟机管理程序	299
虚拟机	300
VoIP电话	302
打印机	303

SNMP 代理	304
NetAlly网络工具	305
主机/客户	306
设备名称和授权	309
为设备分配名称和授权	309
发现设置	319
主动发现端口	322
扩展范围	322
ARP扫描率	326
SNMP 配置	327
问题设置	338
TCP 端口扫描设置	341
路径分析应用	343
路径分析简介	344
路径分析设置	345
从另一个应用程序填充路径分析	345
手动配置路径分析	345
运行路径分析	348
路径分析结果和来源LRAT 卡	350
3层跳	352
二层设备	356
将路径分析结果上传到 Link-Live	360

反射器应用	362
反射器设置	363
运行反射器	368
iPerf 测试应用程序	371
iPerf 设置	373
保存自定义 iPerf 设置	373
发现中的测试配件	374
配置 iPerf 设置	377
运行 iPerf 测试	380
将 iPerf 结果上传到 Link-Live	384
Link-Live 云服务	386
Link-Live 云服务入门	388
注册设备	388
注册后	390
取消注册	390
AllyCare 激活码	391
私有 Link-Live 设定	392
Link-Live 应用程序功能	393
仅在本地保存	396
工作评论	398
Link-Live 和测试应用程序	401
Link-Live 共享屏幕	401

共享文本文件到 Link-Live	405
规格和合规性	408
LRAT 3000-4000 规格	409
规格	409
环境指标	410
索引	411

联系我们

网址: NetAlly.com

电话: (North America) 1-844-TRU-ALLY
(1-844-878-2559)

NetAlly

2075 Research Parkway, Suite 190
Colorado Springs, CO 80920

如需客户支持, 请访问
NetAlly.com/Support.

注册您的 **LRAT 3000-4000**

注册您的产品 NetAlly 使您可以访问有关产品更新、故障排除程序和其他服务的宝贵信息。

在 [NetAlly 技术支持页面](#)。

介绍

它具有由 NetAlly 开发的用于网络发现、测量和验证的应用程序，这些应用程序可从 [主页](#) 和 [应用](#) 屏幕获取。

所有的 NetAlly手持式测试仪都提供在 [Link-Live.com](#) 上访问 Link-Live 云服务。Link-Live 是一个云平台，用于收集、组织、分析和报告您的测试结果。一旦您的测试仪配置正确，测试数据就会自动上传。访问 [Link-Live.com](#) 并 "关联" 你的 LRAT 去访问这些功能。

如何使用本手册

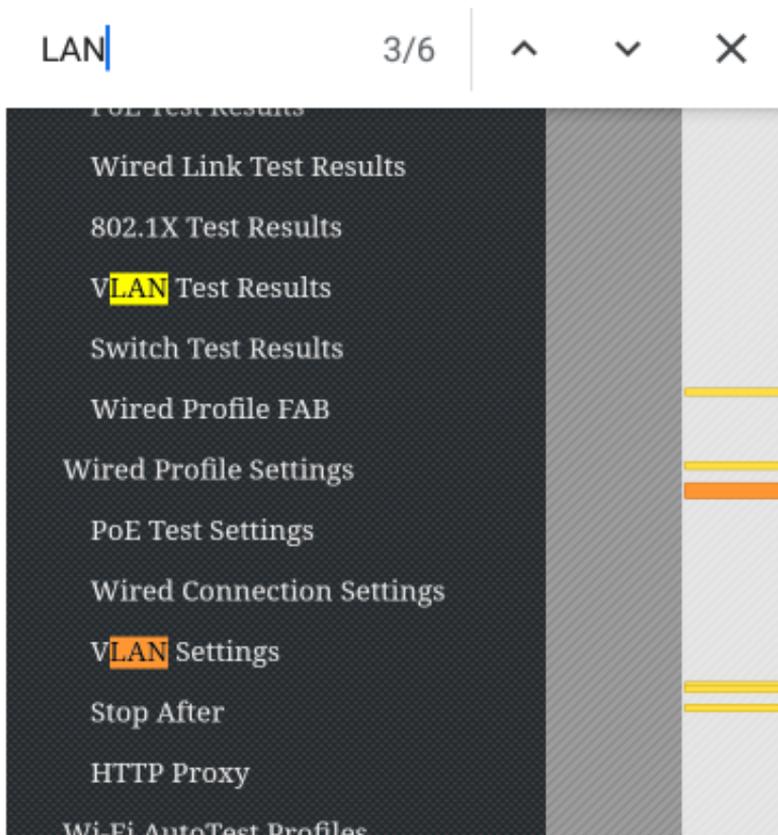
本用户指南描述了 LRAT 3000-4000 的测试功能和系统界面的基本元素。

该手册适用于熟悉网络操作、测试和测量的用户。

此 LRAT 3000-4000 也可以称为只是 LRAT 或本手册中的“单位”。

- 点击 [蓝色链接](#) 去文档的目的地。 [蓝色链接下面](#) 打开外部链接。
- 点按左侧列表中的书签可前往相应版块。
- 点击下面标题里的 [内容](#) 并从第 2 页开始的列表转到相应的部分。
- 搜索单词或短语：
 1. 点击浏览器菜单  右上角的图标。
 2. 选择菜单选项里 **查找页面**
 3. 输入搜索文本。
 4. 点击查找图标 。这将在屏幕顶部显示文本。触摸向上和向下箭头可向前和向后搜索文本。在下图中，用

户搜索了“LAN”。点击右侧的高亮条可转到相应的手册文本。



在线和本地版本的本指南和视频。

- 手册也可在以下位置下载：
<https://www.netally.com/support/user-guides/>

- 要在您的 LRAT 3000-4000上观看用户指南, 您必须连接互联网。当您点击 **指南 > 用户指南** (在 "**主屏幕**" on page 28上), 本指南就会下载并在您的设备上显示。
- 在将用户指南下载到您的设备后, 指南会存储在浏览器的本地缓存中。您无需重复下载, 除非您 **更改了设备语言** 或清空了浏览器缓存。
- 主屏幕上的"指南"图标(用于访问本指南)还提供了访问特定产品的培训和信息视频的功能。

本指南的国际版本

我们提供了中文或英文版本的 LRAT 3000-4000 用户指南, 您可以 **切换设备语言** 为以下语言之一。如果您将语言更改为德语、日语或韩语, 将使用英文用户手册。

模型之间的差异

您的 LRAT 的型号号码显示在 "关于" 屏幕上, 并且印刷在设备的背面面板上。本手册涵盖所有型号, 并识别每个型号特定的功能 (如果有差异的话)。总体而言:

LINKRUNNER-AT-3000, LINKRUNNER-AT-4000

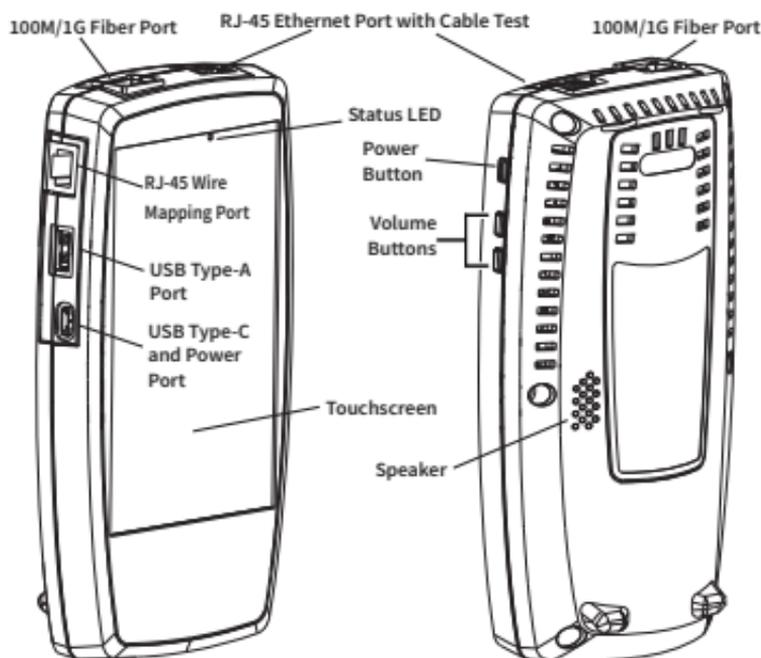
- LinkRunner-AT-3000:
 - 不包括 Capture、Discovery、iPerf 或 Path Analysis 应用程序。
 - 不支持定期自动测试。
 - 在自动测试中不支持 HTTP/FTP 目标。
 - 购买价格不包括 AllyCare 订阅。
 - 在使用应用市场之前需要注册。
- LinkRunner-AT-4000:
 - 包含 Capture、Discovery、iPerf 和 Path Analysis 应用程序。
 - 支持定期自动测试。
 - 在自动测试中支持 HTTP/FTP 目标。
 - 包含了一年的 AllyCare 订阅。

- 在使用应用市场之前不需要注册。

关于更多产品信息请参考 [LRAT 3000-4000 规格](#)。

按键和端口

您的设备 LRAT 上的按键和端口功能如下所述。



功能

描述

状态 LED

红色:设备关闭, USB-C电源适配器已连接

绿色:设备开机, 屏幕关闭 (无论是否连接电源适配器)

LED(红色或绿色)闪烁频率表示电池充电百分比:

- 每1秒2次闪烁:电池电量低, 充电量为0-24%

功能	描述
	<ul style="list-style-type: none"> • 每1秒1次闪烁:充电量25-49% • 每2秒1次闪烁:充电量50-74% • 每4秒1次闪烁:充电量≥75% • 无闪烁:电量已充满
RJ-45 线路映射端口	用于环回电缆测试的内部线路映射器端口
带有电缆测试功能的 RJ-45 以太网端口	通用端口,用于连接网络、运行电缆测试,包含了音频和闪烁端口功能 支持PoE(与兼容的设备硬件配合使用)
USB Type-A 端口	可连接到任何 USB 设备(仅在需要手动软件更新时需要 FAT32 格式的设备)
USB Type-C On-the-Go 端口	连接到 USB Type-C 连接器,用于文件传输,并连接到附带的交流适配器以为设备充电
音量按键	增大或减小外部蓝牙或 USB 扬声器或耳机的音量
电源按键	长按以显示菜单 关机 或 重启
扬声器	产生音频

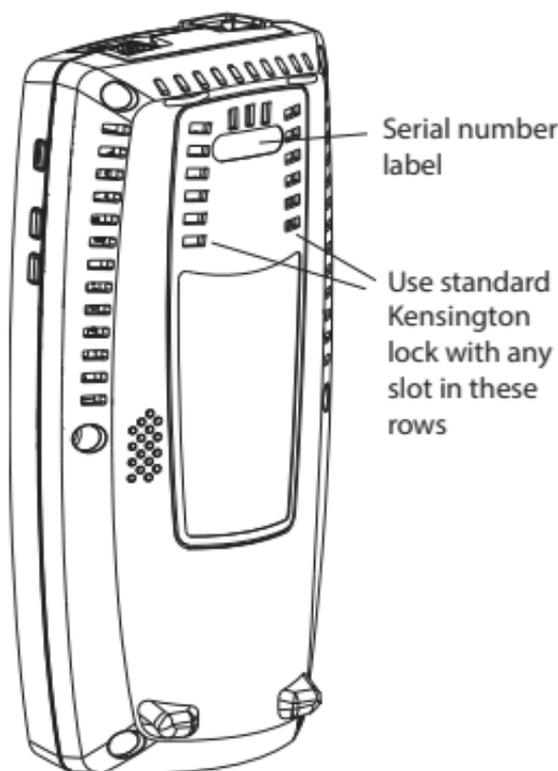
参阅 [测试和管理端口](#) 以获取有关端口功能的详细说明。

参阅 [更新软件](#) 以获取更新系统软件的要求。

如有需要, 请参考产品的 [规格](#)

使用 Kensington 锁

设备的后面板在序列号标签的两侧有两行共六个通风孔。您可以在这两行通风孔中的任意一个插槽上使用标准的Kensington锁。



充电和电源

您的 LRAT 3000-4000 包含了一个 USB-C 15V/3A 电源适配器。

⚠️ 注意: 仅支持 NetAlly 提供的电源适配器

要开始给内部锂离子电池充电, 将附带的电源适配器插入交流插座, 并插入设备左侧的 USB-C 充电端口。当设备处于充电状态时, 电源按钮会变为红色, 在充满电后会关闭。请参考 [规格](#) 以查阅有关电池运行时间和充电时间的信息

在充电模式下(设备关闭但插入交流电源), 设备每 24 小时打开一次并给电池充电, 然后再关闭电源。

PoE 充电

以太网供电(PoE)可以为您的设备提供替代电源, 为设备的电池充电。(对于包含了通过 PoE 为电池充电选项(在 [通用设置](#) 中)的测试设备, 也支持 PoE)

- 经过协商的 PoE 类别 3-8 (≥ 15.5 W) 提供足够的电力来持续运行测试设备并给电池充电。

- 经过协商的PoE类别 0-2 ($\leq 6.4\text{ W}$) 提供一定的电力以延长电池的运行时间,但不足以给电池充电。

请按照以下步骤启用PoE充电：

1. 将设备上方的RJ-45端口连接到支持PoE的网络交换机或PoE注入器上。
2. 确保设备处于开机状态或显示休眠模式。
3. 如果您的测试设备显示通过**PoE**为电池充电选项(在[通用设置](#)中),点击设置以启动PoE充电。
4. 要检测PoE的可用性,可以运行带有通过PoE测试的[AutoTest有线配置文件](#) (**PoE**测试必须启用,并配置为受您的交换机或PoE注入器支持的供电设备类别)参阅[有线配置文件的设置](#)和[有限配置文件的的结果](#).

注意:如果AutoTest应用程序当前未打开,则在您开启设备或LRAT检测到顶部[有线测试端口](#)中的新铜链路时,将自动运行配置文件列表中的最后一个有线配置文件。

参阅[按键与端口](#)以查阅端口位置和描述。

开机

- 要开启设备, 按住电源按钮约一秒钟, 直到 和状态LED 变成绿色。
- 当显示屏进入休眠模式时, 电源按键LED 保持亮起。状态LED会闪烁绿色以指示电池电量。轻触电源按钮即可唤醒显示屏。(您可以在设备设置  设备设置 中设置显示屏休眠和自动关机的时间)
- 关机或重启, 长按电源键一秒, 直到触摸屏出现“关机”和“重启”对话框, 然后点击 关机 或者 重启。
- 如果设备对正常关机没有反应, 请按住电源按钮五秒钟以执行硬关机。

安全与维护

请遵守以下安全信息：

仅使用提供的适配器 或以太网供电 给电池充电。

确保适配器易于访问。

使用正确的端子和电缆进行所有连接。

⚠警告：为避免可能发生的电击或人身伤害，请遵循以下准则：

- 如果产品损坏，请勿使用。在使用产品之前，请检查外壳，并寻找破裂或缺失的塑料。
- 请勿在爆炸性气体、蒸汽或灰尘周围操作本产品。
- 请勿尝试维修产品。没有可维修的部件。
- 请勿更换电池。如果电池更换为不正确的电池类型，则存在爆炸风险。
- 按照您所在机构的处理说明处理电池组和电子设备。
- 按照指示使用。如果以制造商未指定的方式使用本产品，则可能会削弱产品提供的保护。

安全标志



警告或注意：设备或软件损坏或毁坏的风险。



警告：电击危险。



不适用于连接到公共电话系统。

清洁设备

要清洁显示屏，请使用镜头清洁剂和柔软的无绒布。

要清洁外壳，请使用蘸有水或弱肥皂的软布。

深色塑料上的划痕可以通过以下方法去除轻轻的用毛刷将牙膏与水的 1:2 混合物擦洗到受影响的表面。

⚠警告：请勿使用可能损坏产品的溶剂或研磨材料。

法律通知

使用本产品需要接受条款和条件, 请访问 <http://NetAlly.com/terms-and-conditions> 或发货时产品随附, 或 NetAlly 与此产品购买者之间签署的法律协议(如果适用)。

开源软件确认: 本产品可能包含开源组件。
NetAlly 将在 Link-Live.com/OpenSource。

上提供该产品的开源代码组件(如果有)。
NetAlly 保留自行决定随时更改其技术信息、规格、服务和支持计划的权利。

© 2019-2022 NetAlly

主页和安卓界面

本章介绍如何使用系统主屏幕和用户界面的功能来导航和设置您的设备。

此 LRAT 3000-4000 界面支持任何手持式设备的许多典型操作。使用拖动和 [滑动](#) 在触摸屏上移动以浏览应用程序、打开侧边菜单、向下拖动 [通知面板](#) 从主屏幕顶部的状态栏，或向上拖动 [Apps](#) 屏幕从底部。

主屏幕

与其他手持式设备一样，您的 LRAT 3000-4000 主屏幕是可定制的。上图显示了默认配置，但您可以添加、删除和重新组织应用程序图标和小部件以满足您的目的。

您还可以通过点击、按住应用程序图标并将其从主屏幕向右拖动来创建更多主页。

参考 [Apps 页面](#) 部分，了解有关向主页添加更多应用程序的说明。

导航系统

您可以用在屏幕和面板之间进行切换的方式,在 LRAT 3000-4000 上进行导航操作,这与许多其他手机或平板设备的导航方式相似。

主要设备导航按钮出现在触摸屏底部。



后退图标返回上一屏幕。



圆圈图标打开主屏幕。



方形图标显示您最近使用的应用程序,以便在它们之间轻松切换。这也是您可以关闭或停止打开的应用程序的屏幕。

提示:双击方形图标可切换回您之前使用的应用程序并在两个应用程序屏幕之间来回切换(如测试应用程序和本用户指南)。

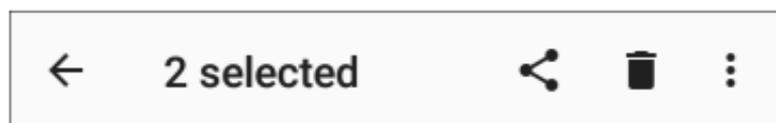
滑动

触摸并拖动手指或向上、向下、向左和向右“滑动”以浏览[主屏幕](#)和应用程序的页面,向上滚动或向下,然后拉出导航抽屉和面板。

长按

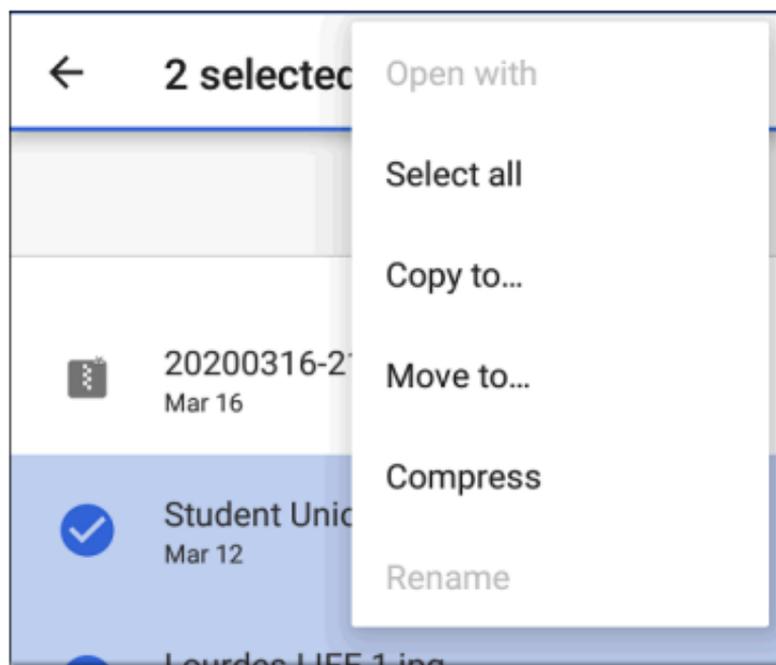
触摸并按住或“长按”文件或应用程序图标以显示其他操作。

例如，您可以在长按一个文件名在 [文件应用](#) 显示带有选项的顶部工具栏 [分享](#) 、删除或移动文件。



附加选

项通常出现在溢出菜单中，由操作溢出图标指定 。



您还可以在大多数屏幕上长按文本以打开复制和[分享](#)文本。

左侧导航栏

在[文件](#)  app, 点击菜单图标 或者 或向右滑动以打开导航抽屉。它显示文件系统中的文件夹。

☰ **LinkRunner AT** 🔍 ⋮

LinkRunner AT

 Images

 Audio

 Videos

 Documents

FILES ON LINKRUNNER AT



 Alarms

 Android

 Audiobooks

 DCIM

 Documents

注意:在文件应用程序中,您可能需要点击操作溢出图标  在右上角并选择显示内部存储 导航到**LinkRunner AT** 文件夹和子文件夹, 如上图.

See the [导航至目录](#) 了解更多信息.
[返回标题和目录](#)

系统状态栏和通知



屏幕顶部的状态栏显示来自系统的通知图标以及 LRAT 3000-4000- 与您的网络连接和测试状态相关的特定图标。

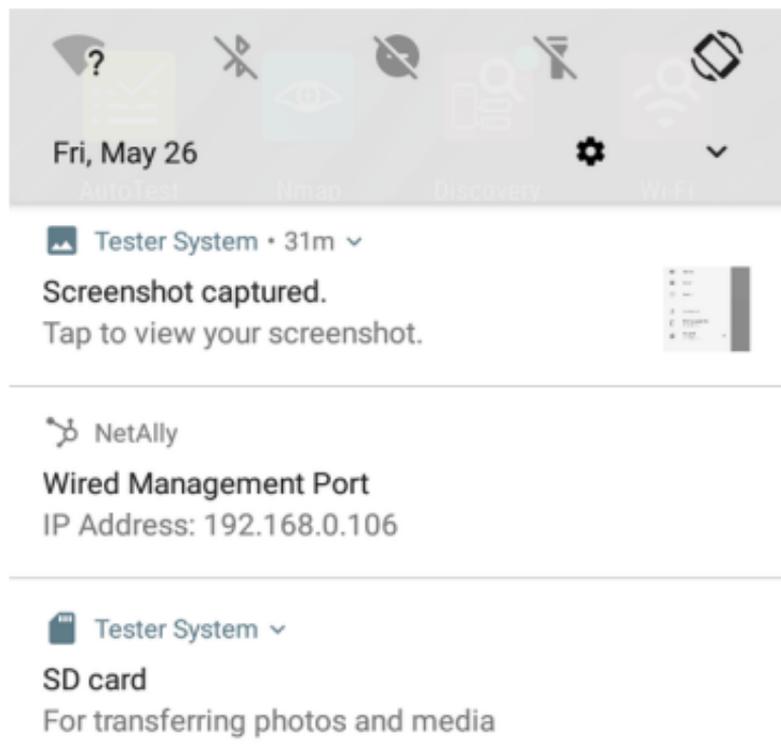
参照 [测试和端口状态通知](#) 有关图标和通知的详细信息 LRAT 3000-4000网络连接、测试和管理。

触摸并向下滑动状态栏以打开通知面板。

通知面板

通知面板包含来自您设备的通知，例如下载和安装、插入的硬件、捕获的屏幕截图、应用程序和连接状态以及更新。该面板还显示常见的系统设置图标以便快速访问。

在屏幕最顶部的状态栏上向下滑动(触摸并拖动)以向下滑动通知面板。



- 触摸标题和向下箭头 \checkmark 在通知上(或向下滑动)以展开框并查看更多详细信息或选项。
- 轻触通知中间可打开相关应用、图片或设备设置或执行其他相关操作。
- 在通知上向左滑动以关闭它。

注意:因为它们对于 LRAT 测试功能,您不能关闭测试和管理端口-相关的测试和端口状态通知。

- 点击清除所有在面板的右下方关闭所有系统系统通知。

应用程序屏幕和APP商店

要访问未显示在主屏幕上的应用程序，请在主屏幕上向上滑动或触摸向上箭头图标。

应用程序屏幕显示您设备上的所有应用程序。上图是一个例子。您的应用程序屏幕可能包含不同的第三方应用程序。

- 点击应用程序的图标以打开该应用程序。
- 按住并向上拖动图标以将其添加到主屏幕。
- 触摸并按住(长按)图标以查看应用程序信息或访问您可以添加到主屏幕的小程序以及您可以执行的其他操作。

App 商店

注意：LinkRunner AT 3000 要求您先[注册产品](#)，然后才能访问 App Store。

从主屏幕或应用程序屏幕，打开NetAlly App Store 下载第三方装置应用程序以在您的设备上使用LRAT 3000-4000.

注意：您的设备必须“捆绑”为 [Link-Live云服务](#) at [Link-Live.com](#)访问应用程序商店。

- 点击搜索图标以搜索应用程序.
- 点击 **升级** 查看已安装应用程序的可用更新.
- 要请求将 App 添加到 App Store, 请访问 Apps ► 在 [Link-Live.com的页面](#), 并选择浮动操作按钮 (FAB) 在右下角 申请 or 上传应用.

设备设置

要访问 系统设备设置，请触摸设置  底部的图标 [主屏幕](#)。

使用设备设置屏幕调整显示、声音和日期/时间；查看已安装的应用程序和内存设备；[连接到Wi-Fi](#)；or [重置为出厂默认值](#)。

快速设置面板

您还可以通过从快速设置面板向下滑动来访问一些最常见的设备设置，例如 [Wi-Fi](#)。[状态栏](#)在触摸屏的顶部。

向下滑动两次以打开完整的快速设置面板。

- 触摸并拖动面板顶部的滑块控件以调整屏幕亮度。
- 点击面板中的图标以启用或禁用相应的功能。
- 点击铅笔图标  在快速设置面板底部配置面板中显示的图标控件。

自动关机

激活自动关机功能有助于延长电池运行时间。

1. 从设备设置 , 选择 显示。
2. 在显示设置界面, 点击设备自动关机。
3. 在弹出的对话框中, 选择您希望设备在不发生任何活动的情况下保持开启状态的时间。选定的不活动时间过后, 设备会自动关闭电源。

同样, 您可以调整控制显示何时进入的设置休眠模式来自显示设置屏幕。

语言

您的设备支持英文、日文和中文显示。参考 ["更改语言" on page 44](#) 有关更改语言的信息。

使用Wi-Fi适配器

LRAT不支持Wi-Fi或蓝牙功能。如果您尝试使用系统界面启用这些服务，它们将立即关闭。然而，要想连接到Wi-Fi，您可以使用支持的外部USB适配器。该适配器需要单独购买。

在使用时，USB转Wi-Fi适配器的行为类似于另一个网络连接。

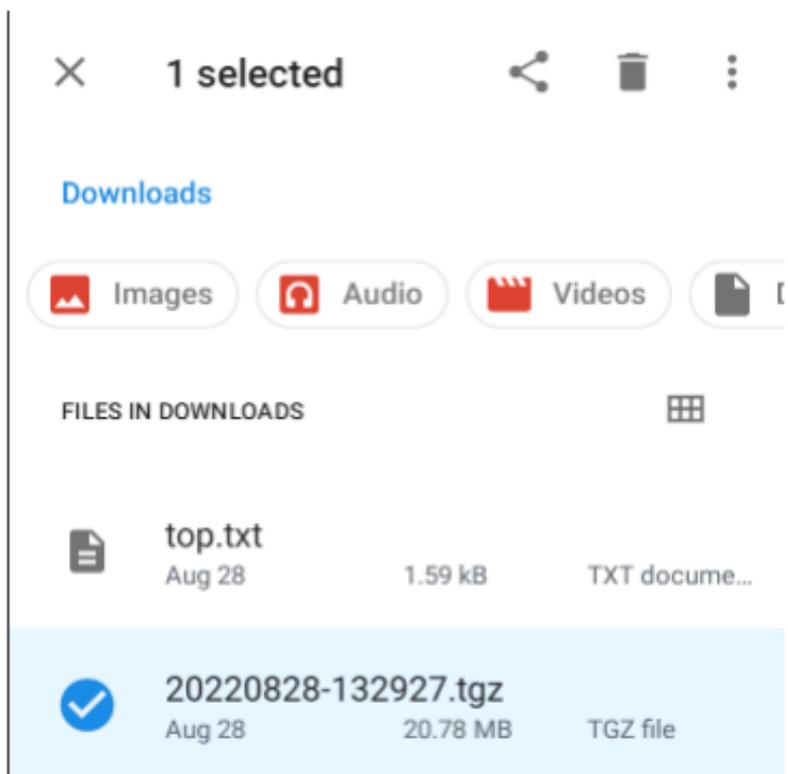
有关更多信息，请参阅 [支持的Wi-Fi/蓝牙适配器](#)。

分享

系统文件  应用程序可让您将文件从内部或外部存储共享到蓝牙打印机或 Link-Live 云服务。您可以一次上传一个或多个选定文件。

注意：设备上的许多应用程序允许您将设置和配置信息直接保存到 Link-Live。请参阅 [保存应用程序设置和配置](#)。

1. 在主屏幕上，点击图标 打开文件应用程序 。
2. 使用导航菜单  或 [左侧导航抽屉](#) 导航到包含要共享的文件的文件夹。
3. 长按选择一个或多个文件。



4. 点击顶部工具栏中的分享图标  以打开分享弹出对话框。
5. 点击选择共享方式, 按照系统提示共享文件。
6. (可选) 如果上传到 [Link-Live 云服务](#):
 - a. 点击 Link-Live  选项。
 - b. 输入您想要附加到文件的任何评论。

- c. 选择 保存至上次测试结果或保存至已上传文件。然后，您的文件将上传并可在 Link-Live.com 上查看。
- d. 有关将 [Link-Live](#) 与您的 结合使用的更多信息，请参阅 [Link-Live 章节LRAT 3000-4000](#)。

分享截图

截取并分享屏幕截图：

1. 同时按住电源按钮和音量降低按钮一秒钟。(请参阅[按钮和端口](#)了解按钮位置)。设备发出蜂鸣声并将通知添加到[通知面板](#)。
2. 通过打开通知面板并点击屏幕截图通知或使用文件应用程序来访问该文件。
3. 按照[共享程序](#)使用 [Link-Live](#)、蓝牙或其他配置的应用程序共享图像。

更改语言

注意：LRAT 3000-4000从 1.1 版开始支持日文

1. 要更改界面语言，请转到[设备设置](#)通过触摸设置  主屏幕底部的图标。
2. 在设置屏幕上，向下滚动并选择系统部分，然后，语言 & 输入。
3. 关于语言 & 输入屏幕，触摸语言。
4. 在语言首选项屏幕上，选择+ 添加语言。
5. 轻触以选择所需语言选项的名称。
6. 在语言首选项屏幕上，触摸语言右侧的图标，然后将所需的语言选项拖到列表顶部 (1) 的位置。



此LRAT按语言首选项屏幕上显示的优先级顺序显示可用的所选语言。

LRAT 3000-4000设置和工具

LRAT 3000-4000具有一套通用的工具和[常规设置](#)适用于多个NetAlly应用程序和测试行为。本章涵盖了特定于LRAT 3000-4000。

(参考[设备设置](#)有关 Android 系统设置的信息的主题。)

访问通用设置和信息屏幕NetAlly通过打开左侧导航抽屉来测试应用程序(如 AutoTest 或 Capture)  或设置 。

导航区域

许多系统应用程序,包括 NetAlly 测试应用程序,在从屏幕左侧滑出的“导航区域”中包含其他设置、工具和信息。

要打开导航区域:

- 点击菜单图标  在一个测试申请屏幕的左上方。
- 触摸并从应用程序屏幕的最左侧向右拖动(滑动)。

例如, AutoTest 导航区域(上图)提供了对启用的 [自动测试配置文件](#),自动测试设置,[常规设置](#),以及关于屏幕。

应用程序章节中描述了每个特定应用程序的设置。

关于

关于屏幕显示您的序列号、MAC 地址、软件版本、SFP 详细信息和当前的 AllyCare 合同状态。LRAT 3000-4000.

如果一个用户定义的 **MAC**在 NetAlly apps' [常规设置](#) 或在 [有线配置设置](#), (User-defined) 出现在“关于”屏幕上的 MAC 地址旁边。

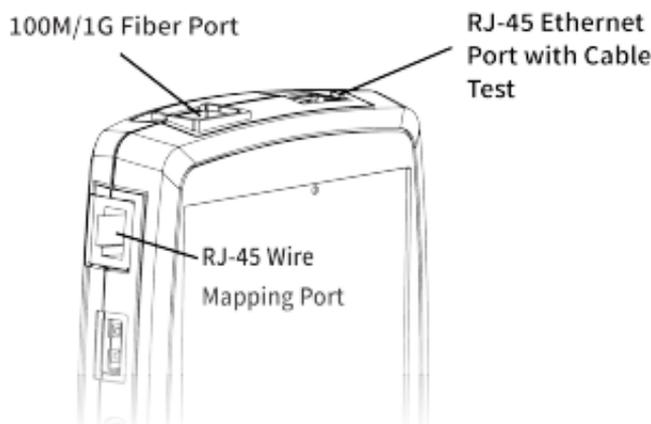
导出日志

关于屏幕包含导出日志功能，它允许您保存设备的日志以供分析 NetAlly 的技术支持团队。

触摸导出日志“关于”屏幕上的链接将 .tgz 文件下载到您设备上的“下载”文件夹。打开[文件](#)应用程序使用电子邮件或其他方法传输文件。(参考[管理文件](#).)

测试和管理端口

The LRAT 3000-4000 有两个有线RJ-45铜端口和一个光纤端口, 每个铜端口具有本节中描述的特定测试或管理功能。



有关端口的更多信息, 请参阅以下部分. 参考 [按钮和端口](#) 和技术 [规格](#).

测试端口

 **有线铜口:** 铜质测试端口是设备顶部的RJ-45端口。要禁用, 请拔下连接。

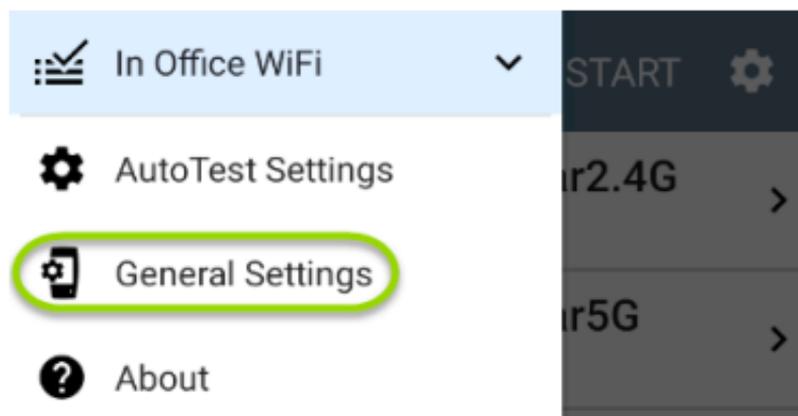
 **有线光纤测试端口:** SFP 和光纤测试端口也在设备顶部。要禁用, 请拔下连接。

注: 如果顶部光纤和铜端口都连接到活动网络, 则 LRAT 使用光纤链路作为有线测试端口连接。

LRAT 运行, 抓包, 发现, 和其他全面的网络分析在测试端口上的应用. Wi-Fi 测试无线电主要由应用程序中的设置控制, 尤其是 AutoTest.

您还必须运行自动测试有线配置文件以在有线测试端口上建立链接。如果 AutoTest 应用程序当前未打开, 配置文件列表中的最后一个有线配置文件会在您打开设备电源时自动运行或 LRAT 在顶部检测到新的铜链路 **有线测试端口**. 有线光纤连接必须手动启动 **自动测试 app**.

请注意, **常规设置** 影响您如何使用测试端口. (常规设置可从大多数 NetAlly 测试应用程序的左侧导航访问.)



 管理端口



USB有线管理端口:您可以使用USB转以太网适配器为您的 LRAT运行备用有线管理端口。该选项允许您建立一个稳定的有线连接,用于 [系统更新](#), [软件更新](#), 与 [Link-Live](#)通信, AP上行, 以及运行基本有线测试, 以帮助诊断可能影响Wi-Fi设备的问题。

注意:NetAlly已经测试了许多USB转以太网适配器与 LRAT 3000-4000的适应性, 但并非全部。以下适配器得到支持:

- j5create 型号 JUE130 (USB 3.0)
- StarTech.com 型号 USB21000S

需要更多信息, 参阅 [以太网适配器和摄像头](#)。

请联系 [NetAlly支持t](#) 如果您需要获取更多详细信息。

要设置适配器接口, 请按照以下步骤操作:

1. 将适配器插入设备上的一个USB Type A 端口。
2. 使用网络RJ-45电缆将适配器连接到网络。

3. 确认适配器上的LED指示灯亮起。这表示连接已激活。
4. 在 [测试和端口状态通知](#) 中，验证USB有线管理端口是否现在被列为管理端口。

现在，您可以在以下应用程序中使用USB有线接口：

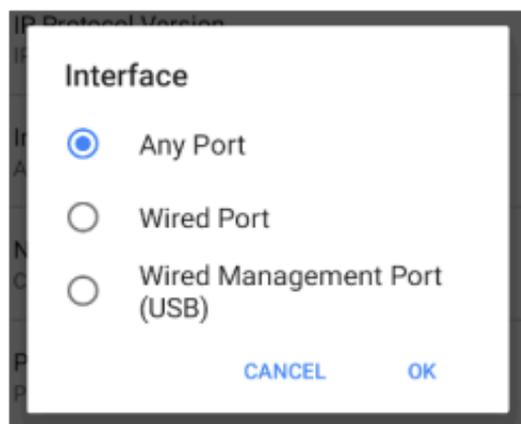
- Discovery(主动发现端口和TCP端口扫描)
- Ping(网络连通性测试)
- 路径分析

有关更多信息，参阅下方的 [选择端口](#)。

选择端口

个别的一些 NetAlly 测试应用程序允许您选择用于测试或分析的端口接口。例如：

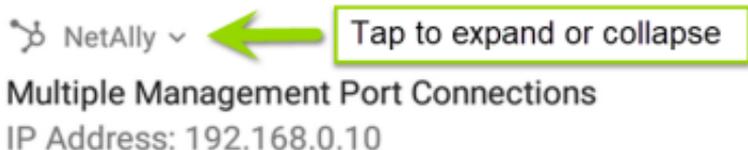
要更改端口，请点按应用的设置图标  显示设置屏幕。然后单击 **端口** 选择端口。



测试和端口状态通知

LRAT 3000-4000 将显示来自 NetAlly 测试应用程序和单元端口的通知，显示在顶部状态栏和 [通知面板](#) 中。向下滑动状态栏可查看通知。

在每个通知上，您可以点击标题和向下箭头以展开框并查看更多详细信息或选项。



以下 LRAT 图标可能会出现在您的状态栏中，并具有如下描述的含义。

注意：参阅 [测试和管理端口](#) 获取端口功能的描述。

另见 [常规设置](#) 获取控制端口功能的设置。

测试端口通知

测试端口上的活动网络连接使用了 [自动测试](#) 应用。



您可以通过运行自动测试有线配置文件,从而设置一个有线测试端口连接(在应用程序设置中称为“有线端口”)

注意:如果光纤端口和顶部铜缆端口都连接到活动网络,则LRAT使用光纤链路作为“有线端口”进行测试。

 NetAlly ▾

Wired Port

Speed: 1 G FDx

IP Address: 10.250.2.191



定期自动测试正在运行或已完成。当定期自动测试运行时,有线测试端口可能不可用于其他测试应用程序。

注意:此功能仅适用于LRAT-4000。

 AutoTest ^

Periodic AutoTest Running

Passed: 3

Failed: 2

Skipped: 1

Time Remaining: 54 m

管理端口通知

 您可以建立一个管理端口连接, 通过可选的USB转Wi-Fi适配器。

 NetAlly

Wired Management Port

IP Address: 192.168.0.123

 备用的有线管理端口连接可以通过可选的USB转以太网接口建立。其详细信息显示在系统管理端口通知下方。参阅 [USB有线管理端口](#) 获取更多信息。

如果管理连接丢失, 将显示以下通知。

 now

No Management Port Connection

发现通知

注意: 此功能仅适用于LRAT-4000。

发现通知显示发现过程的进度。参阅 [发现应用程序](#) 章节获取更多信息。

 当前正在运行的主动发现过程已经达到指定的百分比。



当前没有可用于主动发现的链接,可能是因为没有任何 启用发现功能的端口连接,或者正在运行AutoTest。当AutoTest正在运行时,发现功能会被临时禁用。

PoE



表示您的设备已连接到Power over Ethernet电源。参阅 [PoE充电](#) 获取更多信息。

VNC/远程Link-Live



远程VNC连接已通过独立的VNC客户端和/或 [Link-Live云服务](#) 中的远程功能激活。

 NetAlly ^

Remote Connected

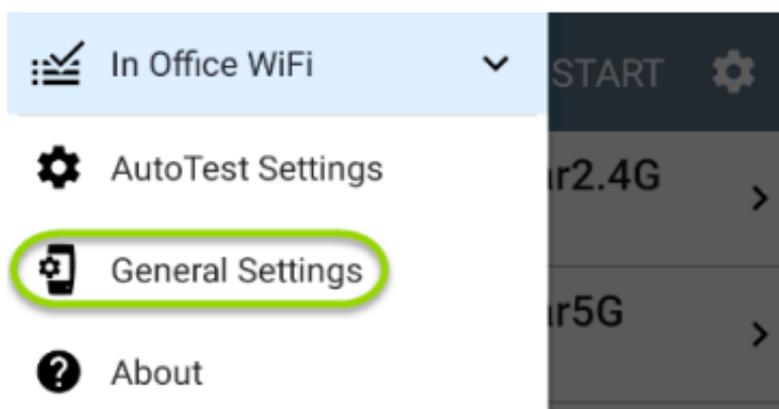
Clients

10.0.0.14

LRAT 3000-4000 常规设置

LRAT的常规设置控制影响多个测试应用程序的测试和管理相关连接。

从常规设置左侧导航区域  在NetAlly测试应用程序，例如 AutoTest、Discovery、Capture、iPerf 等。



See also [测试和管理端口](#) and [测试和端口状态通知](#) 有关端口功能和状态图标的相关信息。



有线常规设置

有线常规设置功能 [有线测试端口](#)。

在链路连接前测试 **POE**:默认情况下,自动测试 [有线配置文件](#) 在 PoE 测试完成之前执行链路测试。启用此设置以使您的 LRAT 在链路测试之前完成 PoE 测试。启用此设置会强制在建立链接之前完成 PoE 协商,从而提高与某些交换机的兼容性。

通过 **PoE** 为电池充电:(如果测试仪硬件支持,则可用。)此设置默认启用。如果您不希望 LRAT 装置在连接到具有 PoE 的交换机时充电,请点击切换按钮以禁用。**AutoTest XXX** [有线配置文件](#) XXX 必须运行并检测 PoE 可用性,然后装置才能使用它进行充电。

另请参阅 [PoE 充电](#)。

只接收:启用此设置可防止 LRAT 从传输数据包上 [有线测试端口](#)。您还可以使用在测试后结束功能在 [有线自动测试配置文件设置](#) 隐藏需要传输功能的自动测试卡。设置自动测试在测试后结束设置交换机。否则,当只接收已启用,有线 DHCP/静态 IP 测试显示“接口配置为仅接收数据包”的结果代码,并且后续测试不运行。

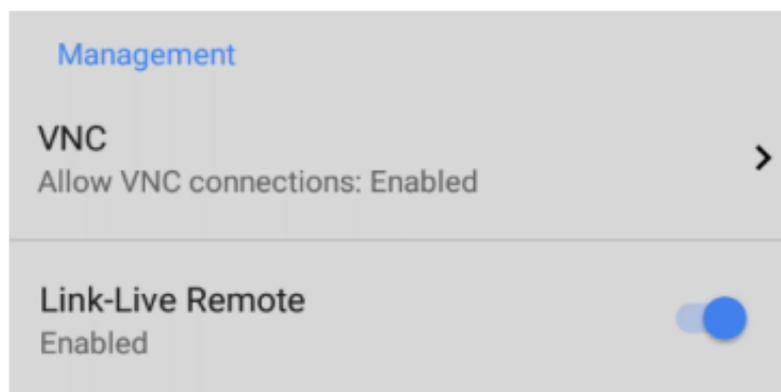
用户自定义MAC: 此设置只会影响 [有线测试端口](#)。点击切换开关以启用用户定义的 MAC 地址。启用时, 额外的 用户自定义MAC 字段出现在切换设置下。点击下方字段输入您想要的 MAC 地址 LRAT。启用用户定义的 MAC 时, **(User-defined)** 出现在 MAC 地址旁边 [关于](#) 屏幕和相关的测试结果屏幕。

注意: 该定义可以被基于配置文件的用户定义的 MAC 覆盖。参考 [有线连接设置](#) 了解更多信息。



管理

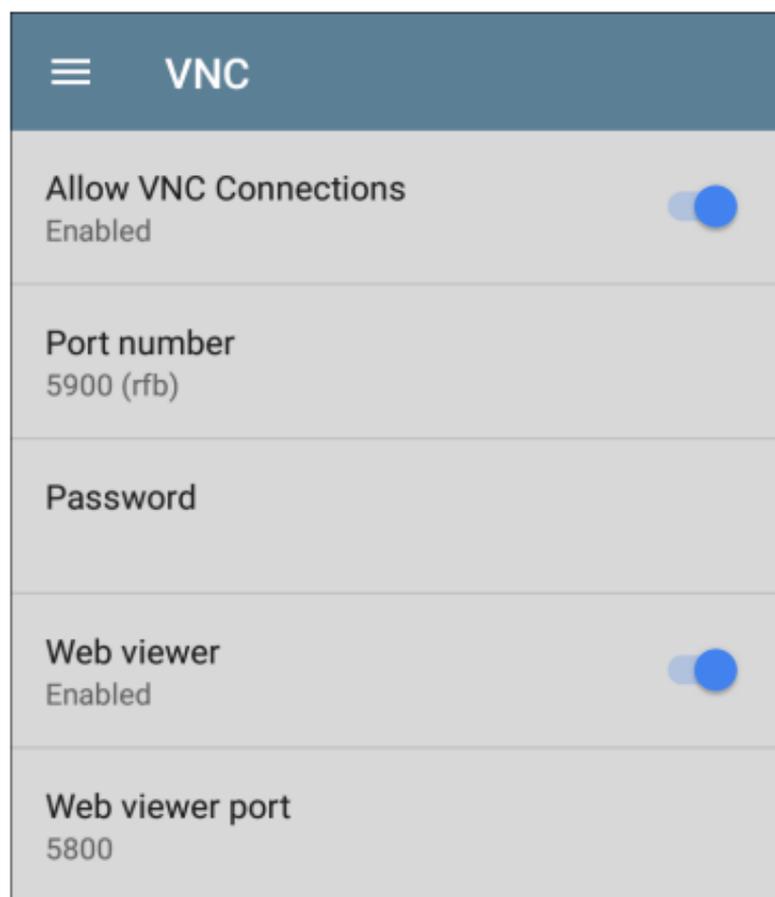
这些设置会影响管理相关功能LRAT, 包括远程访问。



 **VNC**

Touch **VNC** 打开 VNC 设置屏幕并配置设备的 VNC 连接以进行远程操作。

See [远程访问](#) 有关连接到 VNC 客户端或 Link-Live Remote 的更多信息。



允许 **VNC** 连接: 触摸切换按钮以启用或禁用来自 VNC 客户端的远程连接。

端口号:轻触以输入默认端口号以外的端口号。

密码:轻触以输入密码, VNC 用户必须输入该密码才能访问LRAT远程接口。

注意:如果您设置了一个密码 这里在**VNC**设置, 需要密码才能连接到独立的 VNC 客户端和 Link-Live.com 上的远程功能。

网页浏览器:触摸切换开关以启用或禁用 Web 查看器访问。

Web 查看器端口:轻触以输入默认端口号以外的端口号。

Link-Live 远程

此设置启用或禁用LRAT的遥控功能在 [Link-Live](http://Link-Live.com) 云服务 在 Link-Live.com.

注意:Link-Live Remote 功能仅适用于具有 **AllyCare** 订阅服务。您的LRAT必须要**捆绑**。See NetAlly.com/Support 查询更多的信息。

访问远程功能设备 Link-Live.com 上的页面, 通过选择你的 LRAT 3000-4000.

首选项

Preferences

Distance Unit

Feet

Save Locally Only

Disabled



UPDATE GRAPHIC

距离单位:这是单位LRAT用于测试应用程序中的距离测量,特别是 [电缆测试](#)。触摸该字段可在英尺和米之间切换。

仅保存本地:点击此切换字段可更改设备保存文件的默认行为。(默认是让您选择保存到 [Link-Live](#) 或本地。)

趋势图

许多LRAT 3000-4000 测试应用程序具有记录测量的基于时间的折线图,您可以平移和缩放以查看不同的时间间隔。例如,下图显示了显示了无线自动测试信号和使用率图表
[无线链路测试结果](#)。



Ping

STOP

PING
TCP www.google.com

Device Name: --

IP Address: 172.217.11.228

MAC Address: --

Interface: Wired Port

Results

Started: 4:43:12 PM

Status: Success

Metric	Result
Sent	808
Received	807
Lost	1 (0.12 %)

Response Time



Cur Min Max Avg

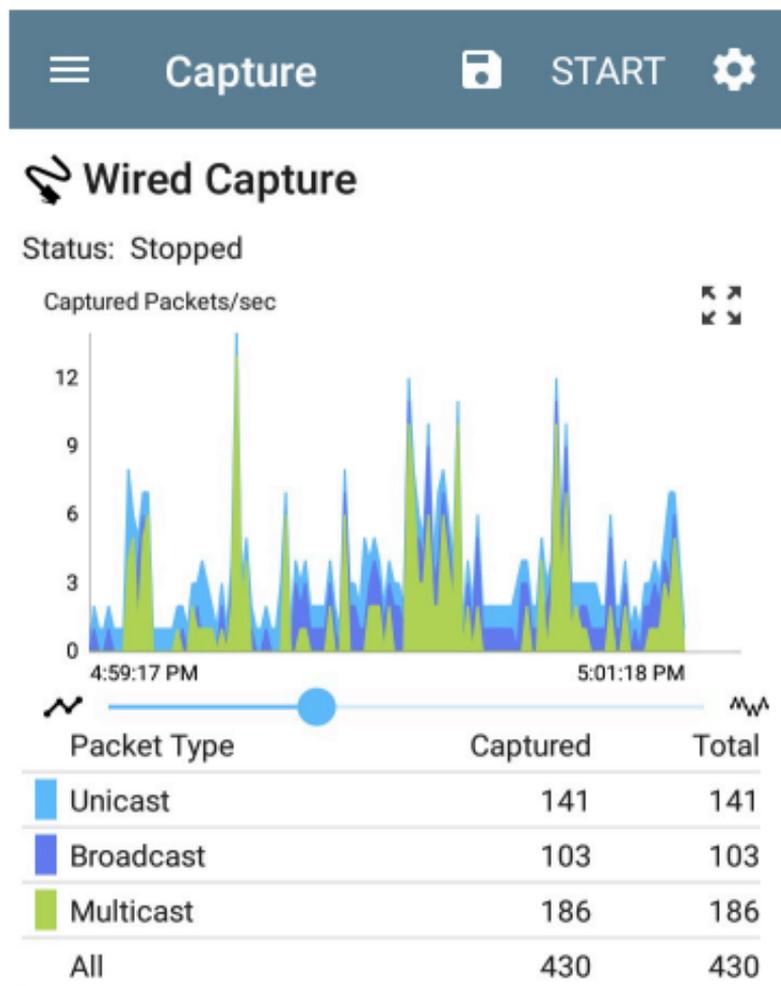
Response	14 ms	12 ms	92 ms	16 ms
----------	-------	-------	-------	-------

Limit	1 s			
-------	-----	--	--	--

这些图表实时更新并保存和显示长达 24 小时的数据(取决于测试类型和/或链接状态)。

在每个图形下，图例表指示与每个绘制颜色对应的测量值。

再举一个例子，下图显示了抓包应用图表。



- 要平移或及时前后移动，请在每个图形上触摸并左右拖动(滑动)。

- 要放大特定时间点，请双击图表上的点。每双击一次，视图会放大 2 倍(或显示一半的时间)。
- 要放大或缩小、减少或增加显示的时间间隔，请拖动滑块或点击图表下方的滑动条。
 - 最大时间间隔(最大缩小)是数据累积的总时间。
- 要将图表重置为默认时间间隔，请点击缩放重置图标 。
 - 出现缩放重置图标在缩放或平移后
 - 默认时间间隔因不同的应用程序而异。

以下应用程序和屏幕包含趋势图：

- [Ping/TCP - Ping 测试](#)
- [抓包](#) (仅限 LinkRunner AT 4000)
- [发现 - 接口统计](#) (仅限 LinkRunner AT 4000)
- [iPerf](#) (仅限 LinkRunner AT 4000)

常用图标

下面的图标出现在多个 NetAlly 测试和系统应用程序中。



菜单图标 - 打开左侧导航菜单或其他菜单



刷新图标 - 在当前屏幕上重新开始测试和测量



设置图标 - 打开当前应用的配置选项



保存图标 - 保存设置或文件或加载保存的配置



浮动操作按钮 (**FAB**) - 打开浮动操作菜单，其中包含其他操作



动作溢出图标 - 包含附加操作



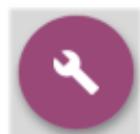
方向箭头 - 指示“钻入”、打开屏幕或展开面板以获取更多详细信息或更改列表顺序的能力

对于具体的 LRAT 出现在屏幕顶部状态栏中的图标，请参阅 [测试和端口状态通知](#)。

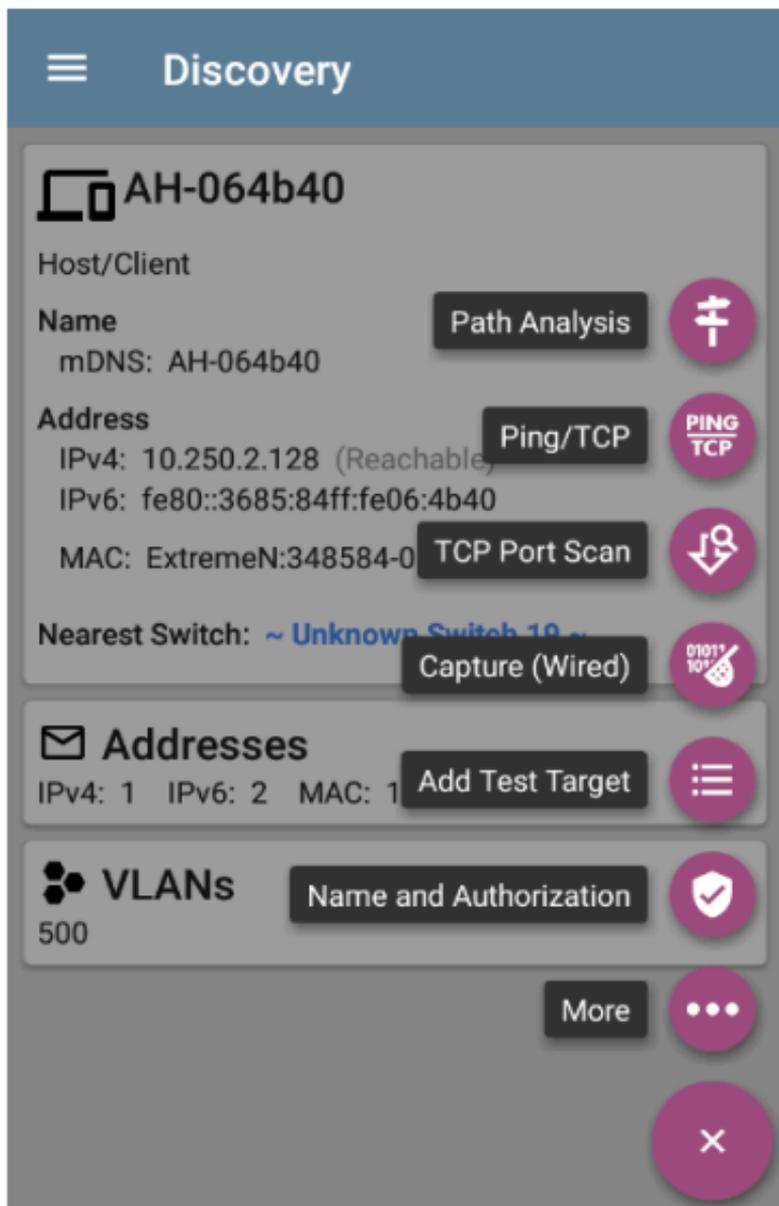
浮动操作按钮 (FAB) 和菜单

许多系统应用程序，包括NetAlly的 AutoTest 和 Discovery 应用程序，具有浮动操作按钮或“FAB” 这将打开一个浮动操作菜单，其中包含更多用于分析的选项。

这将打开一个浮动操作菜单，其中包含更多用于分析的选项。



Discovery 应用程序的详细信息屏幕上的 FAB 会打开其他应用程序以进一步测试所选设备。



出现在测试应用程序中的浮动操作菜单在相关章节中有更具体的描述。例如，[Discovery App 浮动操作菜单](#) 有关更详细的说明，请参阅 [Discovery 应用程序](#) 章节。

常用工具

网页浏览器/Chromium

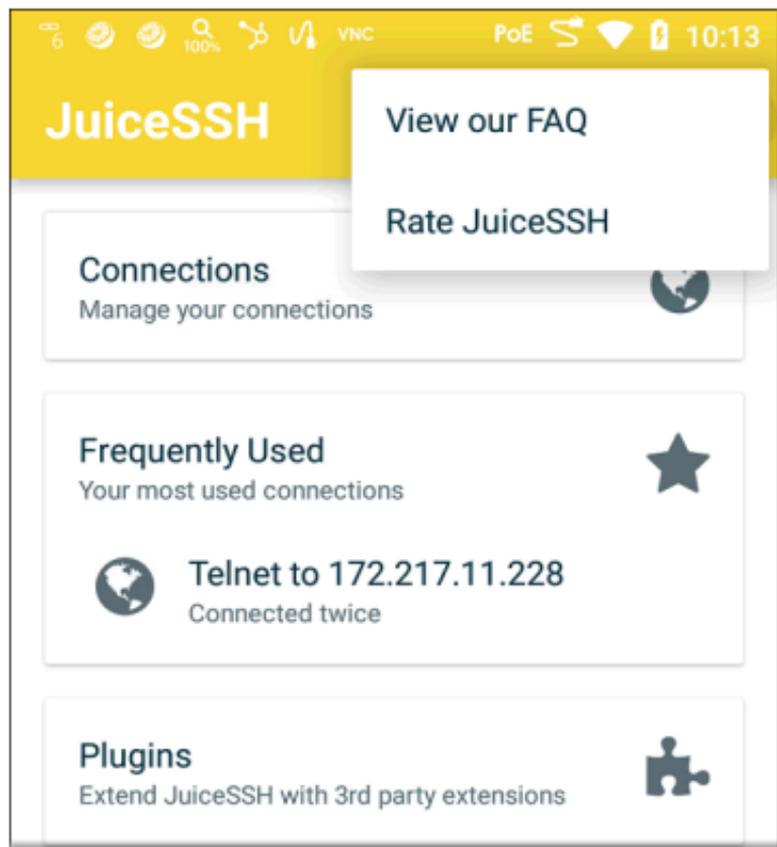
一些测试应用程序，如 AutoTest、Ping/TCP 和 Discovery，让您可以选择浏览使用 Web 浏览器应用程序访问 Internet 地址。LRAT 预装了 Google Chromium。

Telnet/SSH

安装 JuiceSSH  应用程序预安装。AutoTest 和 Discovery 应用程序都提供了使用当前设备地址启动 Telnet 或 SSH 会话的选项。选择这些选项会打开 JuiceSSH 并启动会话。您还可以从以下位置打开 JuiceSSH [Apps](#) 屏幕。

JuiceSSH 应用程序维护一个先前连接的列表。当从一个 NetAlly app, JuiceSSH 使用列表中与 IPv4 地址或设备名称和类型匹配的第一个连接。如果未找到匹配项，则会创建并使用新的连接条目。

作为第三方应用程序，JuiceSSH 包含自己的教程。如需更多帮助，请触摸操作溢出按钮  在 JuiceSSH 应用程序屏幕的右上角，然后选择查看我们的常见问题。



软件管理

本章介绍了如何保存和传输文件、重置应用程序和设备默认值、更新您的软件以及远程访问您的LRAT 3000-4000。

点按下面的链接以跳至您想要的主题：

[管理文件](#)

[更新软件](#)

[远程访问](#)

[重置应用默认值](#)

[恢复出厂默认设置](#)

管理文件

在LRAT 3000-4000的操作系统、图像、文档和其他文件驻留在文件夹系统中，您可以在其中在文件夹之间复制、移动和粘贴它们或到外部存储位置。

另见 [共享](#)。

文件应用

文件应用程序允许您访问保存在您的LRAT。触摸  主屏幕底部的图标(或从[Apps](#)屏幕)来管理文件。

注意:在文件应用程序中,您可能需要点击操作导航图标  在左上角并选择 **LinkRunner AT folder**. 文件夹显示设备子文件夹, 如下图.

 **LinkRunner AT**  

LinkRunner AT



Images



Audio



Videos



Files

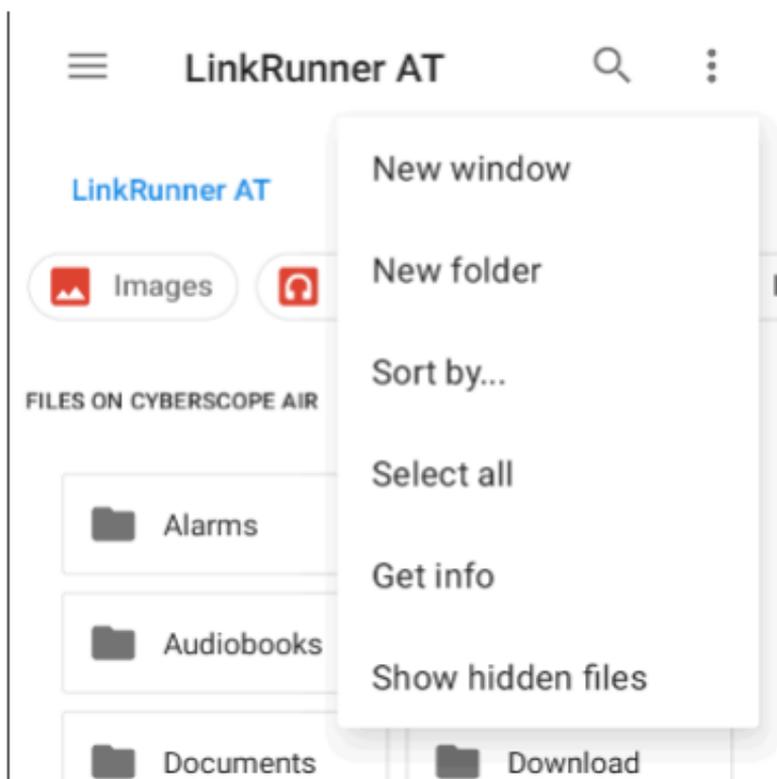
FILES ON LINKRUNNER AT



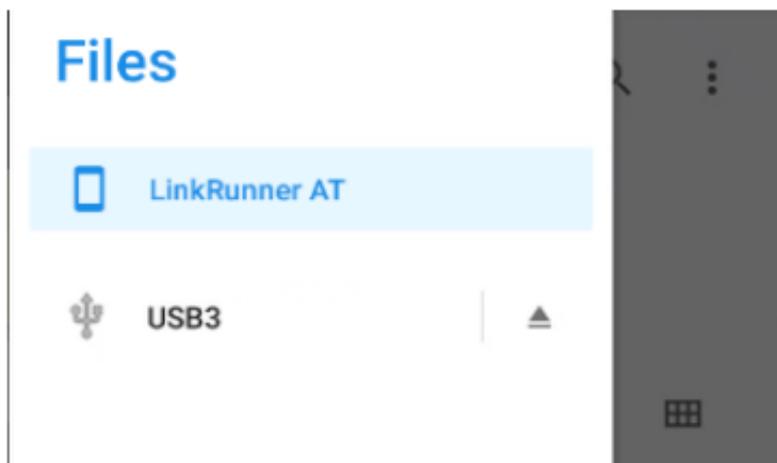
- 点按文件夹或文件以将其打开。
- **长按**在文件夹或文件上选择多个并在顶部工具栏中查看其他文件管理操作，包括**Share** 和删除按钮。



- 点击操作溢出图标 **⋮** 以查看更多操作，例如创建新文件夹、移动文件、删除项目以及显示或隐藏主要内部存储文件夹。



- 打开左侧导航按钮 轻松浏览顶级文件夹和连接的存储设备。



如何移动或复制文件

1. 长按文件以选择它。然后,您可以根据需要通过点击它们来选择更多文件。



2. 触摸溢出图标  在右上角。
3. 选择复制到...或搬去...您选择的操作按钮出现在屏幕底部。



4. 导航到要移动或复制文件的文件夹。
5. 触摸移动或复制屏幕底部的按钮。

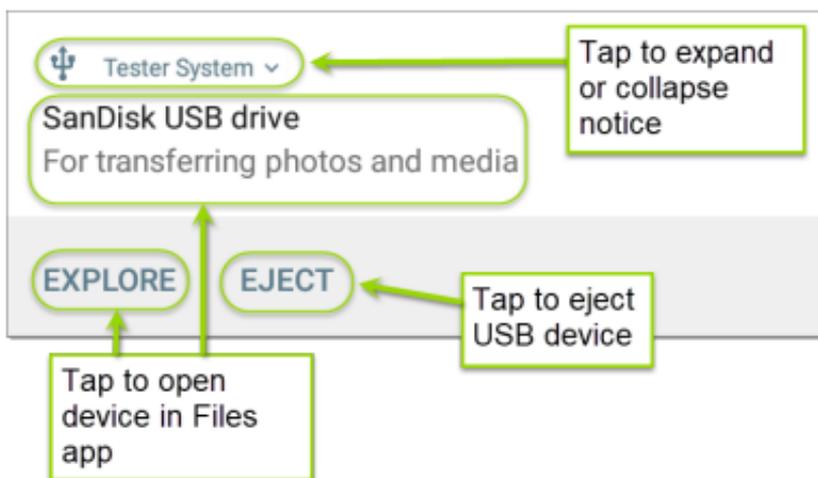
使用USB驱动器

将一个USB闪存驱动器插入 **USB端口**，该端口位于LRAT的顶部。

一个USB图标  会出现在屏幕顶部的状态栏中。向下拉出顶部的 **通知面板** 以显示USB驱动器通知。



点击通知标题或向下箭头展开通知，显示额外选项：



USB存储 位置现在可以通过 **文件**  应用程序访问。

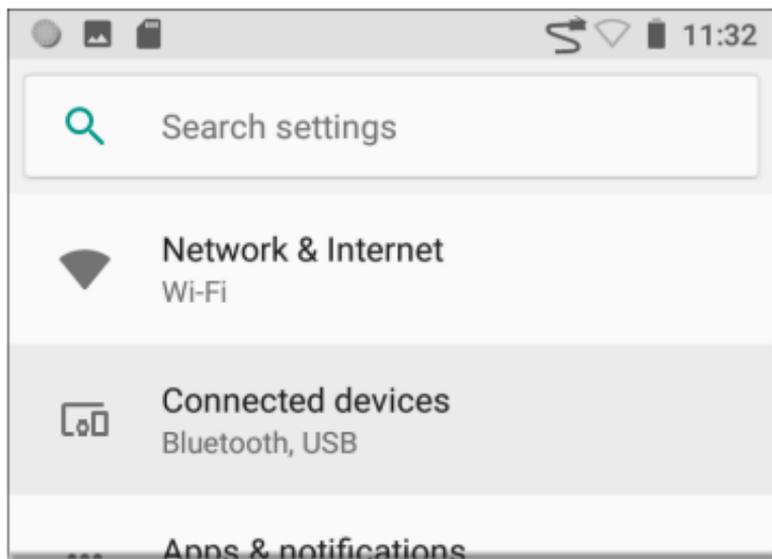
⚠️ 注意：请使用系统的弹出功能后，再从USB端口物理上移除Micro SD卡，以避免可能导致存储设备文件系统损坏的情况发生。

弹出存储介质

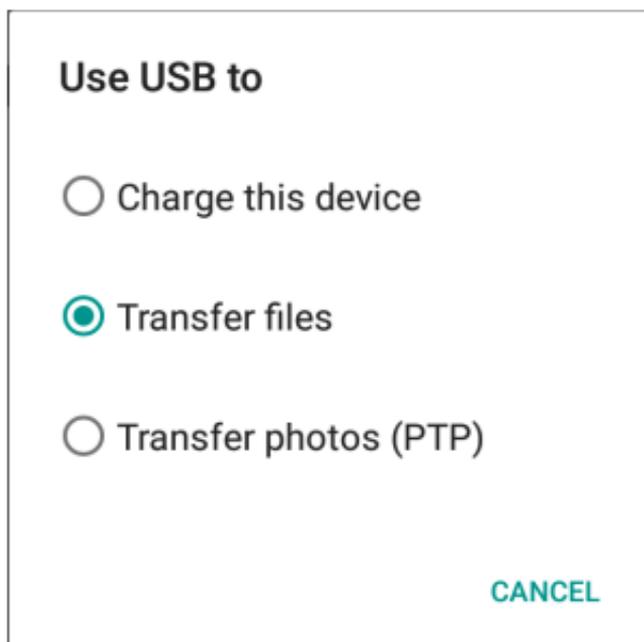
您可以从通知面板中的扩展通知(如上所示)或文件应用程序中的左侧导航抽屉中弹出存储媒体(如下所示)。

使用 USB Type-C 转 USB 电缆

1. 将 USB-C 电缆插入 USB-C 左侧的端口 LRAT, 然后连接到 PC 或平板电脑。
2. 在 LRAT 设备上, 通过点击设置打开系统设备设置 底部的图标主屏幕.
3. 选择连接的设备.



4. 在连接的设备屏幕上，选择**USB**。
5. 在弹出的对话框中，点击传输文件启用文件传输。



注意：LRAT不能通过连接到 PC 的 USB 电缆充电。

6. 在您的 PC 或平板电脑上，导航到LRAT 3000-4000如果没有自动弹出文件夹。从那里，您可以移动、复制和粘贴文件到 LRAT 3000-4000的文件系统。

 **警告：**使用EJECT 物理断开 USB 电缆与 PC 或LRAT以避免您的存储设备的文件系统的潜在损坏。参考[弹出以上存储介质](#)。

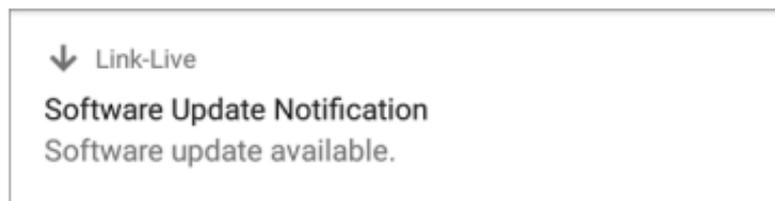
更新软件

您的LRAT 3000-4000从 Link-Live 云服务“空中下载”(OTA)访问软件更新。但是,如果您不想将您的设备捆绑到 Link-Live,您也可以手动下载和安装更新。看[手动更新](#)信息。

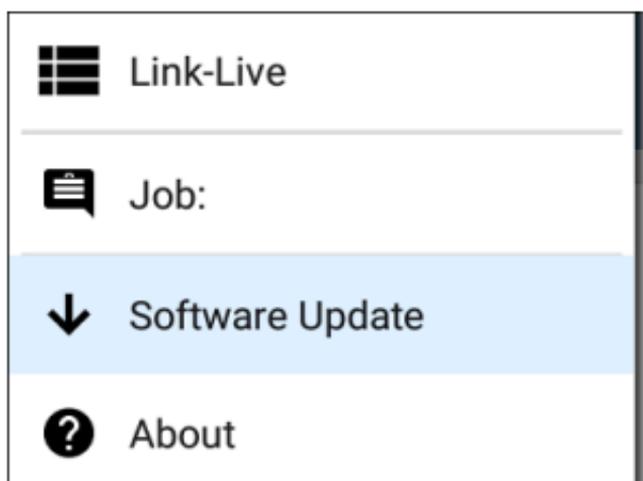
远程更新

您必须创建一个帐户并“声明”您的LRAT 3000-4000设备到Link-Live.com从而LRAT 查找和下载软件更新。看[Link-Live 入门](#)。

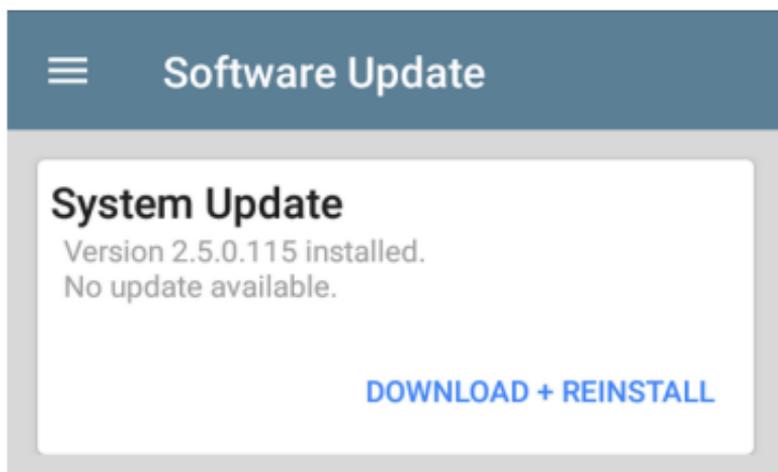
您第一次申领您的LRAT 3000-4000到 Link-Live,可能会有软件更新。如果是这样,更新图标出现在状态栏中。向下滑动[顶部通知面板](#),然后选择通知以更新您的设备。



1. 要随时检查可用的软件更新,请打开[Link-Live 应用](#)  从 [主屏幕](#)。
2. 在 Link-Live 应用程序中,触摸菜单图标  或向右滑动打开左侧[导航部分](#)。



- 轻触软件 升级. 软件更新屏幕打开并显示任何可用更新的版本号。(只有当有更新的版本时会出现应用升级.)



- 点击 下载+安装 (或 下载+重新安装) 以更新操作系统和NetAlly应用程序。更新将自动下载和安装。完成后, 设备将重新启动。

5. 更新后, 请再次检查软件更新屏幕, 以防仍需要另一个更新。

手动更新

您可以通过联系 NetAlly 的技术支持(网址为 (NetAlly.com/Support) 获取更新文件或从 Link-Live.com 下载, 如下所示:

1. 登录 Link-Live 网站。
2. 单击菜单图标打开左侧导航按钮 , 然后选择 技术支持 > 软件下载。
3. 找到并选择您的设备的更新文件. 文件名的格式是: **<product name abbreviation>-ota-user.zip**.
4. 保存更新文件到个人电脑。

更新系统软件

如需要可参考 [按钮和端口](#)。

1. 从您的 PC 中, 将 .zip 文件复制到 FAT32 格式的 USB-A 驱动器, 然后将 驱动器插入您的 LRAT。
2. 关掉你的 LRAT 设备。

3. 按住 **提高音量** 按钮, 然后按 **电源** 按钮. 继续持有 **提高音量** 按钮, 直到出现恢复屏幕.。(你可以松开 **提高音量** 此屏幕出现几秒钟后按钮。)
4. 在恢复模式下, 使用音量按钮突出显示 .
5. 按 **电源** 按钮进行确认。
6. 使用音量按钮突出显示 卡或 USB 驱动器上的正确更新文件。
7. 按 **电源** 按钮进行确认。这 LRAT打开 更新器, 安装更新, 然后在安装更新的情况下重新启动。此过程可能需要 5 到 10 分钟。完成后, 显示 '从USB驱动器安装完成, 状态为0。' 应该显示在安装行。
8. 使用音量键和 **电源** 选择按钮 **现在重启系统**。您的设备应该可以正常启动。

远程访问

LRAT支持使用独立 VNC 客户端或 Link-Live 远程功能进行远程访问和控制，后者通过 Link-Live 网站使用 VNC 客户端。

注意：Link-Live Remote 功能仅适用于具有活动 **AllyCare** 订阅。你的 LRAT 一定是 **绑定**。参考 [NetAlly.com/Support](https://www.netally.com/support) 想要查询更多的信息。

您可以使用有线测试端口建立远程连接。但是，管理端口为远程控制提供了更稳定的链接，因为测试端口可能会频繁断开并重新连接。

参考 [测试和管理端口](#)。

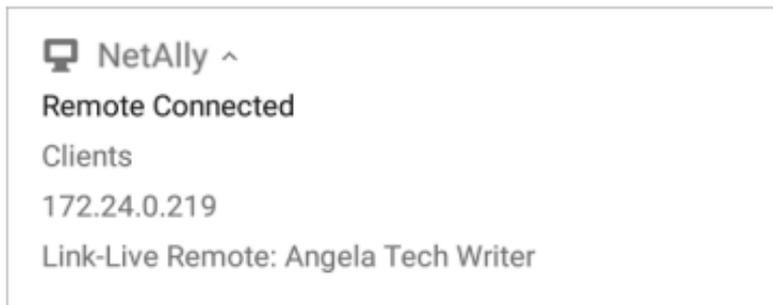
顶端 **通知** 是查找分配给您的 IP 地址的最快方法 LRAT 端口。从底部向下滑动 **状态栏** 查看它们。

 NetAlly

Wired Management Port

IP Address: 192.168.0.123

当远程会话处于活动状态时，远程图标  出现在顶部的状态栏中，以及一条通知。



使用 VNC

远程访问LRAT 3000-4000使用安装在 PC 或其他机器上的对等 VNC 客户端。

See [常规设置 > VNC](#)启用和配置 VNC 连接。

连接到LRAT使用 VNC 客户端：

1. 通过从屏幕顶部的状态栏向下滑动以查看已连接端口(最好是管理端口)的 IP 地址[通知面板](#).
2. 提供 测试或管理端口的 IP 地址到您选择的 VNC 客户端应用程序。
3. 使用您的 VNC 客户端进行连接。
4. 如果需要, 请输入在[VNC 设置](#).

使用 Link-Live 远程

Link-Live 远程功能使用端到端加密, 允许安全远程控制您的LRAT.

在您的LRAT，去[常规设置 > Link-Live 远程](#)以确保启用该功能。

注意：如果密码在[VNC 常规设置](#)，您还必须输入相同的密码才能访问 Link-Live 中的远程功能。

1. 如果您有 AllyCare，请登录Link-Live.com访问 Link-Live 远程功能。你的LRAT一定是[捆绑](#)。
2. 导航到设备  [Link-Live.com](#) 上的页面。
3. 选择LRAT您想从声称的单位列表中远程控制。
4. 单击或触摸远程图标  在页面右上角打开一个嵌入的窗口，其中包含LRAT端口。
5. 如有必要，在窗口顶部，输入密码设置[常规设置 > 管理 > VNC](#)上配置LRAT

要在远程会话处于活动状态时使用 Link-Live 网站，您必须打开一个新的 Link-Live 选项卡或窗口。

管理 NetAlly 应用程序设置

本主题介绍如何重置、[加载](#)、[保存](#)、[导入](#)，和[导出](#) NetAlly 测试应用程序的测试设置。

有关为整个设备恢复出厂默认设置的说明，请参阅[恢复 LRAT 3000-4000 出厂默认值](#)。

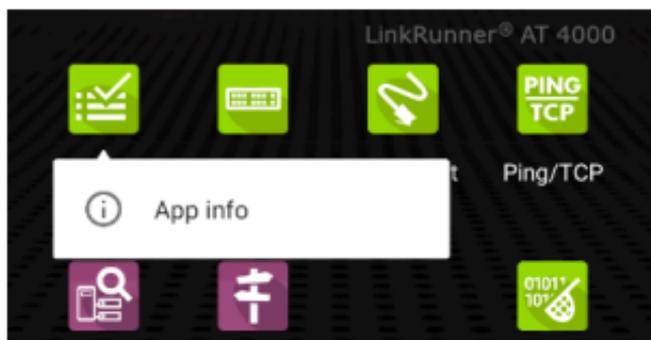
重置测试应用程序默认值

在您调整设置后 NetAlly 应用程序，您可能需要将应用程序的设置重置为默认设置。以下过程将所有特定于应用程序的设置重置为出厂默认设置。

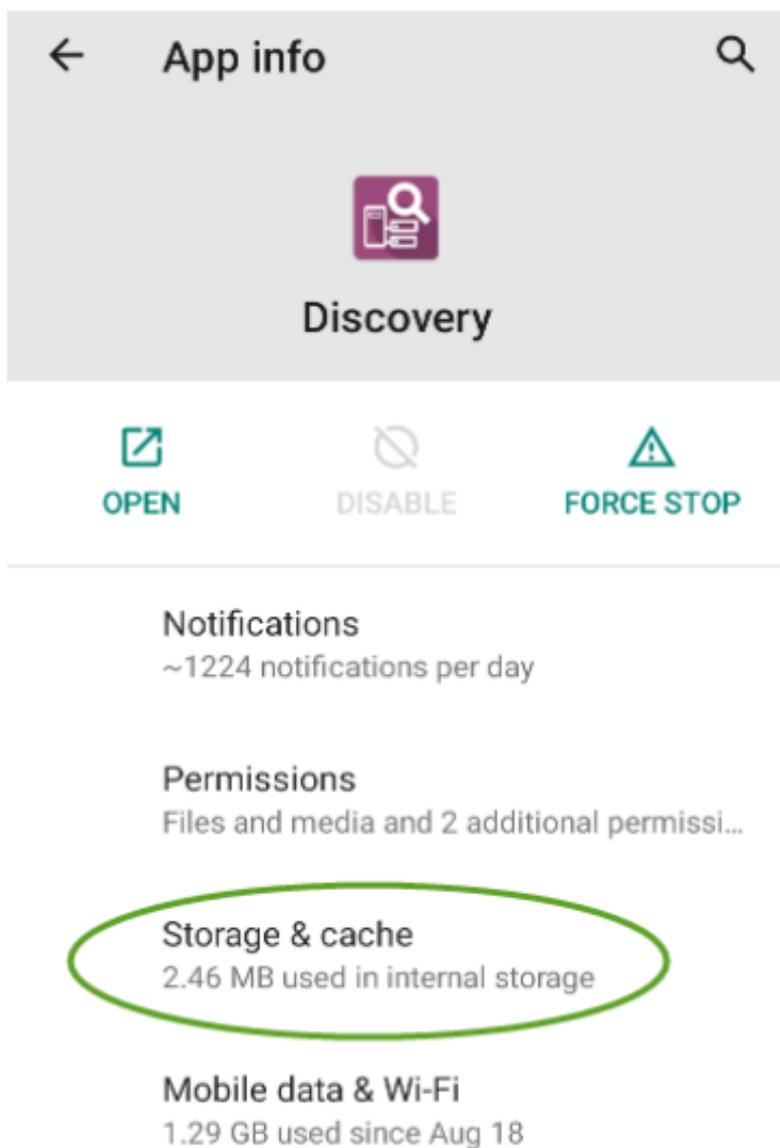
 **警告：**此操作会删除所有保存的设置，包括测试配置文件和其他应用程序数据。

Discovery 应用程序在以下步骤中用作示例：

1. 访问应用信息 长按(触摸并按住)屏幕上的应用程序图标 [主屏](#) or [Apps screen](#).

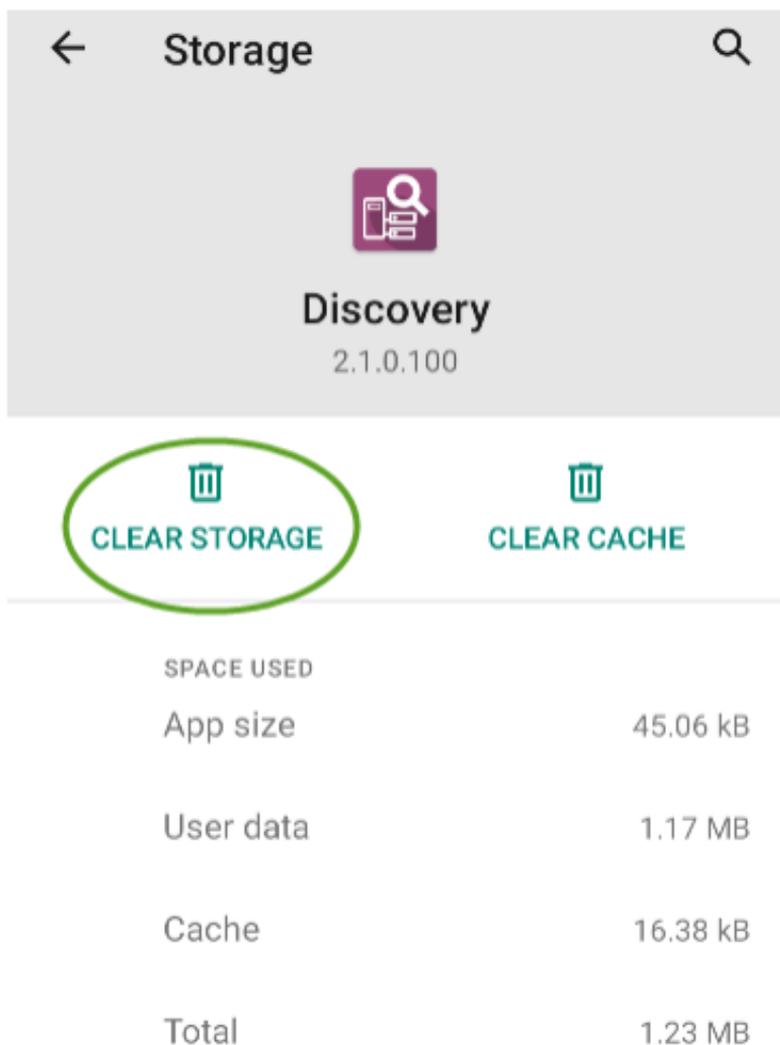


2. 轻触 应用信息.



3. 在应用程序信息屏幕上，选择
(您还可以从 [设备设置](#)  > 存储 > 内部
共享存储 > 其他应用。)

4. 在所选应用的存储屏幕上，点击除存储。



5. 当对话框提示您删除数据时，点击“确定”。

应用程序的所有设置都重置为出厂默认设置。

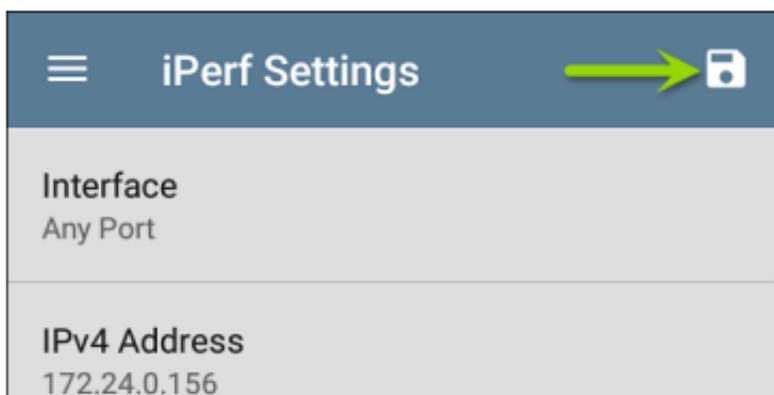
保存应用程序设置配置

许多 NetAlly 测试应用程序允许您通过选择保存按钮来保存和加载设置配置  出现在应用程序主屏幕的右上角。

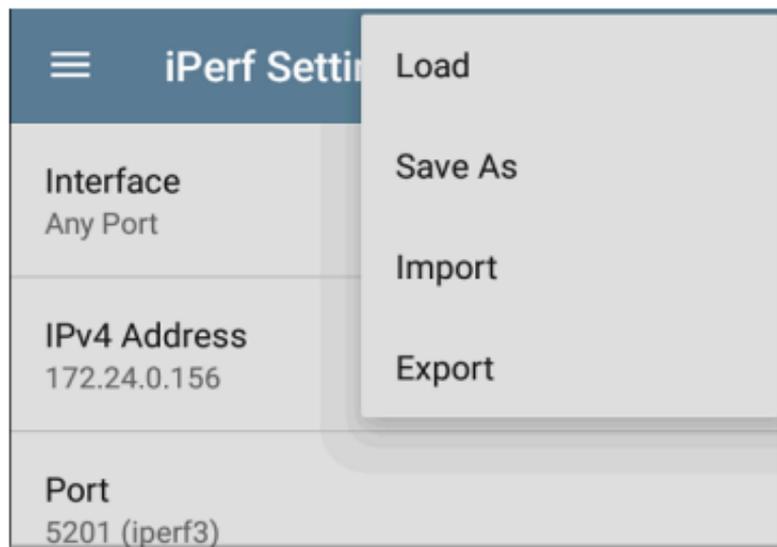
以下应用程序使您能够保存和加载设置配置：

- [自动测试, 包括配置文件组](#)
- [发现](#)
- [发现问题设置](#)
- [iPerf](#)

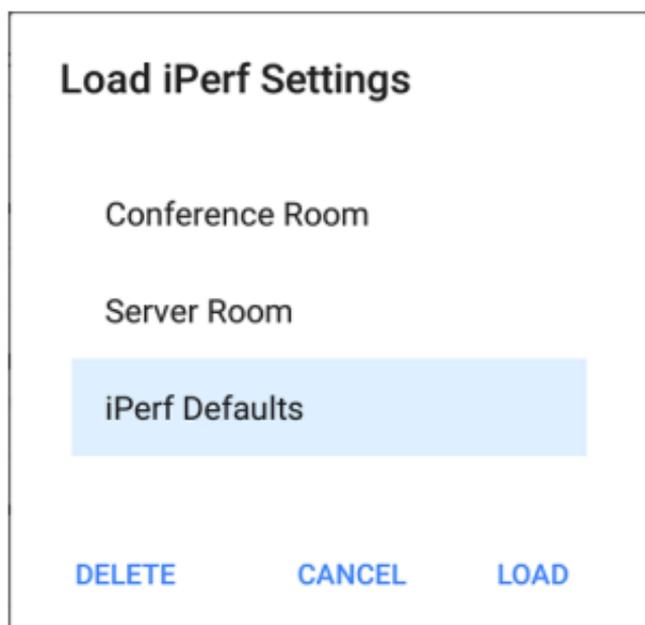
下面以 iPerf 应用程序为例。



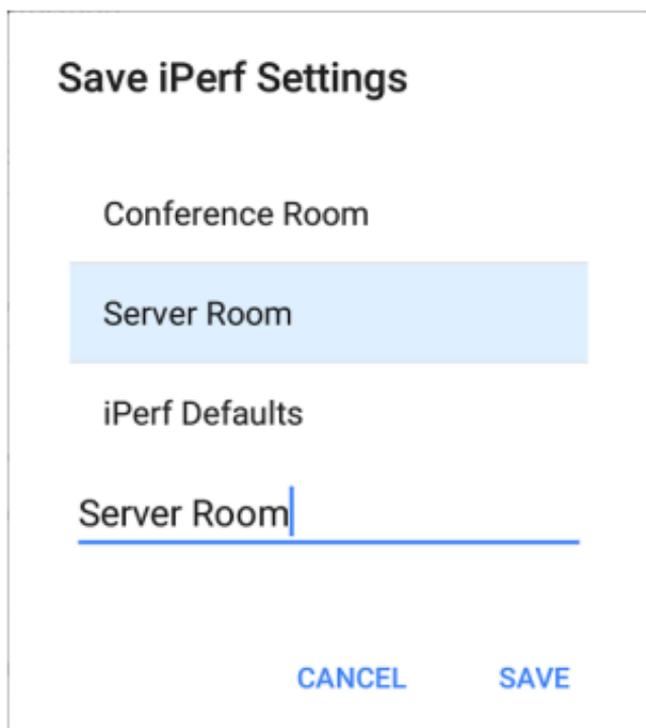
以下选项显示在下拉菜单中：



- 加载:打开之前保存并命名的设置配置。



- 另存为:使用现有名称保存当前设置,或输入新的自定义名称。



Save iPerf Settings

Conference Room

Server Room

iPerf Defaults

Server Room

CANCEL SAVE

- 导入:导入以前导出的设置文件。
- 导出:创建当前设置的导出文件,并将其保存到内部或连接的外部存储。
- 导出到 **Link-Live**:将当前设置直接导出到 [Link-Live](#) 云服务。

See [导出和导入应用程序设置\(下\)](#) 了解更多详情。

保存默认测试应用程序配置

如果您发现您经常重置应用默认设置,您可以保存设置的默认配置供以后使用NetAlly测试应用程序。在应用程序中加载保存的默认配置允许您访问默认设置而不删除其他配置。这个策略对以下情况最有用[发现设置](#)和[问题设置](#)。

1. 转到应用程序的设置屏幕。
2. 将所有设置设为默认值后,点击保存按钮和另存为。
3. 使用明显的名称(如“默认配置文件”或“发现默认值”)保存默认配置。
4. 不要在不保存新的自定义命名配置的情况下将默认配置中的设置更改为非默认值。

导出和导入设置

LRAT 3000-4000提供导入和导出已保存的测试应用程序设置的功能,以便传输到其他单元、[Link-Live](#)、USB 存储或其他设备。

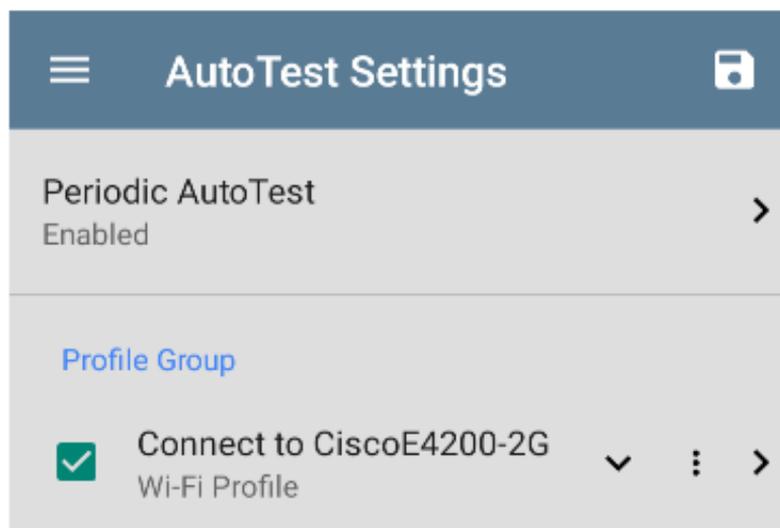
注意:您只能在同类 NetAlly 产品之间导入和导出设置。例如,两个设备都必须是 LinkRunner AT 4000 才能进行传输。您无

法在 LinkRunner AT 3000 和 LinkRunner AT 4000.

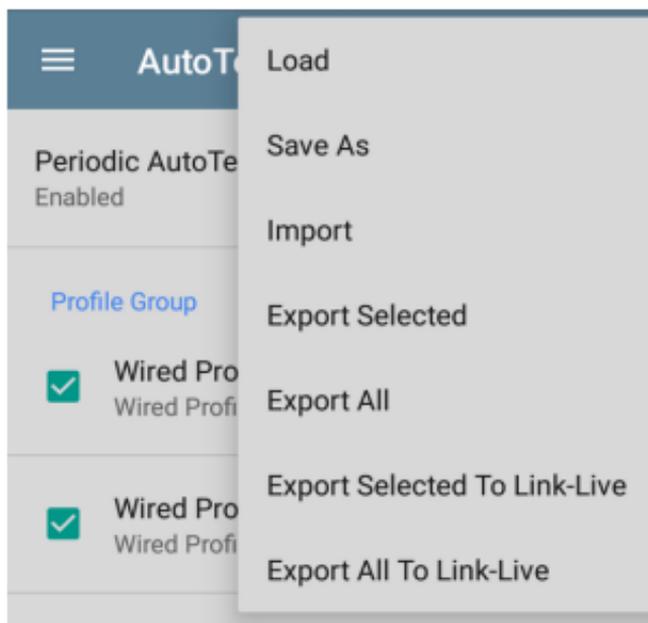
以下应用程序使您能够导入和导出设置配置：

- [自动测试设置, 包括配置文件组](#)
- [发现设置](#)
- [发现 > 问题设置](#)
- [iPerf 设置](#)

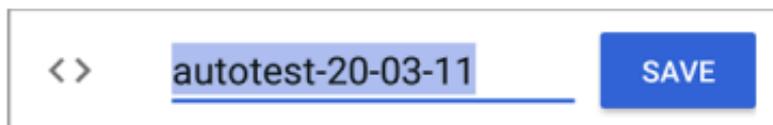
下图中的示例显示了自动测试设置。



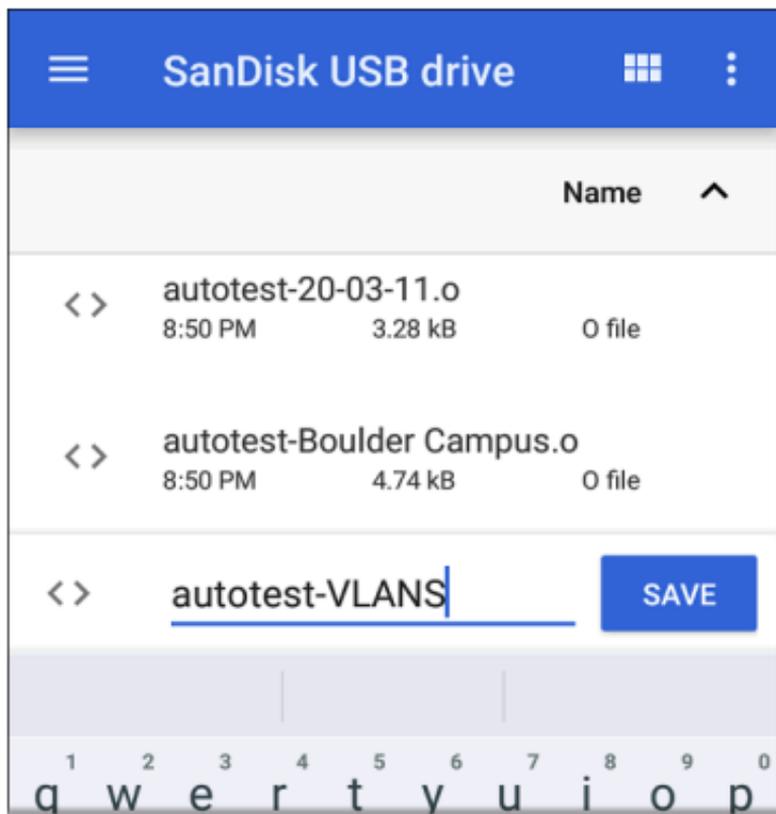
- 触摸保存按钮导入新的应用程序设置或导出当前处于活动状态并被选中应用程序设置。



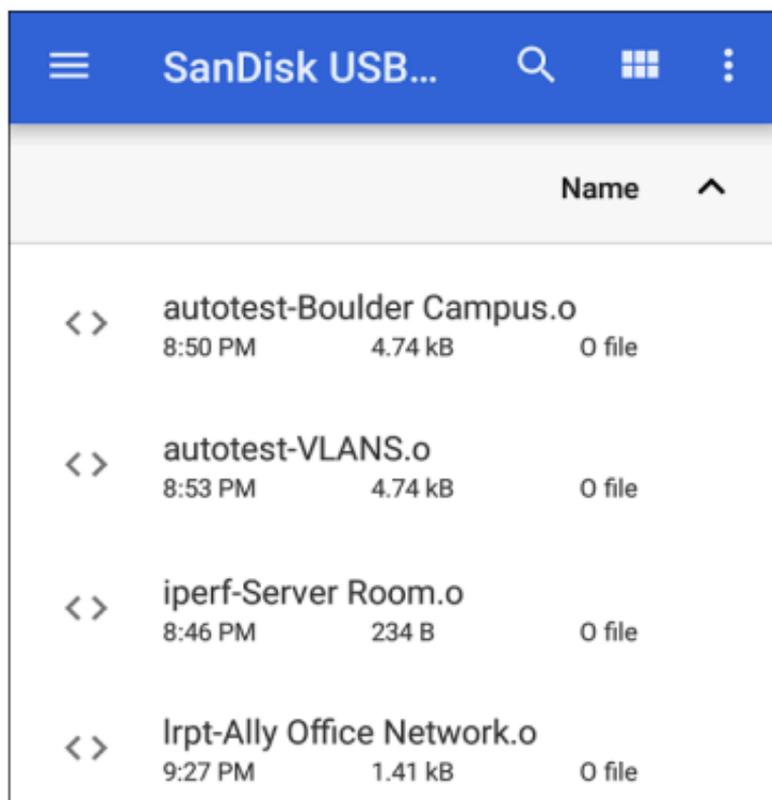
- 共享配置列表中的选定(选中)项目是您选择时唯一导出的项目 **导出选择**. 这可以包括子菜单中的任何选中项(例如 AutoTest 测试目标或社区字符串 [发现设置](#)). 您还可以选择 **导出全部** 导出所有选定和未选定的项目。
- 没有自定义名称的未保存配置会自动命名为应用程序名称和日期：



- 保存的配置使用应用程序名称和自定义设置名称自动命名：



- 您可以根据需要重命名导出文件。
- 设置可以保存到任何连接的外部或内部存储。参考[管理文件](#)有关访问文件夹和移动文件的说明。
- 设置保存在.o文件扩展名。



- 选择导入从应用程序打开[文件](#)应用程序，您可以在其中导航并选择要导入的.o文件。
- 导入的设置配置会覆盖应用程序中已有的同名已保存配置。

通过Link-Live将自动测试的设置导入到其他设备

您可以通过Link-Live的云端服务将自动测试的设置导入到其他LRAT 3000-4000设备。

- 准备工作
- 导出将要共享到Link-Live的设置文件。
- 在Link-Live上选择将要导入设置的设备。
- 在每个设备上导入设置。

开始之前

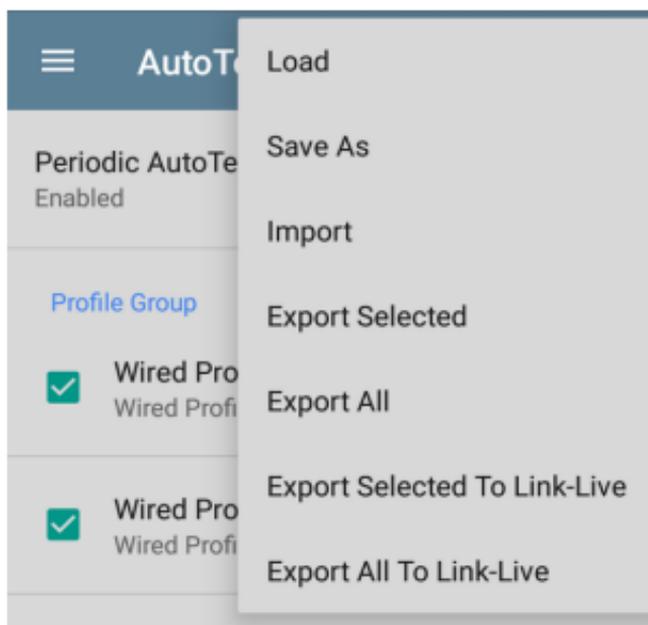
- 请准备好如下环境
 - a. 即将导出设置的设备
 - b. 基于PC的浏览器
 - c. 即将导入设置的设备
- 确保每一台即将导入或导出设置的 LRAT 3000-4000 都已经在Link-Live上注册并且更新至最新版本。(请使用Link-Live app 和浏览器来完成注册. 参考 "[Link-Live 云服务入门](#)" on page 388 以获得详细步骤)

导出设置文件

此过程在导出设置的设备上完成。

1. 在自动测试应用程序主页中, 点击在右上角的配置图标  进入配置列表界面。

2. 如果您计划仅导出选定的配置文件, 请使用复选框从列表中选择这些配置文件。
3. 点击右上角的保存图标  以保存菜单选项。



4. 点击 导出选择的项目到**Link-Live** (如已选择了配置文件) 或 导出所有到**Link-Live**。这将打开Link-Live保存界面。

**Link-Live**
by NetAlly

Settings File Name
autotest-shared settings

Comment
Update for all units

Job Comment
New profiles

 **EXPORT TO LINK-LIVE**

5. (可选) 编辑文件名, 添加备注, 或增加任务备注。

6. 点击 导出到 **LINK-LIVE** 将文件上传至 Link-Live。

在 **Link-Live** 选择配置导入设备

最好在 PC 浏览器上完成此步骤。

1. 在 PC 浏览器上登录 Link-Live 网站。
2. 点击主菜单按钮 .
3. 点击 配置菜单中的配置 按钮。
4. 选择 **LRAT 3000-4000** 列出所有适用于导入设备的 .o 配置文件。
5. 选择要导入的配置文件。
6. 按照屏幕上的说明将文件导入到特定的设备或您注册的所有单元。

在目标设备上导入配置

请在目标设备上完成导入配置过程。

1. 从 Link-Live 推送文件后, 请等待 30 秒。
2. 从主屏幕顶部的状态栏向下滑动(触摸并拖动)以显示通知面板。

- 找到显示有新自动测试设置的通知。

 AutoTest

New settings from Link-Live
autotest-autotest trial.o

- 点击通知以打开自动测试应用程序。
- 点击右上角的保存按钮 。
- 点击 导入 进入下载文件夹。
- 选择下载的 .o 文件使新的配置生效。

所有应用程序的导入/导出设置

您的LRAT 3000-4000支持所有允许导入/导出设置的应用程序的设置导入或导出。

注意:您只能在同类 NetAlly 产品之间导入和导出设置。例如,两个设备都必须是 LinkRunner AT 4000 才能进行传输。您无法在 LinkRunner AT 3000 和 LinkRunner AT 4000。

要执行组导出或导入:

1. 点击任意 NetAlly 应用程序中的导航菜单图标 ，然后点击 关于。
2. 点击操作溢出图标  以显示导出或导入菜单。
3. 要导入设置：
 - a. 点击 。这将打开 [文件](#) 应用程序的默认设置文件夹。
 - b. (可选) 使用文件应用程序导航到其他文件夹。
 - c. 选择您想要导入的 .nas 设置文件。
 - d. 出现提示时点击“是”，以便在下次系统重启时导入所有应用程序的设置。
4. 要导出设置：
 - a. 点击 **Export LinkRunner AT Settings**。这将打开一个对话框，其中包含系统生成的文件名和默认的保存到文件夹。
 - b. (可选) 点击“保存到”文件夹或点击“另存为”打开 [文件](#)”应用程序以选择

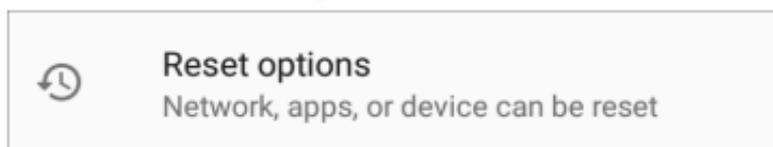
其他文件夹。

- c. 点击**保存**以保存设置文件。

重新设置 LRAT 3000-4000 出厂设置

⚠警告: 将您的设备重置为出厂默认设置可以删除 *所有* 测试结果、用户安装的应用程序、测试应用程序设置和保存的文件。

1. 确保 **备份任何文件** 在重置前保留。
2. 打开安卓 **设备配置** 通过点击设置  主屏幕底部的图标。
3. 在“设置”屏幕上，向下滚动并点击 **系统** 部分。
4. 在系统屏幕上，点击 **重置选项**。



5. 在“重置选项”屏幕上，根据要重置的默认值选择一个选项。您的 LRAT 显示将根据选项和确认按钮重置的项目列表。

重置 Wi-Fi, 移动终端 & 蓝牙: 重置所有网络设置用于 Wi-Fi(测试和管理)、移动数据和蓝牙。

清除所有数据(恢复出厂设置):

⚠警告: 清除 *所有* 来自测试仪内部存

储的用户数据,包括:系统和应用程序数据和设置;下载的应用程序;测试配置文件;证书;数据包信息;和屏幕截图.

6. 点击确认按钮开始重置.
7. 您的设备可能会在重置前要求您确认最后时间。如果是这样,请点击最终确认按钮以重置您的 LRAT 的默认值。然后设备将以您选择的出厂默认设置重新启动.
8. 重置中不包括可移动驱动器上的数据。为了彻底,您可能还想使用 [文件应用](#) 删除您保存在其中的任何应用程序设置、首选项或其他数据 USB U 盘。(不要删除备份文件.)

LRAT 3000-4000 功能控制

本章介绍如何半永久控制 LRAT 3000-4000 中功能的可用性。

点按下面的链接以跳至您想要的主题：

[LRAT 3000-4000 设备功能控制的简介](#)

[控制功能可用性](#)

[更改管理员密码](#)

功能访问简介

LRAT 3000-4000可以半永久地禁用某些功能以满足各种安全需求。这些功能称为受控功能。

对受控特征进行分类,以便更容易识别要禁用的候选特征。受控特征类别和特征是:

移动存储

- USB 访问

连接应用程序

- 浏览器应用
- Telnet/SSH 应用

远程控制

- VNC

文档

- 抓包 (LRAT-4000 仅有的)
- 网络发现 (LRAT-4000 仅有的)

Link-Live 云服务

- Link-Live 访问
- 从App Store下载应用

移动存储

USB 访问

当 USB 访问功能被禁用时，设备顶部的 USB Type-A 端口和设备左侧的 Type-C 端口都会被禁用。这意味着不能通过这些端口在任一方向上传输数据，并且外部设备无法从这些端口接收电源。

注意：USB Type-C 端口继续工作以支持使用交流适配器为设备供电。

连通性 Apps

浏览器 App

当浏览器应用程序功能被禁用时，Chromium 浏览器将被删除。所有通常提供对 Chromium 浏览器访问权限的 NetAlly 应用程序都删除了该选项。其他应用无法访问浏览器。

注意：如果重新启用浏览器应用程序功能，Chromium 浏览器、用户指南和视频应用程序会恢复，但不会出现在主屏幕上。参考 [Apps](#) 有关应用程序屏幕的更多信息。

Telnet/SSH App

The JuiceSSH app, 提供 Telnet 和 SSH 客户端服务, 当 Telnet/SSH App 功能被禁用时被删除。通常提供对此应用程序访问权限的所有 NetAlly 应用程序都删除此选项。

远程控制

VNC

禁用 VNC 功能后, 将禁用使用独立 VNC 客户端远程访问和控制产品 UI 的功能。参考[远程访问](#)有关此功能的更多信息。

注意: 当 VNC 被禁用时, Link-Live 远程功能保持活动状态。要停用 Link-Live Remote, 必须禁用 Link-Live 访问。

文档

Nmap

禁用 Nmap 功能时, Nmap 应用程序也会被禁用。所有通常提供 Nmap 应用程序访问权限的 NetAlly 应用程序都将删除此选项。

注意: 参考[Nmap](#)想要查询更多的信息。

抓包 (LRAT-4000 仅有的)

禁用数据包捕获功能时，捕获应用程序将被禁用。通常提供对 Capture 应用程序访问权限的所有 NetAlly 应用程序都将删除此选项。

注意：参考[抓包](#)想要查询更多的信息。

网络发现 (LRAT-4000 仅有的)

Discovery 和 Wi-Fi 应用程序中的“上传到 Link-Live”或“本地保存”功能已禁用。

注意：参考[发现](#)想要查询更多的信息。

Link-Live 云服务

Link-Live 访问

当 Link-Live 访问功能被禁用时，Link-Live 应用程序将被禁用。所有为 Link-Live 提供接口的 NetAlly 应用程序和服务都将删除访问权限。

注意：当 Link-Live Access 被禁用时，Link-Live 远程功能和 App Store 应用程序也会被禁用。

从 App Store 下载

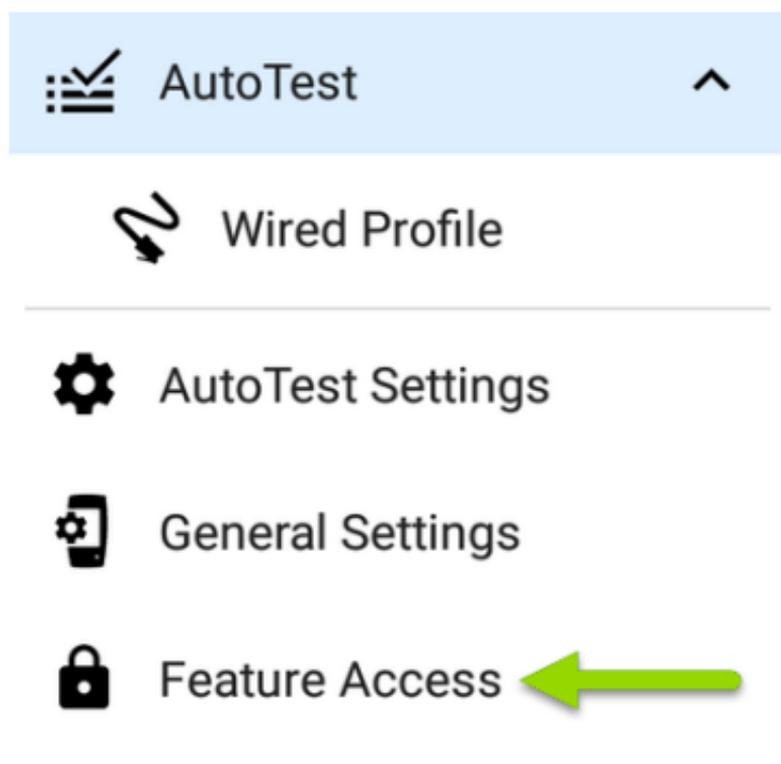
当从 App Store 下载功能被禁用时，App Store 应用程序被禁用。无法向产品添加其他应用程序。

注意：禁用 Link-Live Access 也会禁用 App Store 应用程序。

控制功能可用性

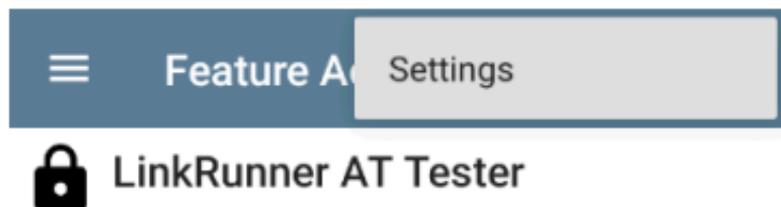
此LRAT 3000-4000支持禁用(和重新启用)某些功能来满足各种安全需求。这些特征被称为受控特征。

使用功能访问本选项来管理受控功能的可用性。它可以从 NetAlly 应用程序中的左侧导航抽屉,例如 AutoTest 和 iPerf。

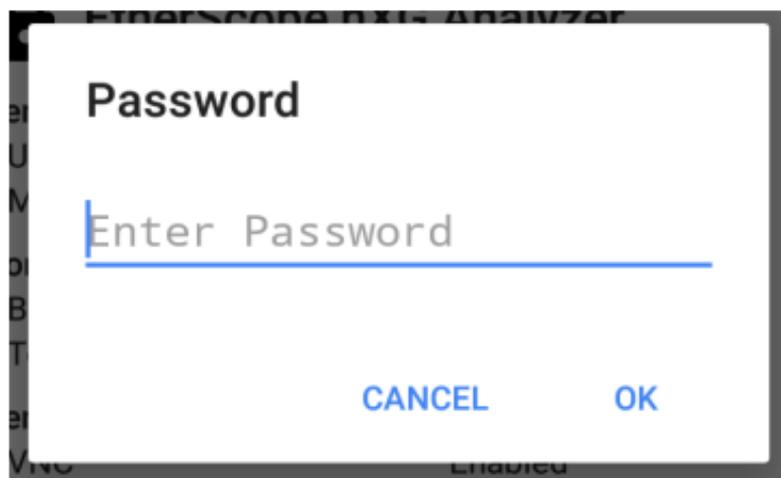


选择 功能访问 以查看 功能访问状态屏幕。该屏幕显示了受控功能的当前状态。

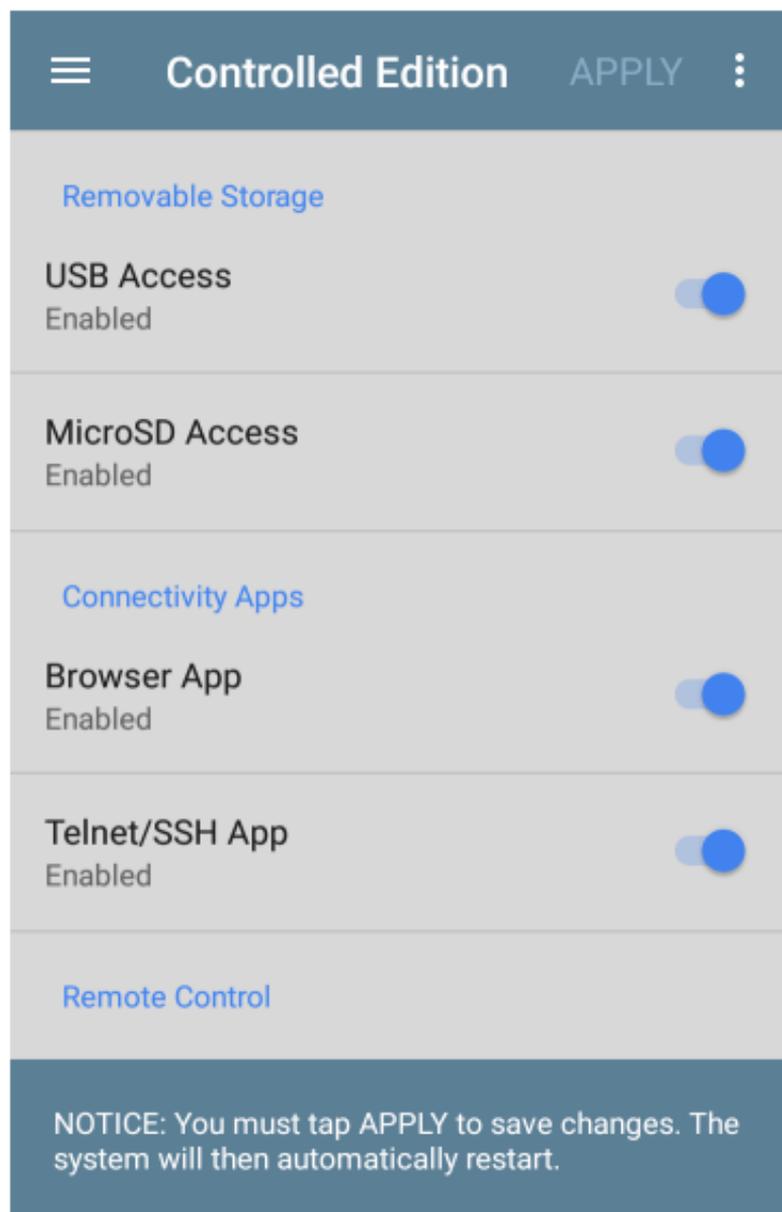
要更改对受控功能的访问权限，请点击溢出菜单图标 ，然后选择 **设置** 选项。



出现提示时，输入管理员密码并选择确定按钮。



功能访问 屏幕显示了受控功能的当前状态，并允许您使用切换按钮

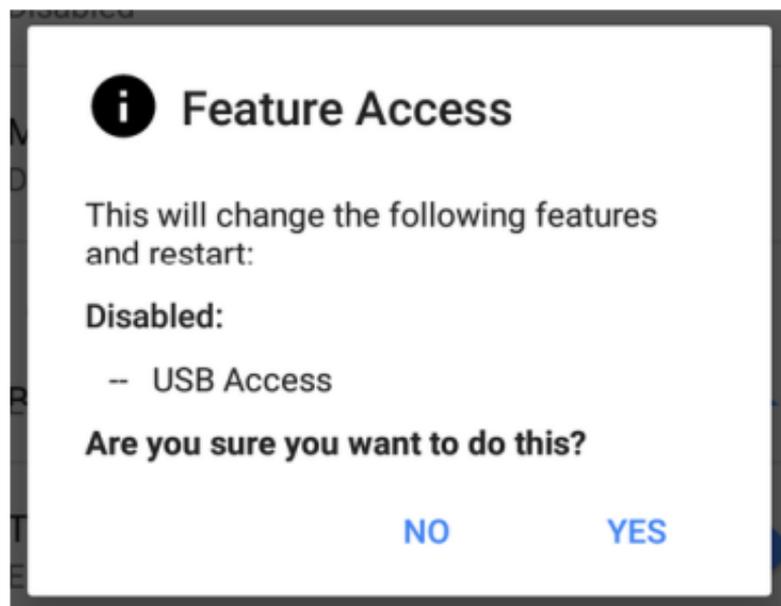


如果进行了更改，屏幕顶部的应用按钮将变为活动状态。



选择应用作为完成更改的第一步。

将显示一条消息，其中列出了待处理的功能更改。



- 选择是来应用更改的配置
- 选择否取消更改并返回到设置屏幕

应用更改后，设备会自动重新启动。

要查看受控功能的状态，请访问 功能访问状态屏幕。



Feature Access



LinkRunner AT Tester

Removable Storage

USB Access Disabled

Connectivity Apps

Browser App Disabled

Telnet/SSH App Disabled

Remote Control

VNC Disabled

Documenting

Packet Capture Enabled

Network Discovery Enabled

Link-Live Cloud Service

Link-Live Access Enabled

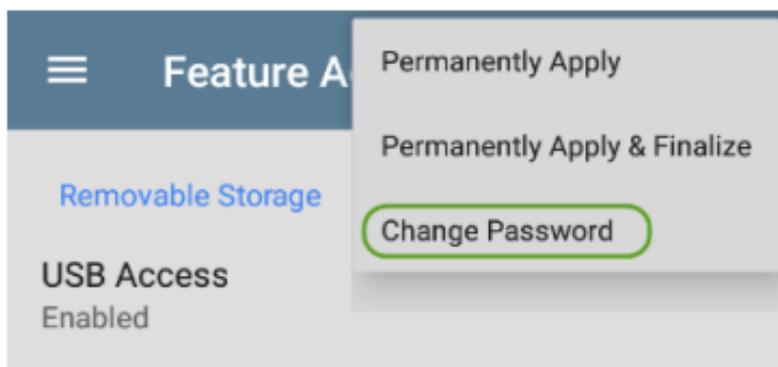
Download from App Store Enabled

更改管理密码

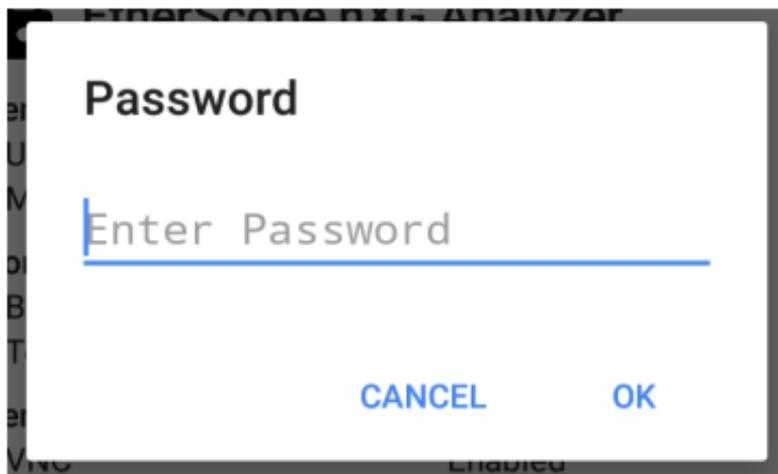
NetAlly建议在配置功能控制时,更改出厂设置的管理员密码,以防止非管理员用户访问的功能控制屏幕。

要修改管理员密码:

1. 依照 [控制功能可用性](#) 中的步骤,访问功能控制选择屏幕。
2. 在选择屏幕上,点击屏幕顶部的溢出菜单图标  以显示溢出菜单。



3. 选择 **更改密码** 以显示当前密码输入屏幕。



4. 输入当前的管理员密码, 然后点击 **确定** 继续。(选择 **取消** 以返回到 功能控制 选择屏幕, 不进行任何更改。)

注意: 出厂设置的管理员密码是: **admin**

5. 等待新密码输入屏幕显示, 将新密码输入到两个字段中, 然后点击 **确定** 完成管理员密码更改。(选择 **取消** 以返回到 功能控制 选择屏幕, 不更改当前管理员密码。)

注意, 只有当新密码字段中包含匹配的条目时, 您才能完成管理员密码更改。

New Password

Enter new password

Confirm new password

CANCEL

OK



LRAT 3000-4000测试应用

用户指南的这一部分描述了NetAlly-开发的网络测试应用程序。每个应用程序都专为快速分析和直观操作而设计，以增强和简化您的网络任务。

通过从主屏幕或应用程序屏幕中选择其图标来打开测试应用程序。



AutoTest 应用程序 和配置文件

AutoTest 是最全面的 NetAlly 测试应用程序 LRAT 3000-4000. 您可以快速运行各种测试类型并保存它们的配置和网络凭据, 以便在需要时进行访问. 该应用程序可通过测试“配置文件”完全自定义 [有线](#) 网络连接, 而且单一的 [测试目标](#)

AutoTest 建立了 [Wired Test Port connection](#) 由其他测试应用程序使用, 例如。

AutoTest 结果会自动上传到 [Link-Live](#) 云服务一旦你注册了你的 LRAT.

自动测试章节内容

本章介绍自动测试配置文件、屏幕、设置和测试结果。

自动测试概述

管理配置文件和配置文件组

主自动测试屏幕

定期自动测试 (仅限 LRAT-4000)

有线自动测试配置文件

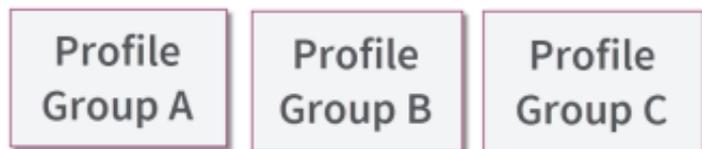
DHCP、DNS 和网关测试

Test Targets

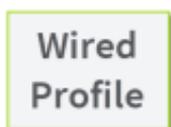
自动测试概述

AutoTest 包含三个不同的测试级别: 测试目标, 配置文件, 和 配置文件组. 您可以根据需要创建任意数量的配置文件组、配置文件和测试目标。

Profile Groups



Profiles



Test Targets



最底层是一组单一 测试目标 连接到网络服务, 例如 Web 应用程序或 FTP 站点。测试目标定义参数, 包括类型、目标 URL/IP 地址、端口号和通过/失败阈值。更复杂的测试, 如 HTTP, 允许进一步的通过/失败标准, 例如必须或不得包含在 HTTP 正文中的字符串。测试目标可以添加到任意数量的 配置文件。

一个配置文件包含一系列单独的网络测试。有一种配置文件类型：有线，其中包括有线 VLAN 的连接测试和凭据。配置文件提供了一种自动化且一致的方式来验证从第 1 层到第 7 层的网络。

配置文件可以添加到任意数量的配置文件组。

一个配置文件组 **p** 是自定义命名的配置文件集合。配置文件组旨在通过单击“开始”按钮进一步自动化测试多个网络或网络元素。

一个测试目标可以在任意数量的配置文件中，一个配置文件可以在任意数量的配置文件组中。

例如，您可以：

- 在 Trunk 端口上测试多个有线 VLAN。
- 从会议室测试有线和 Wi-Fi 访问。

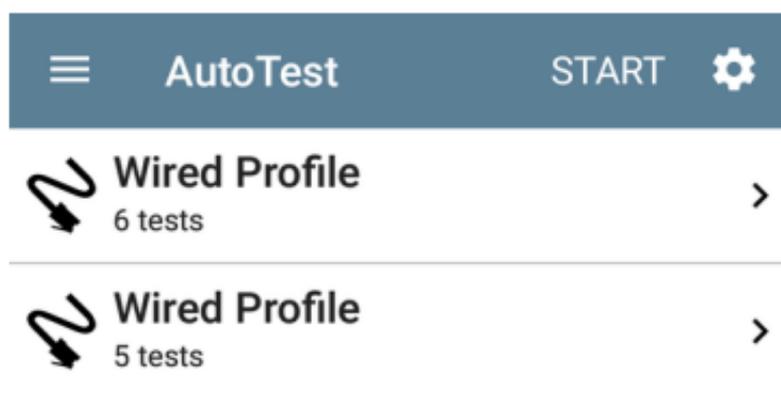
管理配置文件和配置文件组

配置文件是一系列或一组测试，旨在分析您网络的不同特征。这个 LRAT 3000-4000 AutoTest 应用程序功能 一种类型的测试配置文件：

有线配置文件 测试铜缆和光纤连接。

出厂默认配置文件

LRAT 以默认版本开始 AutoTest 配置文件类型，您可以根据自己的目的自定义、删除或替换这些类型。



要使用所需的网络设置和自定义名称自定义每个配置文件，请先轻触配置文件名称，然后选择配置  图标

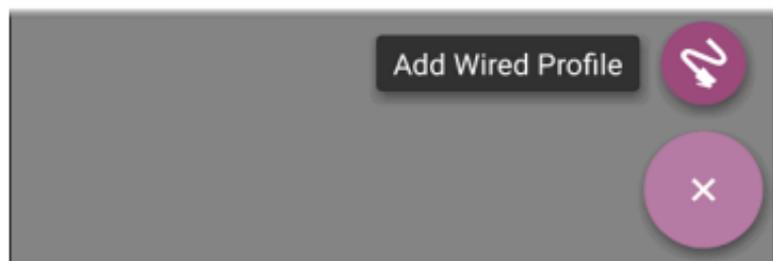
注意: 触摸 AutoTest 主屏幕(如上所示)上的设置图标会打开[自动测试设置和配置文件组](#)屏幕, 而不是个人配置文件设置。

- 默认的有线配置文件一旦您的设备通电并且有活动的以太网连接在设备上可用, 它就会自动运行并建立有线链接[顶端的RJ-45端口](#)。
- LinkRunner AT 4000 的默认有线配置文件包含 HTTP 测试目标。LinkRunner AT 3000 的默认配置文件包含 Ping 测试。

注意: 默认有线配置文件不会通过光纤链路自动运行。您必须在 AutoTest 中触摸 **START** 才能在光纤连接上运行有线配置文件。

添加新配置文件

要将新的测试配置文件添加到当前的 AutoTest, 请点击[浮动操作按钮 \(FAB\)](#)在自动测试屏幕上。



将显示配置文件的配置屏幕 请参阅每个配置文件类型的主题以了解其设置的说明。

配置配置文件的设置后, 点击后退按钮  在屏幕底部打开并运行新的测试配置文件。

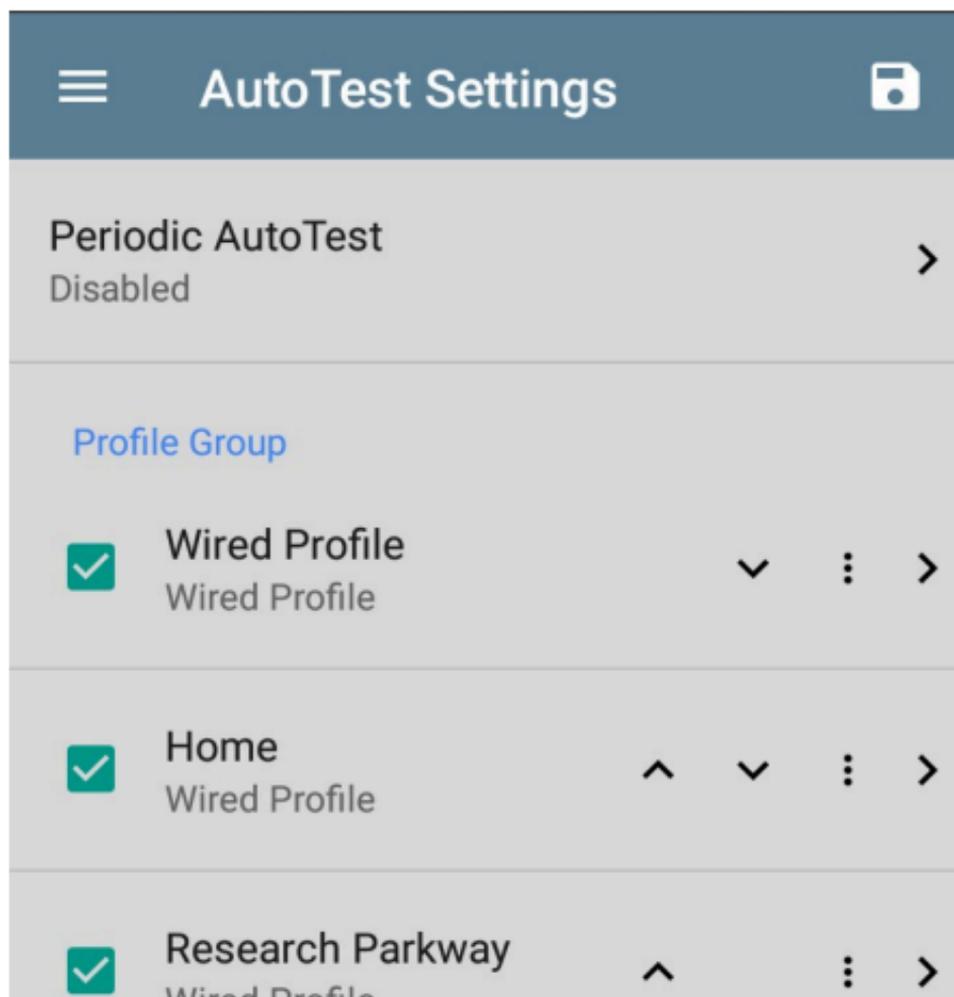
配置组

LRAT 3000-4000还允许您保存配置文件组。配置文件组很简单包含的测试配置文件列表及其运行顺序当您开始自动测试时。(看[自动测试概述](#)有关配置文件组的更多说明。)您可以为不同的位置、作业、网络或其他目的配置和选择配置文件和配置文件组。要管理您的个人资料和个人资料组,请轻触设置  按钮(带有配置文件列表)。

自动测试设置屏幕

自动测试设置屏幕包含[定期自动测试](#)和配置文件组设置。

注意:定期自动测试仅适用于 LRAT-4000。



您可以在“自动测试设置”屏幕上执行以下操作：

- 选中或取消选中复选框以在当前活动的配置文件组中包含或排除测试配置文件。

- 点击向上和向下箭头  重新排序此配置文件和配置文件组的主自动测试屏幕上的测试配置文件。
- 触摸操作溢出图标  到复制或删除一个配置文件

警告: 删除配置文件时, 它会从所有配置文件组中删除。要从当前组中删除配置文件, 只需取消选中它。

- 触摸任何配置文件的名称以打开配置文件的测试和连接设置。
- 触摸保存图标  执行以下操作:

- 加载: 打开以前保存的设置配置, 其中包括配置文件组。
- 另存为: 使用现有名称或新的自定义名称保存当前设置和配置文件组。

参考 [保存应用程序设置配置](#)。

- 导入: 导入以前导出的设置文件。
- 导出: 创建当前设置的导出文件, 并将其保存到内部或连接的外部存储。

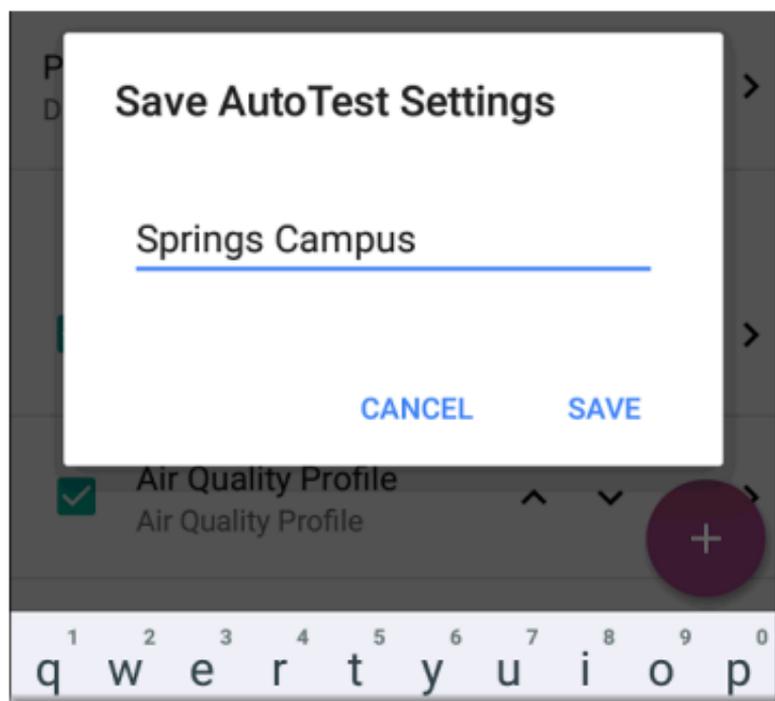
参考 [导出和导入应用程序设置](#) 更多细节。

每个配置文件组可以运行一个或多个配置文件类型的。已保存的配置文件可在所有配置文件组中使用。

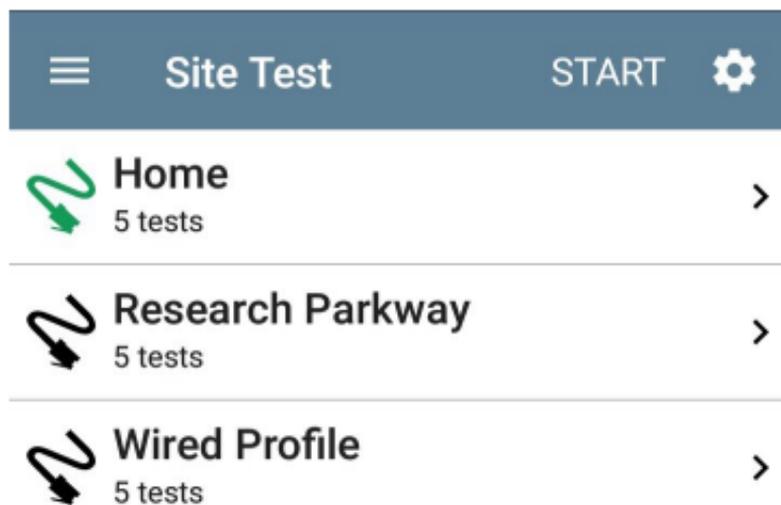
自定义自动测试设置/配置文件组名称

默认情况下，AutoTest 应用程序屏幕在标题中显示“AutoTest”，而 AutoTest Settings 屏幕标题是“AutoTest Settings”。保存自定义名称后，该名称将显示在 AutoTest 应用程序标题和 AutoTest 设置屏幕标题中。

在下面的示例中，用户保存名为“Springs Campus”的自定义 AutoTest 配置。



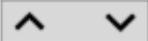
主 AutoTest 应用程序屏幕现在在标题中显示自定义名称。

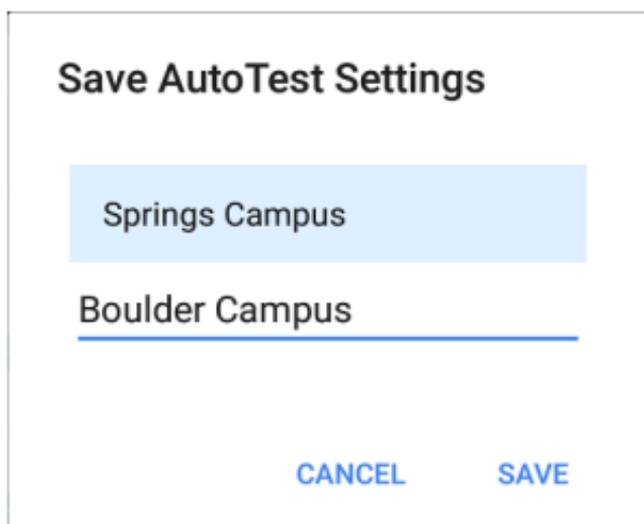


创建新的配置文件组

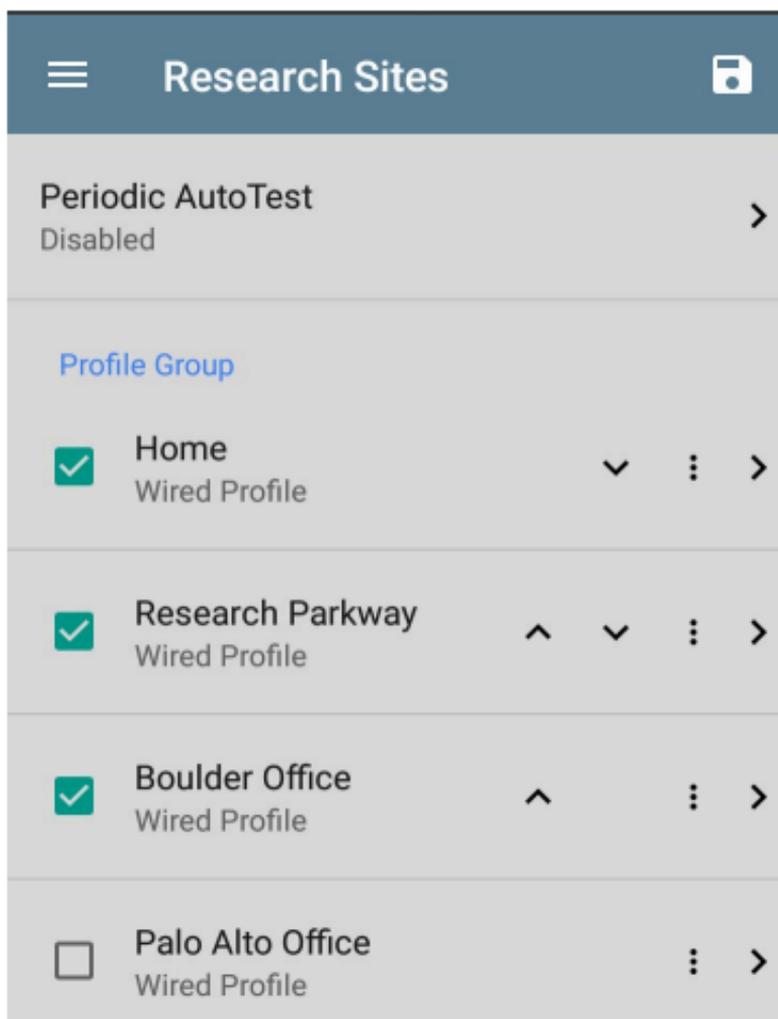
要创建新的配置文件组，请按照下列步骤操作：

1. 通过触摸转到自动测试设置和配置文件组屏幕  在主自动测试屏幕上。
2. 取消选中您不希望包含在新配置文件组中的任何配置文件的复选框。
3. 轻触 FAB  添加要包含在新配置文件组中的新测试配置文件。

4. 点击向上和向下箭头  更改测试配置文件运行的顺序。离开并重新访问此屏幕后，未选中的配置文件会自动移至列表底部。
5. 轻触 ，并选择另存为将打开一个对话框，您可以在其中输入新名称。



6. 输入新的配置文件组名称，然后点击保存。The LRAT 返回到配置文件组屏幕，新组名称显示为标题。



导入和导出自动测试配置

除了创建新的配置文件或使用默认值,您还可以:

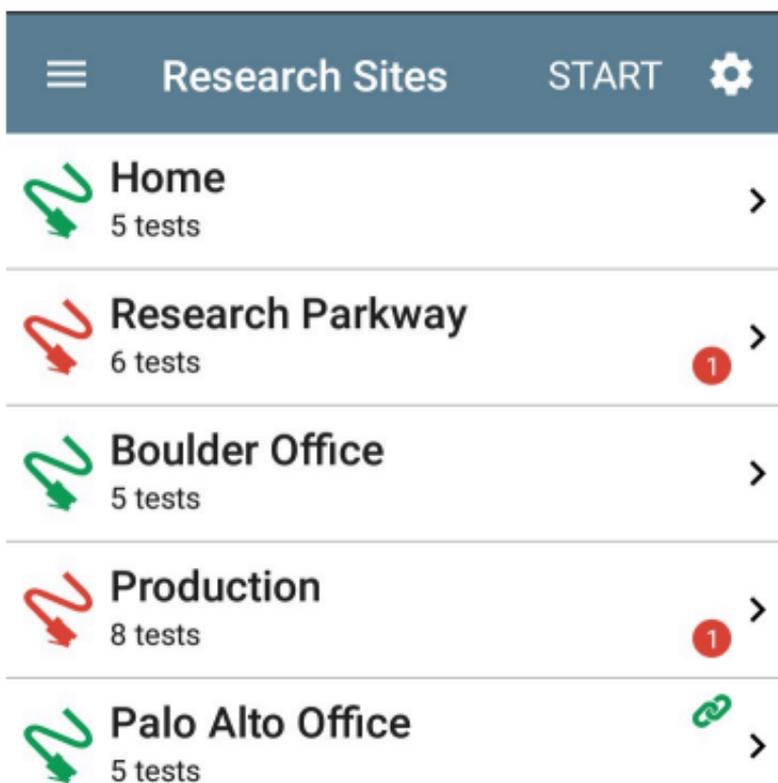
- 将配置文件设置导入和导出到任何连接的外部或内部存储。参考 ["导出和导入设置" on page 95.](#)

- 使用Link-Live云服务以近乎实时的方式将配置文件传输到其他设备。参考 "[通过Link-Live将自动测试的设置导入到其他设备](#)" on page 99.

主自动测试屏幕

要打开 AutoTest 应用程序，请触摸 AutoTest 图标 ，该图标在 [主屏幕上](#)。

点击 **START** 按钮在主自动测试屏幕上运行当前活动的 [配置文件组](#) 中的所有配置文件。



AutoTest 屏幕显示与配置文件、测试或测量类型相对应的图标。运行后，这些图标会改变颜色以指示测试状态：

- **绿色**表示在设定的阈值内测试或测量成功。
- **黄色**表示警告条件。
- **红色**表示测试失败。

每个测试配置文件中警告或失败的数量也显示在每个配置文件卡右侧的彩色圆圈中： (2 个警告, 1 个失败)。控制彩色测试分级的阈值可在设置中进行调整  每个配置文件和测试类型的屏幕。

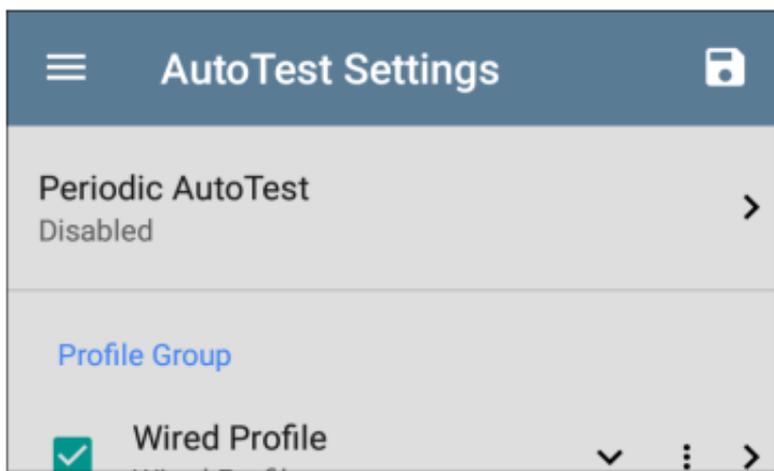
绿色链接图标  表示活动的网络连接。

每个配置文件和测试都汇总在一张卡片上。触摸配置文件或单个测试的卡片以打开并查看测试结果详细信息, 包括任何警告或失败的原因。

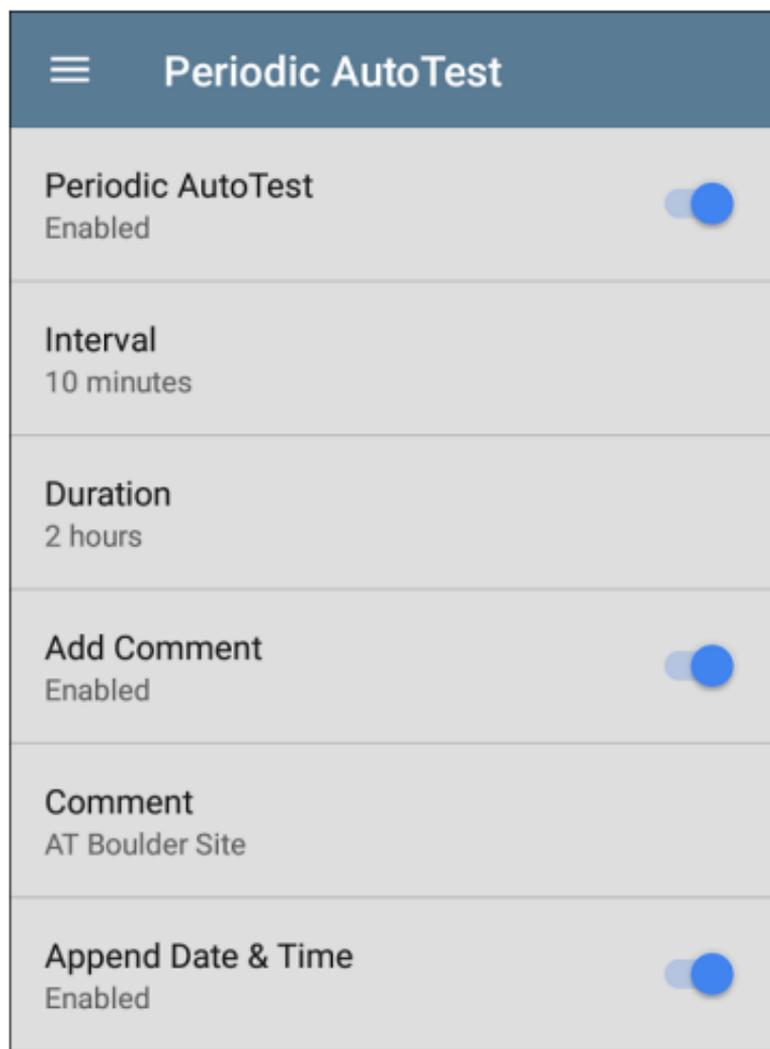
定期自动测试

注意：定期自动测试仅适用于 LRAT-4000。

定期自动测试设置



显示定期自动测试设置屏幕。



触摸定期自动测试字段以启用，并根据需要调整以下设置。

间隔：每次自动测试运行之间的时间量

持续时间：定期自动测试运行的总时间长度

添加注解：启用此设置可让您在 Link-Live 云服务中为定期自动测试结果附加注释。评

论作为标签出现在 Link-Live.com 结果页面。此设置和注解默认情况下启用以下设置。

注解:如果添加注释设置已启用。在 **Link-Live** 上输入要附加到上传的定期自动测试结果的标签。默认值为“定期自动测试”。

附加日期&时间:如果添加评论设置已启用并在末尾添加数字日期和时间注解

运行定期自动测试

轻触开始在主自动测试屏幕上开始定期自动测试。自动测试在选定的持续时间内以设置的间隔继续运行,或者直到您触摸停止自动测试。

The screenshot shows the AutoTest interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "Research Sites" in the center, and a "STOP" button on the right. Below the header, there are three entries for research sites, each with a colored icon (green or red) and a right-pointing chevron:

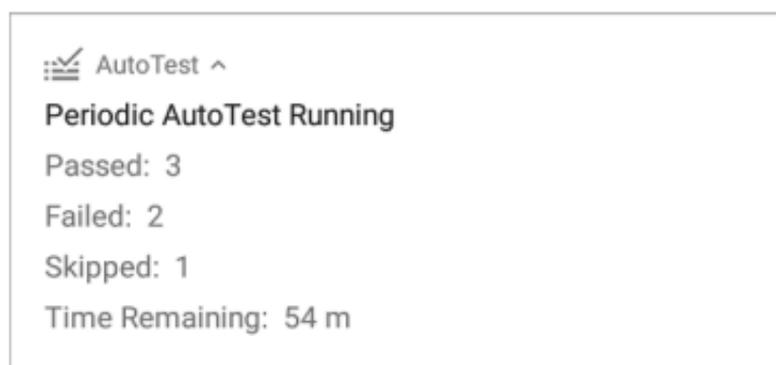
- Research Parkway**: 5 tests, green icon.
- Production**: 7 tests, red icon, and a red circle with the number "1" to its right.
- Palo Alto Office**: 5 tests, green icon, and a green icon to its right.

Below the site list is a grey rectangular area, followed by a dark blue box containing the following text:

Periodic AutoTest Status
Passed: 5
Failed: 3
Time Remaining: 2 m
Next: 13 s

定期自动测试状态汇总在自动测试屏幕的底部。为整个配置文件组的每次运行报告通过和失败，而不是单个配置文件。如果在下一个时间间隔发生时前一个间隔的测试仍在运行，则将跳过定期自动测试，从而无法开始下一次运行。

定期自动测试图标  出现在顶部状态栏。当定期自动测试正在运行或已完成时。在状态栏上向下拖动以查看相应的通知。



注意: AutoTest 具有优先控制权测试端口, 所以其他应用程序, 包括发现, 自动测试完成时暂停。

DHCP, DNS, 和网关有线 测试

DHCP	10.250.2.168	>
	<1 ms	
DNS	Compass	>
	16 ms	
	10.250.0.1	>
	2 ms, 2 ms, 4 ms	

这些测试包含在[有线](#)自动测试配置文件。

从有线配置文件设置屏幕或通过触摸设置按钮访问 AutoTest 的 DHCP、DNS 和网关设置  从每个测试类型的完整结果屏幕。

轻触[蓝色链接](#)或蓝色动作溢出图标  在测试结果屏幕上进行其他操作。

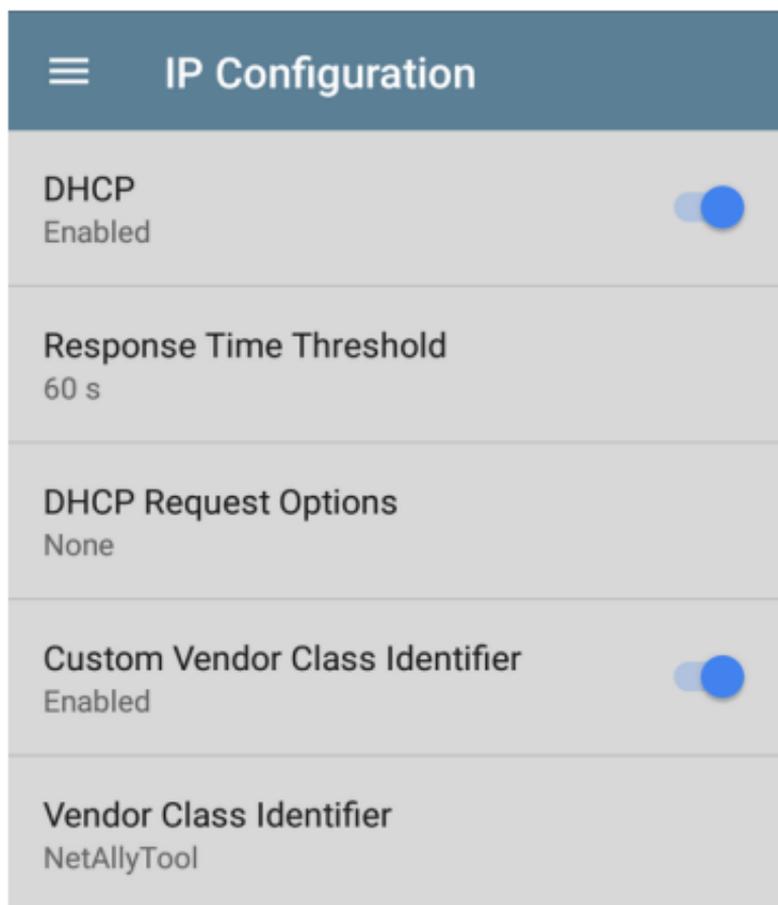
DHCP 或静态 IP 测试

DHCP(动态主机配置协议)测试表明LRAT从DHCP服务器接收IP地址分配。

DHCP 设置 - IP 配置

打开“IP Configuration”界面,可以:

- 打开一个有线配置文件,点击 DHCP 摘要卡,然后在 DHCP 测试结果页上点击设置按钮 。
- 点击主菜单图标 , 选择 **AutoTest Settings**打开一个有线配置文件,然后点击 **IP Configuration**。



DHCP

DHCP 默认启用。点击切换按钮可禁用 DHCP 并输入静态 IP 地址，如下所述。

(仅限 DHCP) 响应时间阈值

(仅当启用 DHCP 时显示。) 点击此字段选择一个值或输入自定义值来设置在 DHCP 测试失败之前 LRAT 等待 DHCP 服务器响应的的时间。

DHCP 请求选项

(仅当启用 DHCP 时才显示。) 点击此字段可以选择一个或多个 DHCP 请求选项。

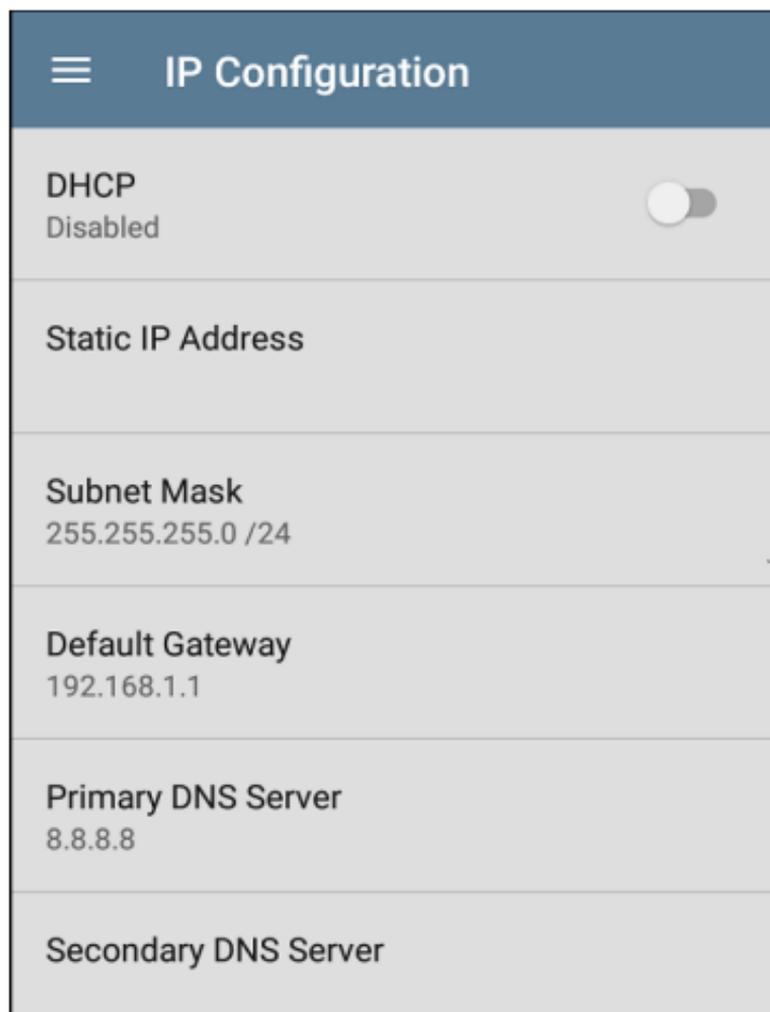
自定义供应商类别标识符

默认情况下, 自定义供应商类别标识符处于禁用状态。点击切换按钮可启用供应商类别标识符字段, 如下所述。

供应商类别标识符

(仅当启用自定义供应商类别标识符时才出现。) 点击此字段可键入供应商类别标识符。

静态 IP 地址



IP Configuration	
DHCP	<input type="checkbox"/>
Disabled	
Static IP Address	
Subnet Mask	255.255.255.0 /24
Default Gateway	192.168.1.1
Primary DNS Server	8.8.8.8
Secondary DNS Server	

静态 IP 地址字段用于子网掩码, 默认网关, 和首选和 辅助 **DNS** 服务器仅在禁用 DHCP 时出现。触摸每个字段以打开弹出式数字键盘并根据需要输入静态地址。触碰 **OK** 以保存您的设置。

DHCP 测试结果

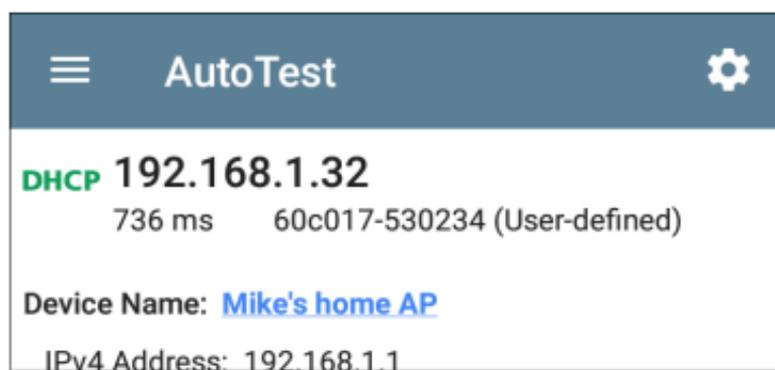
当 DHCP 启用后，DHCP 测试卡和结果页将显示在配置文件中。



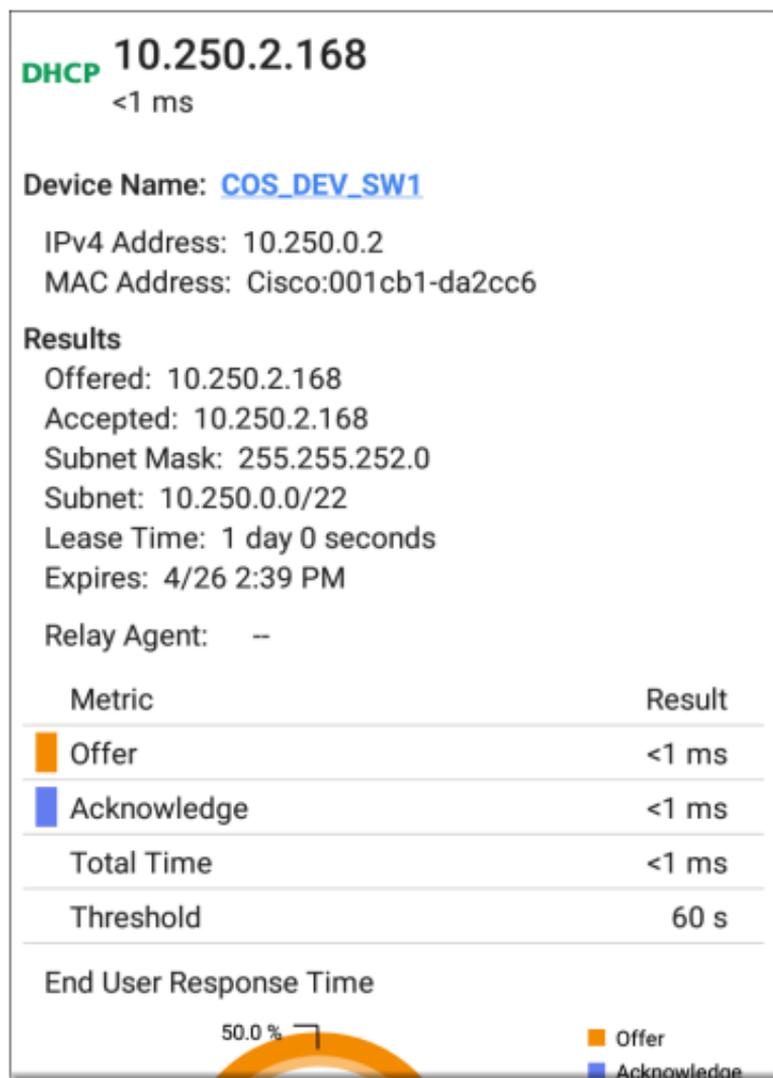
DHCP 测试卡显示 DHCP 服务器的 IP 地址以及完成发现、提供、请求和确认的总时间。

轻触卡片以打开 DHCP 测试页。

注意：如果一个用户定义的 **MAC** 已为此有连接在 [常规设置](#)，(用户定义) 出现在结果屏幕上 DHCP IP 地址下方的 MAC 地址旁边。



DHCP测试结果屏幕



设备名称:发现的 DHCP 服务器名称, 如果没有发现名称, 则为 IP 地址

IPv4地址: 服务器的IP地址

MAC地址:服务器的 MAC 地址。两个破折号 -- 表示没有从服务器提供 MAC 地址。

结果

提供: DHCP 服务器提供的 IP 地址

接受: 接受的 IP 地址 LRAT

子网掩码: 用于确定哪些地址是本地地址, 哪些必须通过网关到达

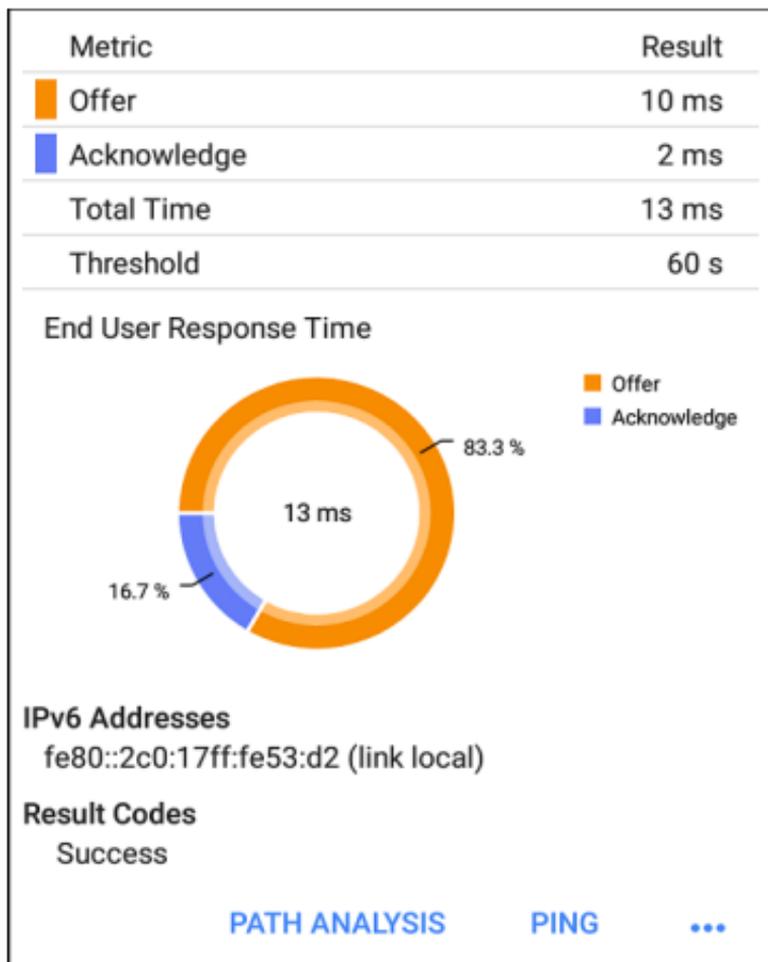
子网: 子网掩码和提供的 IP 地址的组合

租期: IP 地址被租用的时间 LRAT 通过 DHCP 服务器

过期: IP 地址的到期日期和时间

中继代理: 如果存在 BOOTP DHCP 中继代理, 则此字段显示其 IP 地址。中继代理在不同 IP 网络上的 DHCP 客户端和 DHCP 服务器之间中继 DHCP 消息。

最终用户响应时间表和图表: 获取 DHCP IP 地址过程的时间细分



提供: 之间的时间LRAT发送发现并从 DHCP 服务器接收地址提议

确认: 之间的时间LRAT发送请求并接受来自 DHCP 服务器的确认

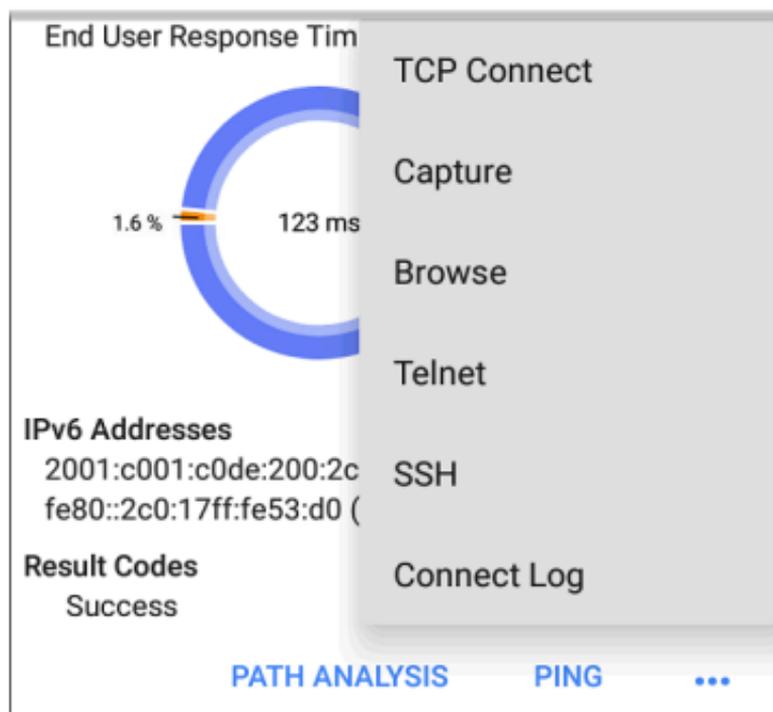
总时间: DHCP 进程消耗的总时间

阈值:来自 DHCP 测试设置的 DHCP 响应时间阈值,它控制多长时间LRAT在 DHCP 测试失败之前等待 DHCP 服务器响应。

最终用户响应时间:饼图以百分比形式显示要约和确认时间

IPv6 地址:通过路由器通告获得的地址

结果代码:测试的最终状态(成功或失败)

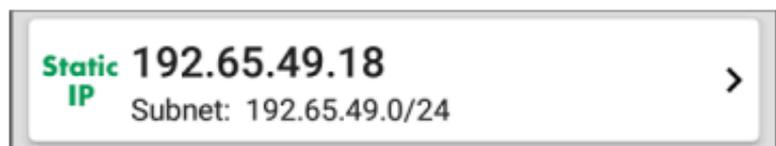


DHCP 测试页上可用的其他操作包括打开[路径分析](#), [Ping/TCP](#), or [抓包](#)填充了 DHCP 服务器地址的应用程序,在 Web 浏览器中浏览到

IPv4 地址, 启动 [Telnet](#) 或者 [SSH](#) 连接, 或者查看 [连接日志](#).

静态 IP 测试结果

如果禁用了 DHCP, DHCP 测试将变成“静态 IP”测试, 并显示在 DHCP 测试设置中输入的子网和地址。



静态 IP 卡显示配置的 IP 和子网地址。
触摸卡片以打开测试结果屏幕。

The screenshot shows the AutoTest application interface. At the top, there is a blue header bar with a hamburger menu icon on the left, the text "AutoTest" in the center, and a gear icon on the right. Below the header, the main content area displays network configuration information:

- Static IP** 192.65.49.18
 - Subnet: 192.65.49.0/24
- Subnet Mask: 255.255.255.0
- Gateway: [192.168.1.1](#)
 - IP Address: 192.168.1.1
- DNS 1: [8.8.8.8](#)
 - IP Address: 8.8.8.8
- DNS 2: --
 - IP Address: --
- IPv6 Addresses
 - fe80::2c0:17ff:fe53:d2 (link local)
- Result Codes
 - Success

静态 IP 测试屏幕显示配置的地址。

子网: 子网掩码和提供的 IP 地址的组合

子网掩码: 用于确定哪些地址是本地地址, 哪些必须通过网关到达

网关: 如果找不到名称, 则解析网关的主机名或其 IP 地址

IP地址: 网关的IP地址

DNS (1 和 2): 主要和次要 DNS 服务器的名称和 IP 地址

IPv6 地址: 通过路由器通告获得的地址

结果代码: 测试的最终状态(成功或失败)

重复的 IP 地址

DHCP 和静态 IP 测试还会检测并报告是否存在使用相同 IP 地址(重复 IP)的设备。如果配置的地址正在使用中,则自动测试失败。

● IP Address In Use By: [BRW2C6FC94A974E](#)

MAC Address: HonHai:2c6fc9-4a974e

IPv6 Addresses

fe80::2c0:17ff:fe53:d2 (link local)

Result Codes

IP address already in use (11)

正在使用的 IP 地址: 显示当前使用配置的静态 IP 地址的设备名称。触摸带有蓝色下划线的链接以打开[发现详情屏幕](#)

MAC地址: 使用IP地址的设备的MAC

DNS测试

有关概述信息, 请参阅[DHCP](#)、[DNS](#) 和 [网关测试](#)。

DNS(域名系统) 服务器测试检查解析指定 URL 的 DNS 服务器的性能。这LRAT通过 DHCP或静态地址配置获取DNS地址。

DNS Test Settings

DNS Test	
DNS Test Enabled	<input checked="" type="checkbox"/>
Lookup Name www.google.com	
IP Protocol Version IPv4	
Lookup Time Threshold 1 s	
Reverse Grading Disabled	<input type="checkbox"/>

DNS测试

如果需要，您可以点击 DNS 设置页上的顶部字段并切换开关以禁用当前自动测试中的 DNS 测试。DNS 卡仍显示在主自动测试结果页面上，因此您仍可以看到 DNS 服务器的地址。但是，以下查找值设置为“--”，结果代码设置为“测试已禁用”。

查找名称

这是 DNS 服务器尝试解析的 URL。触摸该字段以输入默认 URL 以外的 URL: `www.-google.com`。

IP协议版本

触摸该字段可在 IPv4 和 IPv6 之间切换。

查找时间阈值

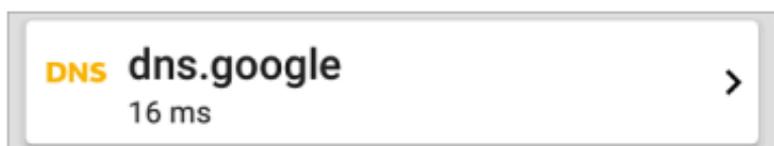
这个阈值控制了多长时间 LRAT 在测试失败之前等待来自 DNS 服务器的响应。默认值为 1 秒。触摸该字段以选择或输入新阈值。

反向评价

启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

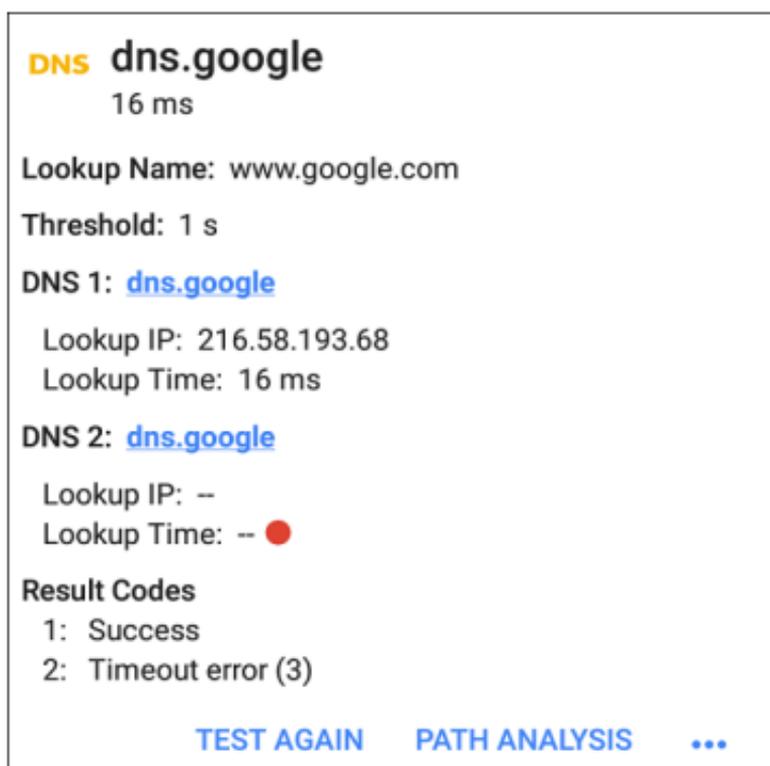
DNS 测试结果

DNS 1 的服务器名称和查找时间显示在 DNS 测试卡上。



触摸卡片以打开 DNS 测试结果屏幕。

DNS 测试结果页面



查找名称: DNS 服务器解析的名称

阈值: 来自 DNS 测试设置的查找时间阈值

DNS #: 列出的 DNS 服务器的名称:

查找IP: 解析IP地址

查找时间: 发送查找请求后接收IP地址的时间

结果代码: 每个 DNS 服务器的测试的最终状态(成功或失败)

14 ms

Lookup Name: www.google.com

Threshold: 1 s

DNS 1: [dns.google](#)

Lookup IP: 172.217.11.

Lookup Time: 14 ms

DNS 2: [dns.google](#)

Lookup IP: 172.217.11.

Lookup Time: 14 ms

Result Codes

1: Success

2: Success

Ping

TCP Connect

Capture

Browse

Telnet

SSH

TEST AGAIN PATH ANALYSIS ...

轻触 [蓝色链接](#) 或蓝色动作溢出图标 **...** 在测试结果屏幕底部运行 DNS 再次测试, 打开另一个填充有 DNS 1 的名称和 IP 地址的应用程序, 或浏览到 Web 浏览器中的主 DNS 服务器。

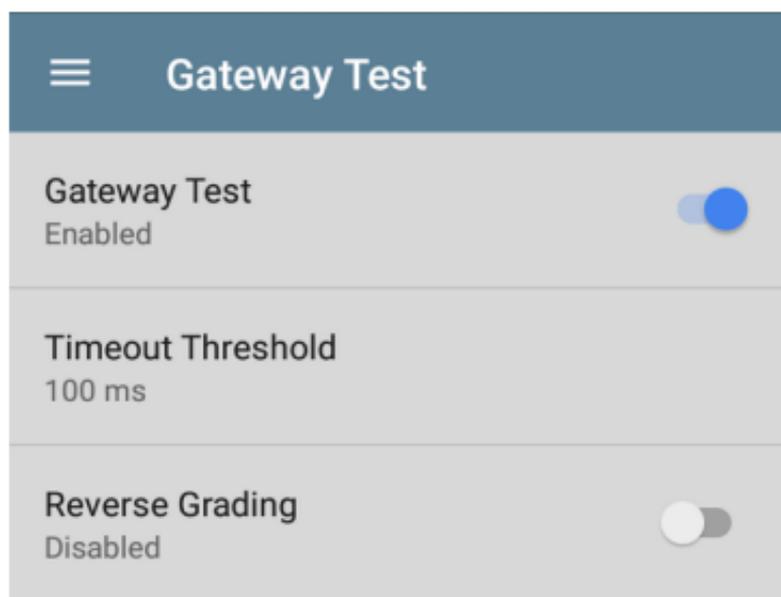
[返回标题和内容](#)

网关测试

有关概述信息，请参阅 [DHCP](#)、[DNS](#) 和 [网关测试](#)。

此测试指示是否可以成功 ping 默认网关并识别当前 IPv4 和 IPv6 路由器的地址。

网关测试设置



网关测试

要禁用当前 AutoTest 中的网关测试，请点击此屏幕的顶部字段将其设置为已禁用。网关卡仍显示在主 AutoTest 结果屏幕上，因此您仍然可以看到网关服务器的地址。但是，以

下查找值设置为“--”，并且结果代码设置为“Test is disabled”。

超时阈值

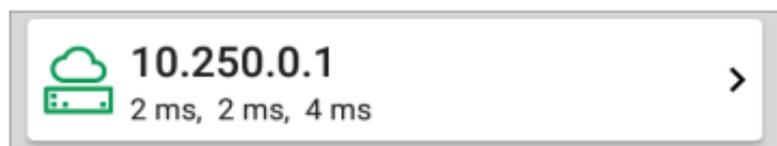
表示LRAT在将测试被评定为失败之前等待网关响应的的时间。点击字段以选择值选项之一，或输入自定义值。

反向评价

启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

网关测试结果

LRAT从DHCP或静态IP配置中获取网关的IP地址，并使用SNMP获取系统组信息和服务端口的统计信息LRAT的子网。参考[发现设置](#)有关的信息[SNMP配置](#)。



网关测试卡显示网关的IP地址和三个Ping响应时间。

网关测试结果页面



The screenshot shows the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and a gear icon on the right. Below the header, the main content area has a white background. It starts with a green cloud icon and a server rack icon, followed by the text "COS_DEV_SW1" and "2 ms, 2 ms, 3 ms". Below this, there are three sections: "IPv4 Gateway Name: COS_DEV_SW1" with sub-headers for "IPv4 Address: 10.250.0.1" and "MAC Address: Cisco:00000c-07ac01"; "IPv6 Gateway Name: Andromeda Automation Procurve"; and "Protocols: RIP, OSPF, HSRP, Statically Configured Router, Proxy ARP Agent, Virtual Router (HSRP)". A "Ping Results" section follows, showing "Response Times: 2 ms, 2 ms, 3 ms" and "Threshold: 100 ms". Below that is a "Result Codes" section with three entries: "1: Success", "2: Success", and "3: Success". At the bottom of the white area, there are three blue buttons: "TEST AGAIN", "PATH ANALYSIS", and an ellipsis "...".

IPv4 网关名称: 解析的网关主机名或其 IP 地址, 如果找不到名字。

IPv4 地址: 网关的内部 IPv4 地址。

MAC 地址: 服务器的 MAC 地址。两个破折号 -- 表示没有从服务器提供 MAC 地址。

IPv6 地址:路由器的 IPv6 地址(如果可用)。

IPv6 网关名称:IPv6 路由器通告的名称(如果可用)。

协议:路由协议LRAT用于获取网关数据

Ping 结果

- 响应时间从发送到网关的三个 Ping。
- 阈值:网关设置中配置的网关超时阈值。

结果代码:三个网关 Ping 中每一个的测试的最终状态(成功或失败)。

COS-IT-SW1.netally.com
1 ms, 1 ms, 1 ms

Gateway Name: [COS-IT-S](#)

IPv4 Address: 172.24.0
MAC Address: Cisco:6c
IPv6 Address: --

Protocols: Statically Cont

Ping Results
Response Times: 1 ms,
Threshold: 100 ms

Result Codes
1: Success
2: Success
3: Success

Ping
TCP Connect
Capture
Browse
Telnet
SSH

[TEST AGAIN](#) [PATH ANALYSIS](#) ...

轻触 [蓝色链接](#) 或蓝色动作溢出图标 [...](#) 在测试结果屏幕底部运行网关再次测试, 打开另一个应用程序, 浏览到网关的 IPv4 地址, 或启动一个 [Telnet](#) 或者 [SSH](#) 到网关的会话。

测试目标 有线 测试

PING	google	>
	28 ms, 28 ms, 15 ms	
TCP	NetAlly	>
	80 ms, 76 ms, 82 ms	
HTTP	github	>
	1.114 s	
FTP	Asset Server	>
	246 ms	

AutoTest Target 测试是用户可分配的端点，LRAT 3000-4000每次自动测试配置文件运行时尝试连接。这些测试可确保内部或外部网站、服务器和设备对网络用户的可用性。

点击下面的链接转到测试的主题：

AutoTest Target 测试是用户可分配的端点，每次 LRAT 3000-4000 运行AutoTest配置文件时都尝试连接到这些端点。这些测试确保内部或外部网站、服务器和设备对网络用户的可用性。

[Ping](#)

[TCP连接](#)

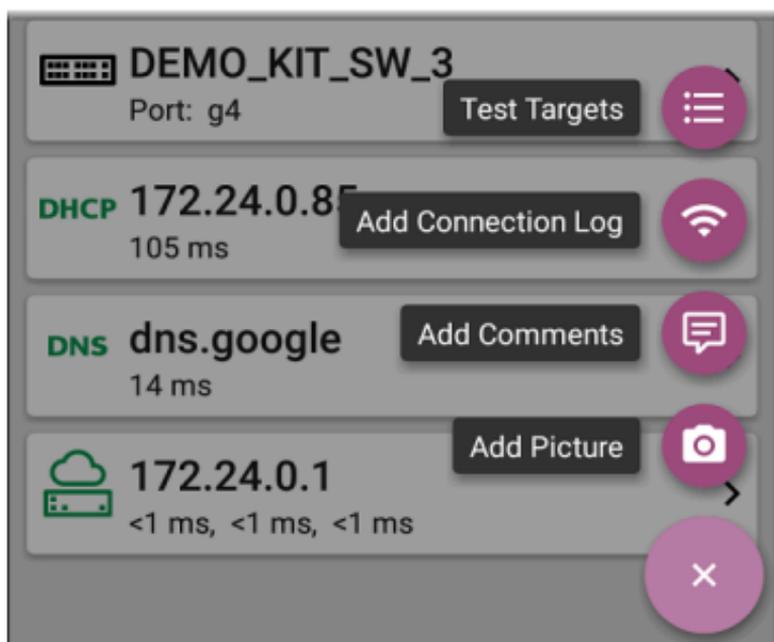
HTTP

FTP

注意:HTTP和FTP测试只在LinkRunner AT 4000上可用。

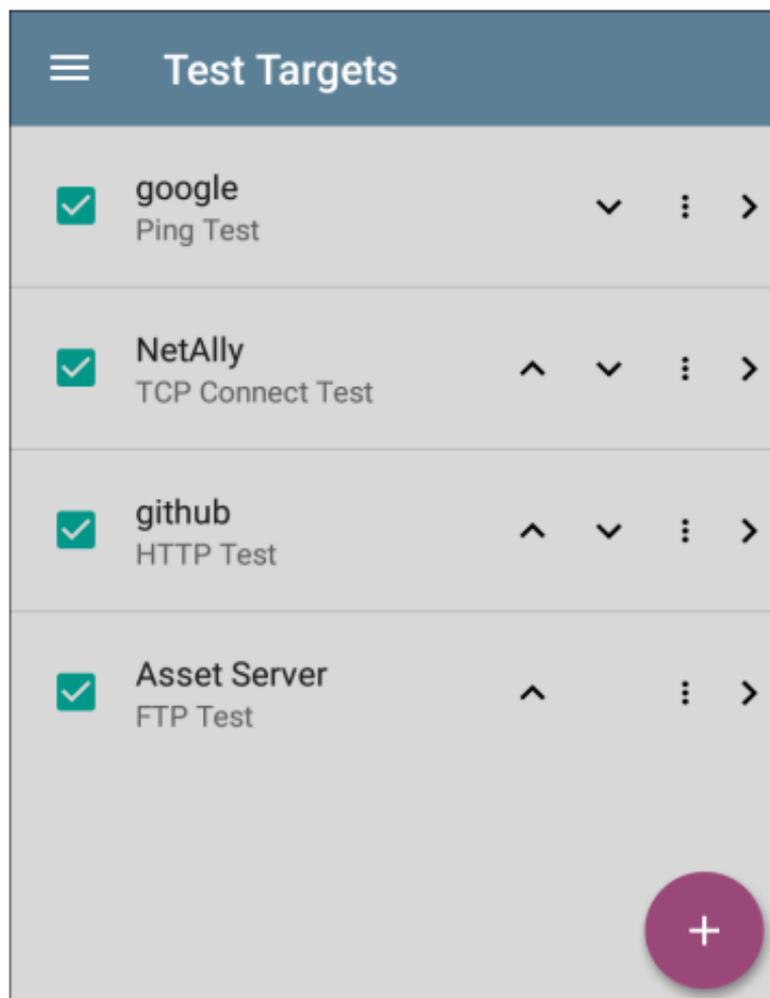
添加和管理测试目标

要向AutoTest配置文件添加测试目标并管理已保存的目标,请打开 **Test Targets** 页面从 [有线](#) 配置文件  或通过点击FAB  [有线](#) 结果页面。



测试目标页列出了所有已定义和保存的测试目标。选中的框表示在当前配置文件中启用

用的测试目标。请记住,测试目标可以添加到任意数量的 Wired Profiles.)



在测试目标页上,您可以执行以下操作:

- 选中要包含在当前配置文件中的每个目标的复选框.

- 点击向上和向下箭头在此页和主自动测试配置文件页上重新排序保存的测试目标。
- 点击操作溢出图标  可复制或删除目标测试。

注意：删除测试目标时，会将其从所有配置文件中删除。要从当前配置文件中删除测试目标，只需取消选中它即可。

- 点击 FAB icon  添加一个新的目标测试：Ping, TCP Connect, HTTP, 或者 FTP (FTP and HTTP 仅适用于 LinkRunner AT 4000)。



- 点击任何目标测试名称来打开该测试的设置。然后,您可以输入自定义测试名称,目标,地址或阈值。有关设置的更多详细信息,请参见:
 - [Ping 测试](#)
 - [TCP 连接测试](#)
 - [HTTP 测试](#) (LinkRunner AT 4000 适用)
 - [FTP 测试](#) (LinkRunner AT 4000 适用)

目标测试结果

目标测试类型图标显示绿色、黄色或红色以指示已完成测试部分的状态(或等级): **Success**/警告/失败.

例如,在下面的 Ping 测试图像中,整个 Ping 测试的评分为警告,因为在设置中配置的超时阈值内未返回第三个 Ping。

PING google

9 ms, 33 ms, --

Device Name: [172.217.1.196](#)

IPv4 Address: 172.217.1.196

MAC Address: --

Results

Lookup Time: 3 ms

Response Times: 9 ms, 33 ms, -- ●

Threshold: 250 ms

Result Codes

1: Success

2: Success

3: Timeout error (3)

第三个响应时间显示两个破折号——表示没有收到响应，在结果标题下，黄点指出第三个响应时间是警告的原因。此外，第三个结果代码将“超时错误”列为警告的原因。

其他目标测试操作

[TEST AGAIN](#)[PATH ANALYSIS](#)[...](#)

目标测试完成后，触摸任何蓝色链接以执行其他操作，包括打开其他测试应用程序。

- 触摸蓝色链接的设备名称以打开一个[发现](#)所选设备的详细应用程序屏幕。从那

里, 您可以打开其他应用程序并运行其他测试。

- 轻触 **重新测试** 再次运行目标测试。
- 轻触 **路径分析** 打开路径分析应用程序。路径 **Destination** 配置了当前目标。
- 触摸操作溢出图标 **•••** 打开已预先填充目标的列出的应用程序或工具, 例如:
 - 打开 **Ping/TCP** 具有当前目标地址的应用程序。
 - **抓包** 来自测试目标的流量。
 - 使用您的浏览器浏览到 Internet 上的目标 URL **web browser app**。
 - **Telnet** 或 **SSH** 打开 **Telnet/SSH tools** 使用当前目标地址。

自动测试 Ping 测试

Ping 测试向所选目标发送 ICMP 回显请求，以确定是否可以访问服务器或客户端以及响应所需的时间。AutoTest 目标 Ping 测试向目标发送三个 Ping 并报告响应时间。目标可以是 IPv4 地址、IPv6 地址或命名服务器 (URL 或 DNS)。

Ping 测试设置

Ping Test	
Name	google
Device Name	www.google.com
IP Protocol Version	IPv4
Frame Size (bytes)	64
Do Not Fragment	<input type="checkbox"/>
Timeout Threshold	1 s
Reverse Grading	<input type="checkbox"/>

名称

此字段允许您为测试分配自定义名称。该名称出现在配置文件中的目标测试卡上。

设备名称

输入要ping的服务器的IP地址或URL。如果您输入IP地址，则会跳过测试的DNS查找部分。

IP协议版本

默认使用IPv4。触摸该字段可在IPv4和IPv6之间切换。

帧大小(字节)

此设置指定有效负载和发送的标头的总大小。有效大小为64字节到1518字节。要沿到目标的路由测试最大传输单元(MTU)，请选择要测试的MTU帧大小，然后设置不分段设置成启用。

不分段

触摸切换按钮以启用。

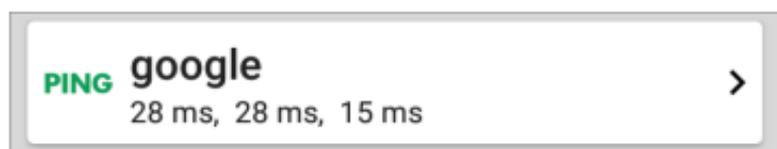
超时阈值:这个阈值控制多长时间LRAT在测试失败之前等待目标的响应。

反向评价

启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

例如，您可能有一个会计部门使用的关键服务器。该服务器必须可以通过会计 VLAN 访问，但不能通过任何其他网络访问。要验证配置，您可以设置反向分级 Ping 测试，然后运行有线将 AutoTest 配置文件。测试报告 ping 失败，这是期望的结果。

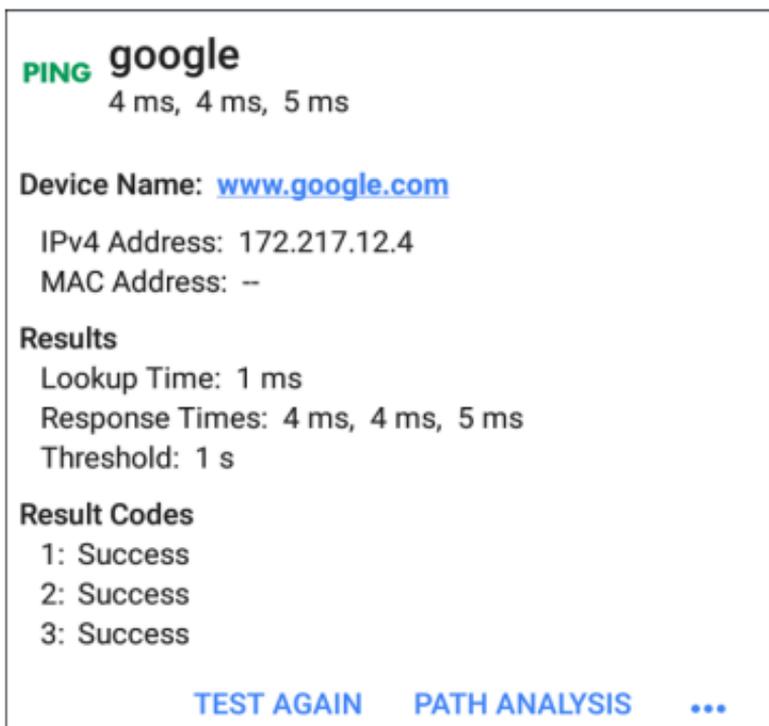
Ping 测试结果



Ping 卡显示在 Ping 测试设置中输入的 Ping 测试名称以及来自目标的三个 Ping 响应时间。

触摸卡片以打开 Ping 结果屏幕。

自动测试 Ping 结果屏幕



设备名称

目标设备的主机名或地址

- **IPv4 或 IPv6 地址:** 目标设备的 IP 地址
- **MAC 地址:** 目标设备的 MAC 地址。两个破折号 -- 表示没有从服务器提供 MAC 地址。

结果

- **查询时间:** 将 URL 解析为 IP 地址需要多长时间

- 响应时间: 花了多长时间LRAT在发送三个 Ping 中的每一个后接收来自目标的响应
- 阈值: 测试设置中指示的超时阈值

结果代码

使用测试结果屏幕底部的蓝色链接或蓝色操作溢出图标按钮执行其他操作。

- 点击**再次测试**以再次运行 Ping 测试。
- 点击**路径分析**以打开路径分析应用并查看 Ping 测试的信息。
- 点击蓝色操作溢出图标可以打开另一个测试应用程序(Ping、TCP 连接或捕获), 在您的网络浏览器中浏览到 Ping 目标地址, 或者启动 **Telnet 或 SSH** 会话。

The screenshot shows the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and a gear icon on the right. Below the header, the main content area displays the results of a ping test for "google". The test results show three successful pings with a response time of 3 ms each. Below the ping results, there are sections for "Device Name" (www.goog), "IPv4 Address" (172.217.), and "MAC Address" (–). The "Results" section shows a "Lookup Time" of 14 ms, "Response Times" of 3 ms, and a "Threshold" of 1 s. The "Result Codes" section shows three successful results (1: Success, 2: Success, 3: Success). A semi-transparent menu overlay is positioned on the right side of the screen, listing several options: "Ping", "TCP Connect", "Capture", "Browse", "Telnet", and "SSH". At the bottom of the screen, there are three buttons: "TEST AGAIN", "PATH ANALYSIS", and a three-dot menu icon.

PING google
3 ms, 3 ms, 3 ms

Device Name: [www.goog](http://www.google.com)
IPv4 Address: 172.217.
MAC Address: –

Results
Lookup Time: 14 ms
Response Times: 3 ms,
Threshold: 1 s

Result Codes
1: Success
2: Success
3: Success

TEST AGAIN PATH ANALYSIS ...

Ping
TCP Connect
Capture
Browse
Telnet
SSH

自动测试 TCP 连接测试

TCP 连接测试打开与选定目标的 TCP 连接，以使用 3 次握手 (SYN、SYN/ACK、ACK) 测试端口可用性。AutoTest Target TCP Connect 测试运行三个连接测试并报告响应时间。

TCP 连接测试设置

TCP Connect Test	
Name	google
Device Name	www.google.com
IP Protocol Version	IPv4
Port	80 (www-http)
Timeout Threshold	1 s
Reverse Grading	<input type="checkbox"/> Disabled

名称

此字段允许您为测试分配自定义名称。该名称出现在配置文件中的目标测试卡上。

设备名称

输入要测试的目标的 IP 地址或 URL。如果您输入 IP 地址，则会跳过测试的 DNS 查找部分。

IP协议版本

默认使用 IPv4。触摸该字段可在 IPv4 和 IPv6 之间切换。

端口

指定 TCP 端口号 LRAT 用于连接到目标。

超时阈值

这个阈值控制多长时间 LRAT 在测试失败之前等待目标的响应。

反向评价

启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

TCP 连接测试结果

TCP NetAlly >
 80 ms, 76 ms, 82 ms

TCP 卡显示在设置中输入的测试名称和来自目标的三个响应时间。

触摸卡片以打开 TCP 结果页面。

自动测试 TCP 结果页面

☰
AutoTest
⚙️

TCP NetAlly
 50 ms, 44 ms, 42 ms

Device Name: ip-184-168-221-49.ip.secureserver.net
 IPv4 Address: 184.168.221.49
 MAC Address: –
 Port: 80 (www-http)

Results
 Lookup Time: 21 ms
 Response Times: 50 ms, 44 ms, 42 ms
 Threshold: 250 ms

Result Codes
 1: Success
 2: Success
 3: Success

TEST AGAIN
PATH ANALYSIS
...

设备名称: 测试设备的 DNS 名称

IPv4 或 IPv6 地址: 目标设备的 IP 地址

MAC 地址: 设备的 MAC 地址。两个破折号 -- 表示没有提供 MAC 地址。

端口: 要测试的端口号

Results

查找时间: 将 URL 解析为 IP 地址需要多长时间

响应时间: 花了多长时间 LRAT 为三个连接测试中的每一个接收来自服务器的响应

阈值: 测试设置中指示的超时阈值

结果代码: 三个 Ping 中每一个的测试的最终状态(成功或失败)

结果代码

使用测试结果屏幕底部的蓝色链接或蓝色操作溢出图标按钮执行其他操作。

- 点击 [再次测试](#) 以再次运行 Ping 测试。
- 点击 [路径分析](#) 以打开路径分析应用并查看 Ping 测试的信息。

- 点击蓝色操作溢出图标可以打开另一个测试应用程序(Ping、TCP 连接或捕获), 在您的网络浏览器中浏览到 TCP目标地址, 或者启动 [Telnet](#) 或 [SSH](#) 会话。

HTTP 测试

注意: HTTP 测试仅在 LinkRunner AT 4000 上可用。

HTTP 测试执行全面的最终用户响应 下载指定网页时的时间 (EURT) 测量 页。目标可以是 IPv4 地址、IPv6 地址或 URL。

HTTP 测试设置

除了时间阈值之外, HTTP 设置还允许基于响应、返回代码和时间阈值。

HTTP Test	
Name	github
URL	https://www.github.com
IP Protocol Version	IPv4
Allow Redirects	<input checked="" type="checkbox"/> Enabled
Response Time Threshold	10 s
Web Page Transfer Size	ALL
Response Must Contain	

名称

此字段允许您为测试分配自定义名称。该名称出现在配置文件中的目标测试卡上。

URL

输入目标地址。要访问在非默认端口上运行的 Web 服务器,请输入冒号 (:) 并在 URL 后指定端口号。

IP协议版本

默认使用 IPv4。触摸该字段可在 IPv4 和 IPv6 之间切换。

允许重定向

尝试连接到目标时,触摸切换按钮以允许 Web 重定向。

响应时间阈值

这个阈值控制了多长时间LRAT在测试失败之前等待来自 URL 的响应。触摸该字段以更改值。

网页传输大小

此设置允许您限制下载的数据量,从 HTML 仅报头到整个页面(所有)。触摸该字段以选择不同的传输大小。

Response Must Contain	
Response Must Not Contain	
Return Code	
200 - OK	
Reverse Grading	<input type="checkbox"/>
Disabled	
HTTP Proxy	<input type="checkbox"/>
Disabled	

响应必须包含

此处输入的文本用作**通过/失败**测试标准基于文本字符串在指定服务器或 URL 上的存在。要构建文本字符串，请输入一个或多个具有精确间距的单词。指定多个单词时，它们必须在源处连续出现。如果找到文本字符串，则测试通过。如果未找到该字符串，则测试失败并返回代码：“响应不包含必需的文本”。

响应不得包含

与上面的设置类似，除了此处输入的文本功能为**通过/失败**测试标准基于缺少指定服务器或 URL 上的文本字符串。如果未找到文本字符串，则测试通过。如果找到该字符串，则测试失败并返回代码：“响应包含排除的文本”。

返回代码

此处设置的返回代码用作**通过/失败**测试标准。默认值为“OK (HTTP 200)”。触摸该字段以从列表中选择不同的返回代码。如果您选择的返回代码值与实际返回代码值匹配，则测试通过，如果LRAT收到不同的返回码，测试失败。

反向评价

启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

HTTP 代理

目标测试设置中的代理控制使用主配置文件设置中指定的服务器地址和端口。触摸切换开关以使用这些代理设置。

目标测试设置中的代理控制使用主配置文件设置中指定的服务器地址和端口。触摸切换开关以使用这些代理设置。

HTTP 测试结果



HTTP 卡显示在测试设置中输入的测试名称和来自目标的响应时间。

HTTP测试结果页面

HTTP github	
3.671 s	
Device Name: lb-192-30-253-113-iad.github.com	
IPv4 Address: 192.30.253.113	
MAC Address: --	
URL: https://www.github.com	
Results	
Metric	Result
Ping	54 ms
DNS Lookup	59 ms
TCP Connect	165 ms
Data Start	1.288 s
Data Transfer	2.157 s
Total Time	3.671 s
Threshold	10 s
Data Bytes	90.9 K
Rate (bps)	206.2 K
End User Response Time	

设备名称: 测试的服务器的 DNS 名称

IPv4 或 IPv6 地址: 服务器的 IP 地址

MAC 地址: 服务器的 MAC 地址。两个破折号 -- 表示没有从服务器提供 MAC 地址。

URL: 目标网址

结果

Ping: Ping 测试与 HTTP 测试同时运行, 此结果字段显示 Ping 响应时间。如果 HTTP 测试在 ICMP 回显回复数据包到达之前完成, 则 ping 测试结果会显示破折号 --。Ping 结果不影响测试的通过/失败状态。

DNS 查询: 将 URL 解析为 IP 地址所花费的时间。如果您输入 IP 地址, 则不需要 DNS 查找, 因此会显示破折号以指示未执行此部分测试。

TCP 连接: 在服务器上打开端口所花费的时间

Data 开始: 是时候从 Web 服务器接收 HTML 的第一帧了

Data 传输: 从目标服务器接收数据的时间

总时间: 最终用户响应时间 (EURT), 即下载网页所用的总时间。它是 DNS 查找、TCP 连接、数据开始和数据传输时间的总和。如果总时间超过设置中的响应时间阈值, 则测试失败。

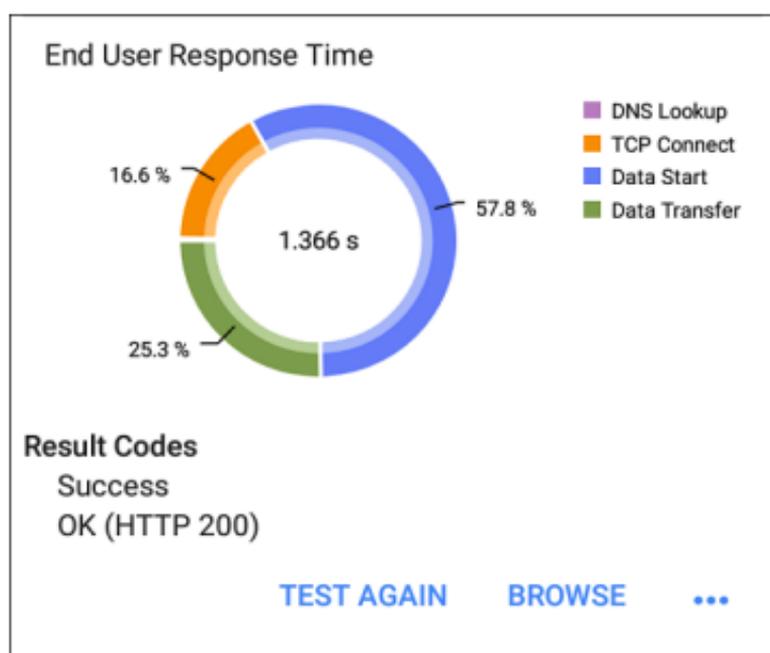
如果在测试的某个步骤中超过了响应时间阈值, 则测试的当前阶段 (DNS、查找、TCP

连接、数据启动或数据传输)用红点表示,其余测试将中止。

阈值:来自测试设置的响应时间阈值

数据字节:传输的数据字节总数。这不包括头字节

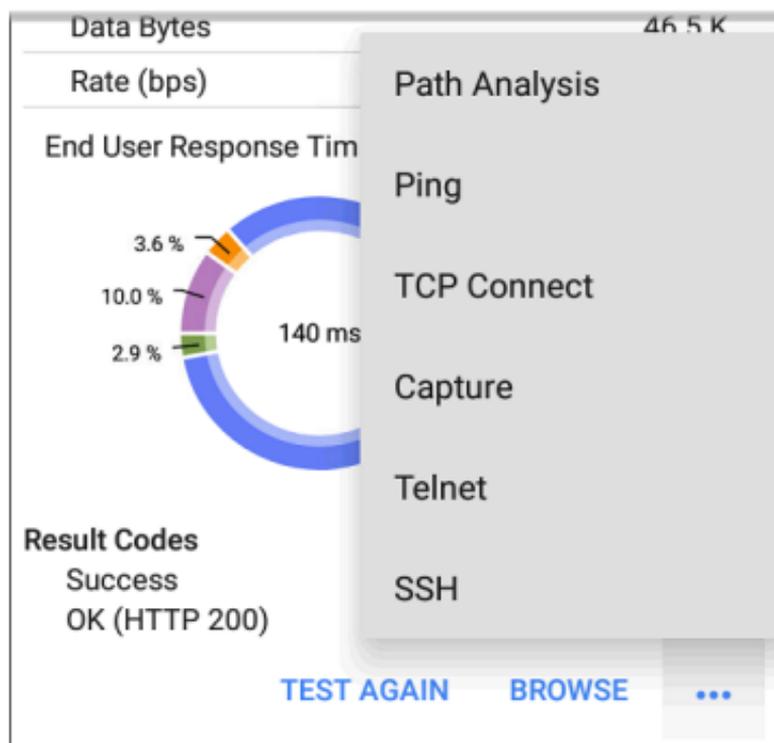
速率 (bps):测得的数据传输率



最终用户响应时间:测试每个阶段的时间饼图(DNS、查找、TCP 连接、数据启动和数据传输)

结果代码:测试的最终状态(成功或失败)

HTTP 测试还显示返回代码从网站服务器。



轻触[蓝色链接](#)或蓝色动作溢出图标 **...** 在测试结果屏幕底部运行 HTTP 重新测试, 打开另一个测试应用程序, 或浏览到您的网络浏览器中的目标地址。

FTP 测试

注意:FTP 测试仅适用于 LinkRunner AT 4000。

FTP 测试执行文件上传到 FTP 服务器或从 FTP 服务器下载,允许验证服务器和网络性能。目标可以是 IPv4 地址、IPv6 地址或 URL。结果提供了将整个文件传输时间完整分解为各个组成部分的细目。

FTP 测试设置

FTP 设置允许您指定一个 **Get or Put** 测试以及文件路径和名称。

FTP Test	
Name Asset Server	
FTP Server 10.250.2.218	
IP Protocol Version IPv4	
File internal/iperf3	
File Transfer Size ALL	
Direction Get	<input checked="" type="checkbox"/>
Response Time Threshold 10 s	

名称

此字段允许您为测试分配自定义名称。该名称出现在配置文件中的目标测试卡上。

FTP服务器

输入要测试的 FTP 服务器的 IPv4 地址或 URL。如果您输入 IP 地址，则会跳过测试的 DNS 查找部分。

IP协议版本

默认使用 IPv4。触摸该字段可在 IPv4 和 IPv6 之间切换。

文件

此设置指定下载的文件的文件和文件名 (**Get**)或上传到(**Put**)服务器，基于方向下面设置。触摸该字段以输入文件路径和名称。

文件传输大小

此设置可让您限制要下载或上传的数据量。默认传输大小为所有。

- 当方向设置是**Get**，传输大小为 ALL 会导致下载继续，直到下载整个文件或超过响应时间阈值。指定大于正在检索的文件的传输大小不会导致测试失败。文件下载完成后，测试停止。
- 当方向设置是**Put**，ALL 的默认传输大小导致LRAT创建并上传一个文件10 MB。

方向

触摸切换按钮可在 **Get** (下载文件从服务器) 或 **Put** (上传文件到服务器) 测试。

- 如果 **Direction** 设置为 **Get**, 则检索文件, 并计算大小和数据速率。下载后, 此数据将被丢弃, 并且不会保留在 **LRAT**。
- 如果 **Direction** 设置为 **Put**, 则在 **FTP** 服务器上创建上面命名的文件。该文件的大小由文件传输大小环境。该文件包含一个文本字符串, 表明它是从 **LRAT**, 并重复测试字符串以产生设置的文件大小。

响应时间阈值

这个阈值控制了多长时间 **LRAT** 在测试失败之前等待来自 **FTP** 服务器的响应。触摸该字段以更改值。

Username	
Password	
Reverse Grading Disabled	<input type="checkbox"/>
HTTP Proxy Disabled	<input type="checkbox"/>

用户名和密码

输入这些凭据以访问您指定的目标服务器。输入“anonymous”作为用户名以建立匿名连接。如果配置的用户名或密码在目标 FTP 服务器上无效，则测试失败。

反向评价

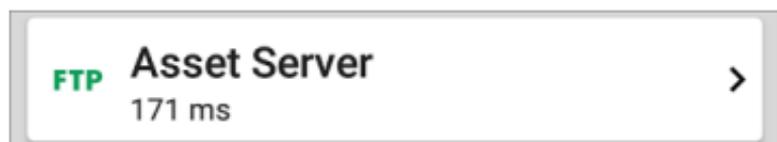
启用反向评分后，如果测试失败则视为成功，如果测试成功则视为失败。结果屏幕的结果代码部分包含“评分已反转”消息。

HTTP 代理

目标测试设置中的代理控制使用主配置文件设置中指定的服务器地址和端口。见[有线](#)

配置文件设置。

FTP 测试结果



FTP 卡显示在测试设置中输入的测试名称和目标的响应时间。

FTP 测试结果页面

FTP Asset Server	
171 ms	
Device Name: 10.250.2.218	
IPv4 Address: 10.250.2.218	
MAC Address: --	
Get File: /internal/ipperf3	
Results	
Metric	Result
Ping	50 ms
DNS Lookup	--
TCP Connect	44 ms
Data Start	116 ms
Data Transfer	10 ms
Total Time	171 ms
Threshold	60 s
Data Bytes	24 K
Rate (bps)	1.2 M

设备名称: 测试服务器的主机名

IPv4 或 IPv6 地址: 服务器的IP地址

MAC地址: 服务器的 MAC 地址。两个破折号 -- 表示没有从服务器提供 MAC 地址。

获取文件:在设置中输入的文件路径和名称,与 FTP 服务器之间传输。

结果

Ping: Ping 测试与 FTP 测试同时运行,此结果字段显示 Ping 响应时间。如果 FTP 测试在 ICMP 回显回复数据包到达之前完成,则 ping 测试结果将显示破折号 --。Ping 结果不影响测试的通过/失败状态。

DNS 查询:将 URL 解析为 IP 地址所花费的时间。如果您输入 IP 地址,则不需要 DNS 查找,因此会显示破折号以指示未执行此部分测试。

TCP 连接:在服务器上打开端口所花费的时间

数据开始:从 FTP 服务器接收第一帧的时间

数据传输:从目标服务器接收文件的时间

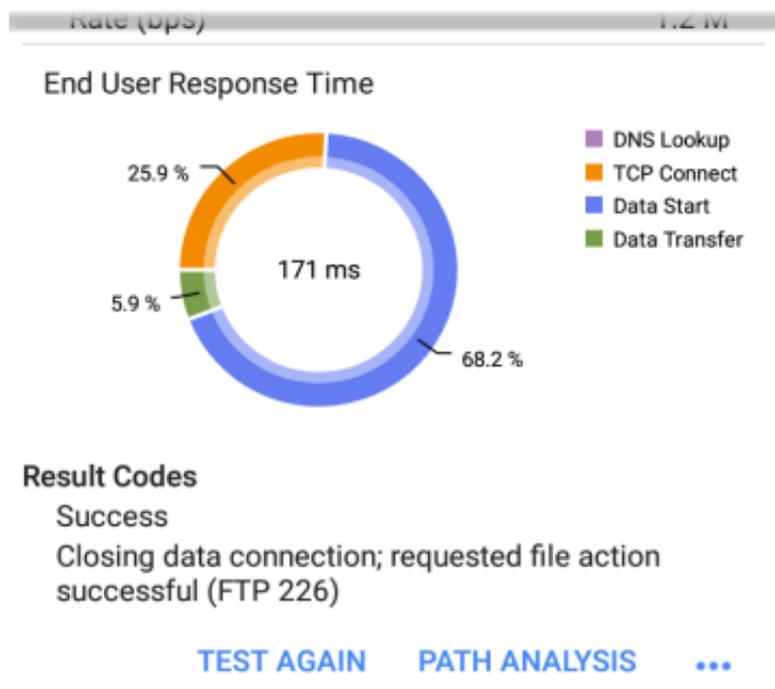
总时间:最终用户响应时间 (EURT),即下载网页所用的总时间。它是 DNS 查找、TCP 连接、数据开始和数据传输时间的总和。如果总时间超过设置中的响应时间阈值,则测试失败。

如果在测试的某个步骤中超过了响应时间阈值，则测试的当前阶段(DNS、查找、TCP 连接、数据启动或数据传输)用红点表示，其余测试将中止。

阈值:来自测试设置的响应时间阈值

数据字节:传输的数据字节总数。这不包括头字节。

速率 (bps):测得的数据传输率



最终用户响应时间:测试每个阶段的时间饼图(DNS、查找、TCP 连接、数据启动和数据传输)

结果代码:测试的最终状态(成功或失败)

FTP 测试还显示返回代码从服务器。

轻触 [蓝色链接](#) 或蓝色动作溢出图标  在测试结果屏幕底部运行 FTP 再次测试, 打开另一个测试应用程序, 或浏览到 Web 浏览器中的 FTP 服务器。

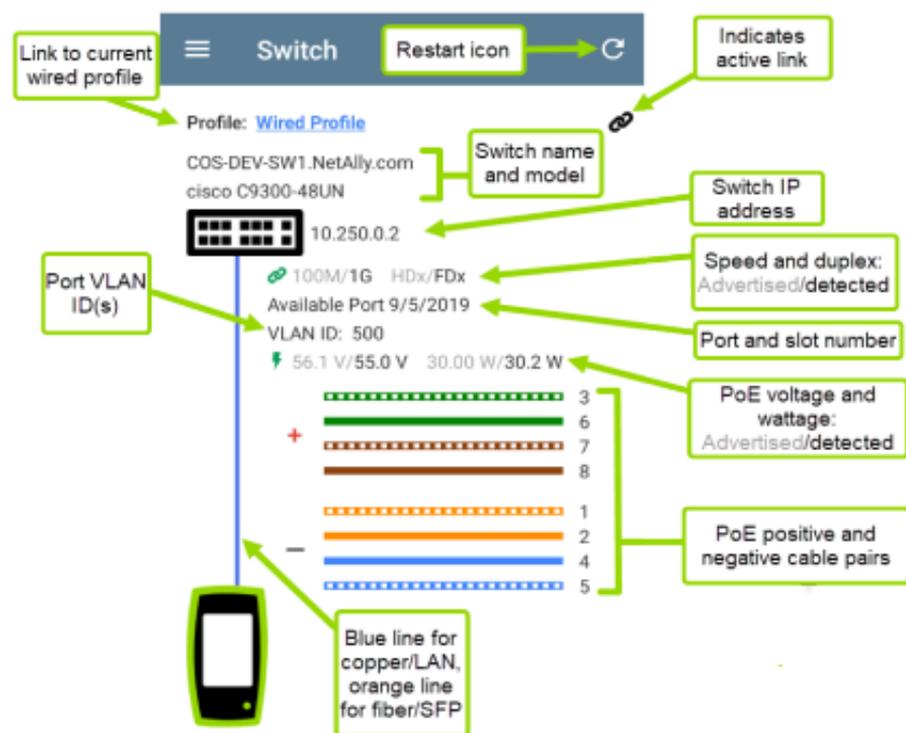


交换机应用

交换机应用从链路、PoE和最近交换机结果屏幕中显示自动测试有线配置文件结果的摘要。这为您提供了一种快速显示有关您的 LinkRunner AT 3000/4000 连接方式的信息的方式。

运行交换机

在运行交换机之前，使用自动测试启动一个有线配置文件，以便在需要时Switch能够获取信息。要运行Switch，只需点击Switch应用程序图标即可。这将打开主要的Switch屏幕。



交换机主屏幕只有少量控件，没有设置选项。

- 点击重启图标  以更新交换机信息。该应用程序将显示最近交换机的结果，这些结果是根据最近运行或当前正在运行的有线AutoTest配置文件而生成的。
 - 当测试仪处于活动链接状态时，屏幕右上角会显示一个黑色的链路图标 。
 - 如果没有可用的连接，将显示一个"无线缆"图标：



注意：即使在断开连接后，显示的结果仍然保留。只需点击重启图标  以捕获并显示来自交换机的最新信息。

- 要打开自动测试配置文件，请点击配置文件链接：

Profile: [Wired Profile](#)

要获取详细信息, 请点击显示链路图标 、PoE图标  或交换机图标  的自动测试卡片。



缆线测试应用

LRAT 3000-4000的电缆测试可以帮助您确定电缆长度和故障状态,验证接线和结构化布线的布线图,并使用音频定位电缆连接。线缆测试端口为主机左侧的RJ-45 端口LRAT设备。将电缆连接到此端口以使用音频功能进行测试和跟踪。

电缆测试设置

电缆测试应用程序的设置有限。点击导航菜单图标  或滑动左侧滑动栏以打开电缆测试设置。

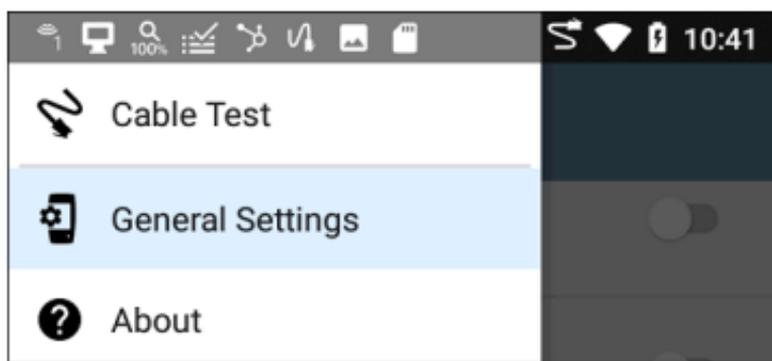
闪烁端口

点击此设置选项可激活 Flash Port 功能，该功能会闪烁端口 LED 以帮助您找到电缆和端口。请参阅[运行电缆测试](#) 获取有关使用该功能的说明。

距离单位

距离单位 设置包含在 [常规设置](#) 菜单中。该设置指定英尺或米。

1. 要访问常规设置，请触摸菜单  Cable Test 应用程序屏幕上的图标，然后选择常规设置。



2. 滚动到“设置”列表底部首选项标题。
3. 点击距离单位字段，然后选择英尺或者米根据需要，然后触摸确认。
4. 点击“返回”按钮 以返回电缆测试页面，该按钮在页面底部。

运行电缆测试

电缆测试应用程序具有针对电缆的常规测试以及 [音频功能](#) 和 [闪烁端口功能](#)。可帮助您跟踪电缆和端口。您还可以将结果上传至 [Link-Live](#)。

通用电缆测试

参考 LRAT 3000-4000's [按键和端口相关信息](#)。

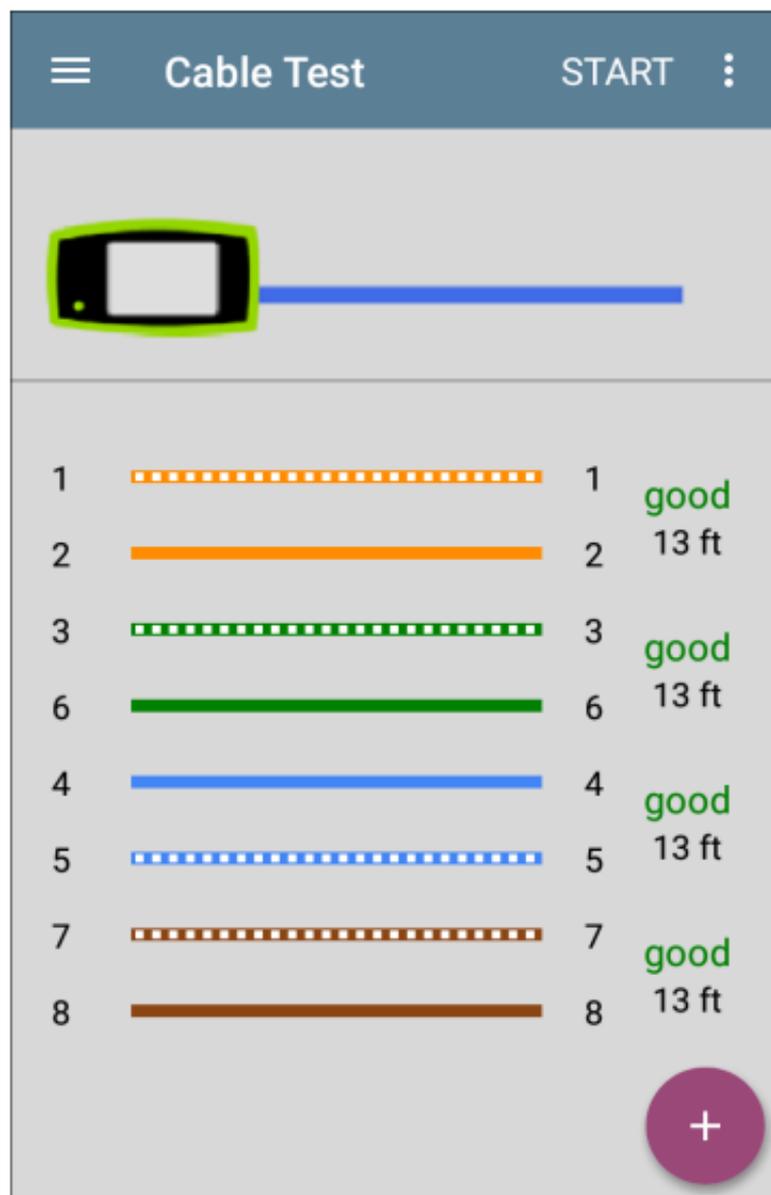
- 与 [开放或未终止](#) 将电缆连接到 RJ-45 电缆测试端口(设备顶部), 您可以测量长度、识别短路和分裂并定位开路。
- 使用终止于 [WireView 电缆 ID 附件](#), 您可以测量电缆长度并识别短路、开路、分离线对、交叉电缆、正常或负极对极性以及屏蔽电缆。
- LRAT 3000-4000 无法对连接到交换机的电缆进行电缆测试; 但是, 您仍然可以使用 [音调功能](#) 跟踪电缆到连接的端口。
- 此外, 如果设备检测到连接的电缆上有电压, 您将无法运行电缆测试或使用音频功能。电缆测试屏幕上的闪电图标表示检测到的电压。



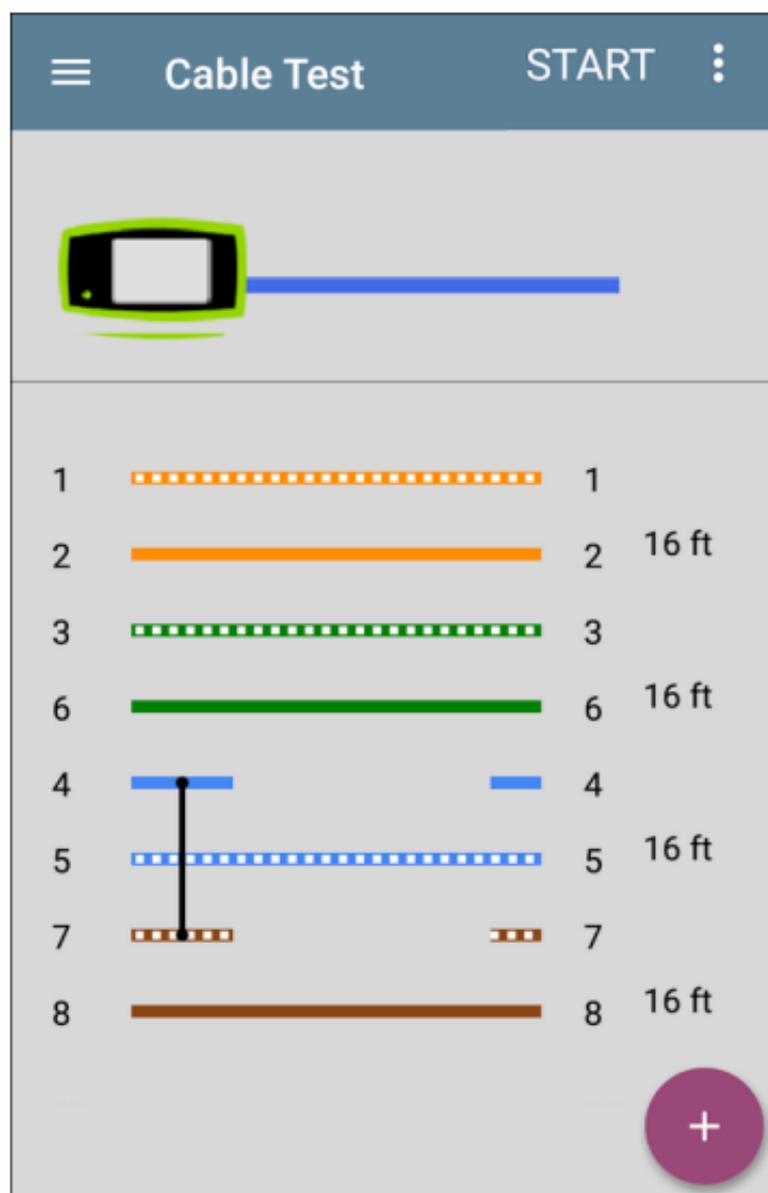
要开始电缆测试, 请点击开始在 Cable Test 应用程序屏幕的右上角。

打开电缆 TDR 测试

通过使用时域反射计 (TDR) 测量电缆的电反射, 可以测量电缆的长度并检测一些故障。将开放式电缆(未端接)连接到位于顶部的 RJ-45 端口单位来测量其长度并查看任何短路、开口或分裂。



当电缆未检测到故障时，长度测量值上方的每对电缆旁边会显示“良好”。检测电缆中“分裂”或“开路”的电缆测试也会显示相应的词。



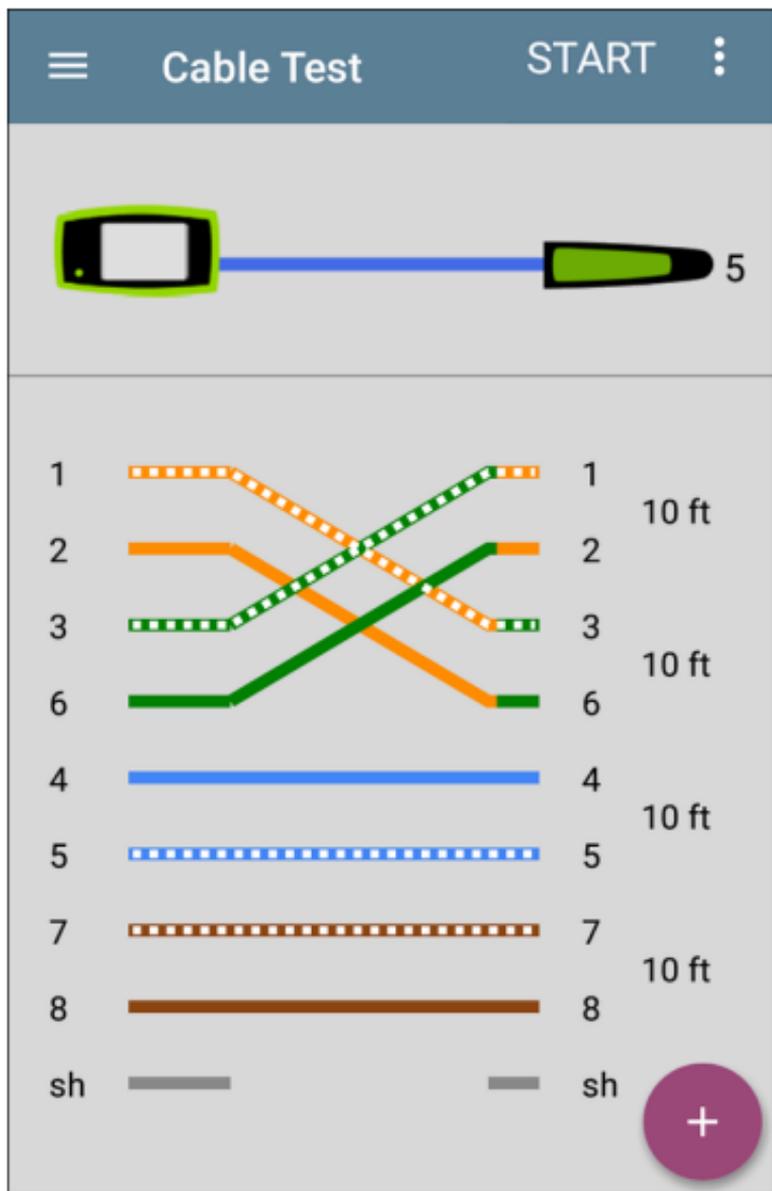
此末端接电缆测试图像显示了针脚 4、5 和 7 之间的短路电缆。

终止的 **WireView** 测试

使用 **WireView** 附件可提供更详细的每线结果。**WireView #1** 包含在您的 **LRAT 3000-4000** 额外的 **WireViews 2-6** 可供购买。

要运行端接电缆测试, 请将顶部 **RJ-45** 端口连接到以外部 **WireView Cable ID** 附件端接的电缆。

端接电缆测试屏幕显示连接的 **WireView** 的编号, 除非电缆故障阻止 **LRAT** 从检测 **WireView**。



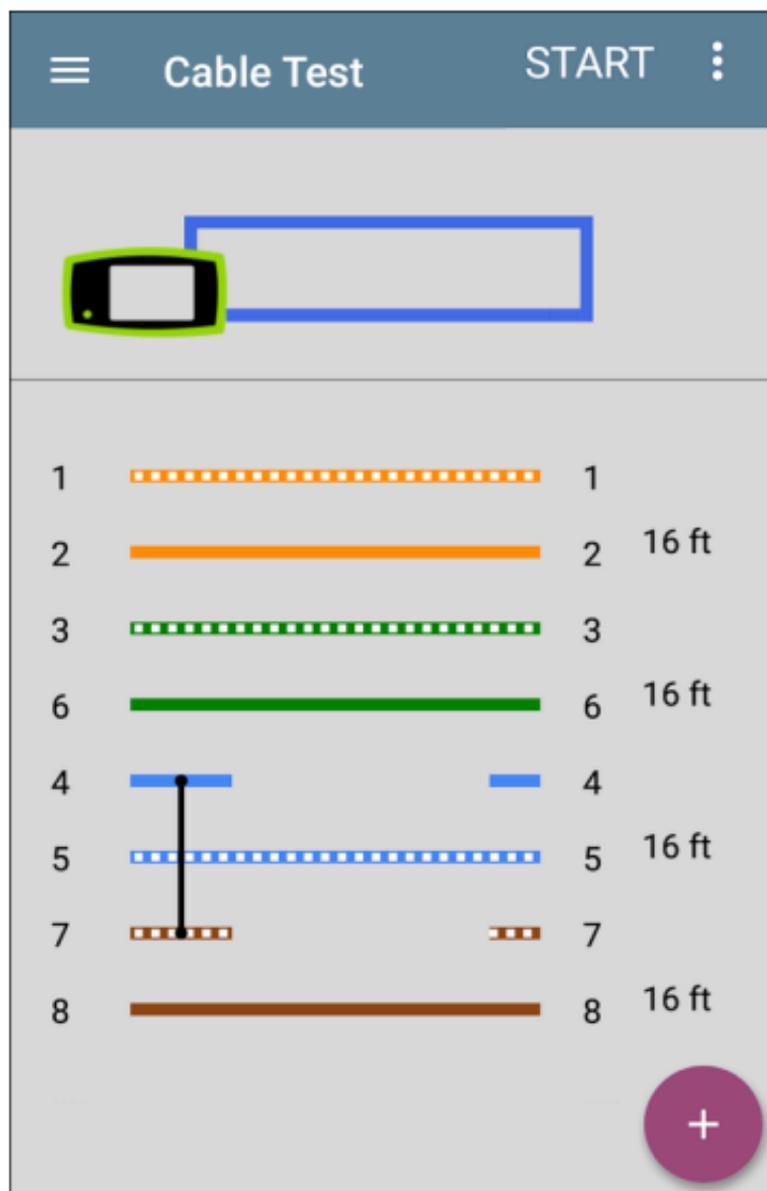
上图表示 1、2 和 3、6 对与 WireView 附件编号 5 之间的交叉。

WireView 结果的最后一行表示电缆是否被屏蔽：**sh** 表示检测到屏蔽电缆。



跳线测试

将电缆从顶部 RJ-45 LAN 测试端口连接到侧面 RJ-45 WMAP 线路图端口，以计算电缆长度和线路图，包括任何故障。下图显示了电缆长度和针脚 4 和 7 之间的短路电缆。

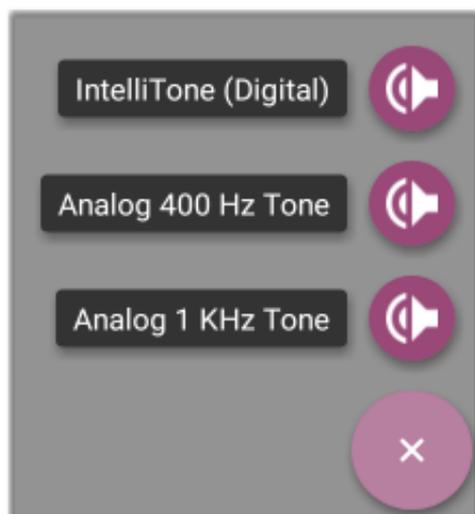


音调功能

您还可以使用 Fluke Networks* IntelliTone™ 探头或任何模拟探头和音频功能跟踪电缆。

* IntelliTone 是 Fluke Networks 的商标。

1. 将电缆连接到左侧的 RJ-45 端口。
2. 轻触 **FAB**  显示音调菜单：



3. 为您的探头选择合适的音调选项。这通过电缆发出音调，探头检测到它，让您可以追踪电线或在开关柜中找到它。

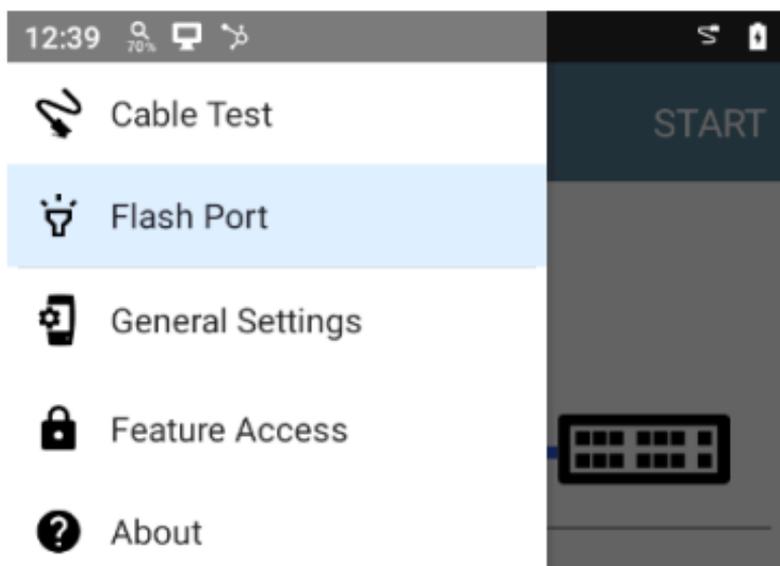
Flash 端口功能

Flash Port 可让您使设备的 RJ-45 测试端口和设备所连接的交换机上的 LED 闪烁。这有助于在交换机上更轻松地找到连接的端口。

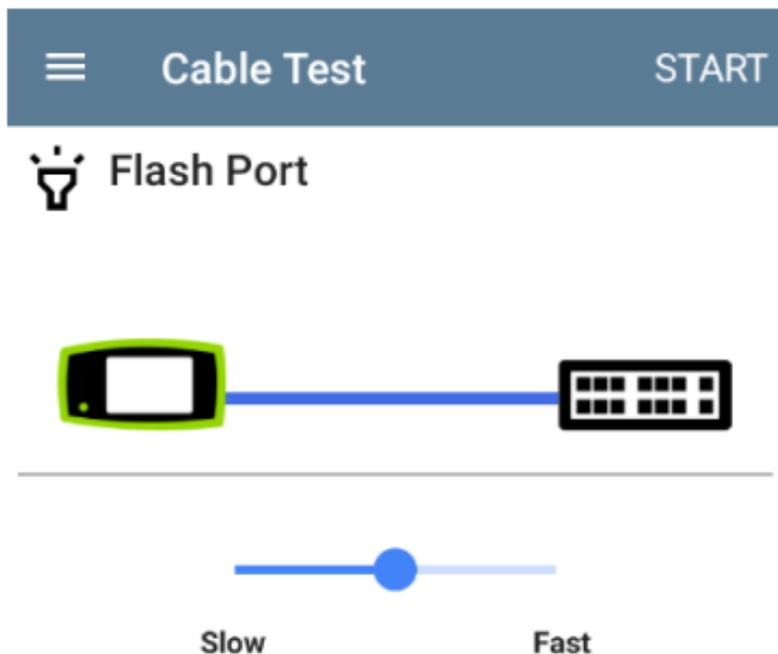
要使用闪烁端口功能：

* IntelliTone is a trademark of Fluke Networks.

1. 将顶部 RJ-45端口连接到有源网线。
2. 点击导航菜单图标  或从左侧抽屉滑动以打开电缆测试设置。



3. 点击 **Flash Port** 打开 Flash Port 屏幕。如果与交换机的连接良好，则会出现一条蓝线将测试单元图标连接到交换机图标。



4. 使用滑块设置闪光速率。

提示：某些端口 LED 可能无法以非常快的频率闪烁。将频率设置为低于最大值可能会更好。

5. 点击“**开始**”按钮。当闪光功能开始时，交换机图标上方会出现一个绿色圆圈，并以您使用滑块设置的速率闪烁。绿色圆圈、测试设备顶部 RJ-45 端口上的 LED 以及交换机上连接端口的 LED 都会同时闪烁。

Flash Port



6. 当您使用完 Flash Port 功能后，点击停止按钮。

将电缆测试结果上传到 **Link-Live**

触摸操作溢出图标  在电缆测试屏幕的右上角，然后选择上传到 **Link-Live** 将当前电缆测试结果发送到结果页面  在 Link-Live.com。

请参考 [Link-Live 章节](#) 了解更多的信息。



Ping/TCP 测试应用程序

Ping/TCP 测试应用程序对您选择的目标运行 Ping 或 TCP Connect 测试，允许您监控连接变化。

Ping 测试向所选目标发送 ICMP 回显请求，以确定是否可以访问服务器或客户端以及响应所需的时间。TCP 连接测试打开与选定目标的 TCP 连接，以使用 3 次握手 (SYN、SYN/ACK、ACK) 测试端口可用性。

您可以从主屏幕打开 TCP/Ping 应用程序，或者您可以选择 Ping 或者 TCP 连接从另一个应用程序 (例如 AutoTest 或 Discovery) 查看设备的详细信息。

Ping/TCP 设置

要配置测试，您可以在设置中手动输入主机名或 IP 地址，或者您可以从另一个测试应用程序的设备屏幕中选择 Ping 或 TCP Connect。

从另一个应用程序填充 Ping/TCP

当您从另一个应用程序打开 Ping/TCP 应用程序时，地址会预先填充为 Ping 或 TCP 目标设备。例如，**FAB** 菜单上**发现**下面显示的应用程序屏幕包含打开 Ping/TCP 应用程序的选项。

The screenshot shows a network discovery application interface. At the top, a cloud icon is next to the device name 'cos-lab-vm-cisco'. Below it, the device is identified as a 'Router'. The 'Name' field shows 'SNMP: cos-lab-vm-cisco'. The 'Address' section is highlighted with a green oval and contains 'IPv4: 10.250.0.11 (Reachable)' and 'MAC: Cisco:40f4ec-f47681'. Below this, it says 'Protocols: Statically Configured Router' and 'Attributes: Discovered via SNMP Switch, Port Aggregation'. A 'Path Analysis' button is visible. The 'Addresses' section has a green arrow pointing to a 'Ping/TCP' button. Other sections include 'VLANs' (1, 196, 500, 508, 526, 560) with a 'Capture (Wired)' button, 'Interfaces' (Up: 2, Down: 41) with a 'Browse' button, and 'MIB' and 'SNMP' sections. On the right side, there are several circular icons: a purple one with a cross, a pink one with 'PING/TCP', a purple one with a signal icon, a pink one with a square and up arrow, and a purple one with an 'X'.

如果从此屏幕打开 Ping/TCP 应用程序，则来自 Discovery 应用程序的 IPv4 地址已配置为 Ping/TCP 目标。

The screenshot shows the interface of the Ping/TCP application. At the top, there is a blue header bar with a hamburger menu icon, the text 'Ping', the text 'START', and a gear icon. Below the header, the text 'PING/TCP' is on the left, and the IP address '10.250.0.11' is in the center, both highlighted with a green oval.

手动配置 Ping/TCP 设置

要手动配置目标和设置, 请打开应用程序的设置 .

Ping/TCP Settings	
Device Name	www.google.com
IP Protocol Version	IPv4
Interface	Any Port
Number Of Tests	Continuous
Protocol	Ping
Frame Size (bytes)	64
Interval	1 s

设备名称: 输入目标的 IP 地址或 DNS 名称。

IP协议版本:默认使用 IPv4。触摸该字段以启用 IPv6。

端口:此设置决定了LRAT运行测试的端口。触摸该字段以选择端口。(请参阅[测试和管理端口](#)获取对不同端口的解释。)

测试次数:轻触以选择要运行的 Ping 或 TCP 连接测试的数量。默认设置为连续的继续运行测试,直到您轻触停止按钮。

协议:点击以选择**Ping** 或者**TCP** 连接测试的协议。

以下某些设置取决于所选协议。

帧大小(字节):此设置仅在 **Ping**选择了协议。它指定了有效负载和标头的总大小 LRAT发送。点击单选按钮选择新大小,或输入 64 到 1518 字节的自定义值。

要沿到目标的路由测试最大传输单元 (MTU), 请选择要测试的 MTU 帧大小, 然后设置不要碎片化设置(下)到启用。

间隔:此设置仅在**Ping** 选择了协议。它控制从发送的每个 Ping 之间经过的时间LRAT. 默认情况下, Ping 每秒(1秒)发送一次。点击单选按钮选择不同的时间间隔, 或输入 100 到 10,000 毫秒之间的自定义值。

端口:此设置仅在**TCP**连接选择了协议。它表示您的端口号LRAT用于连接到目标地址以进行TCP端口开放测试。如果需要,请轻触端口字段以打开弹出式数字键盘并输入新的端口号。轻触确定保存它。

超时阈值:这个阈值控制多长时间LRAT在测试失败之前等待目标的响应。

不要碎片化:此设置仅在**Ping**选择了协议。触摸切换按钮以启用。请参阅上面的帧大小设置说明。

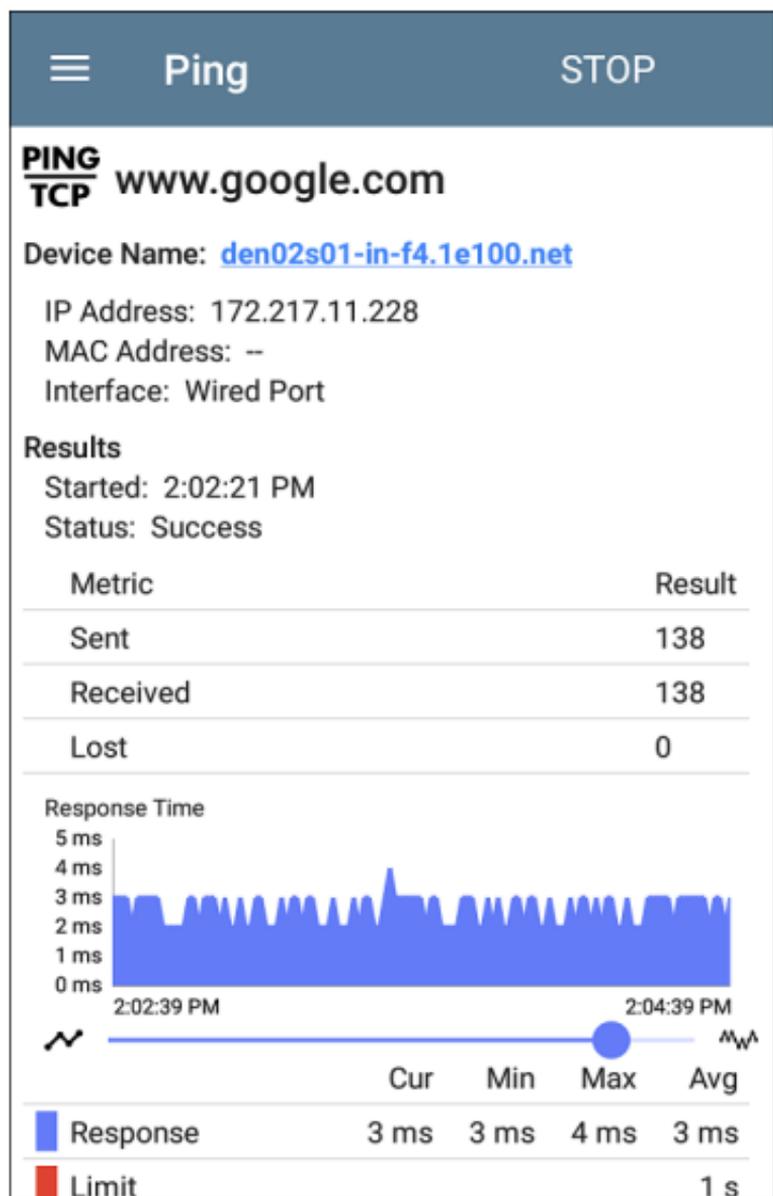
运行 Ping/TCP 测试

您的设备必须连接到运行的网络(测试或管理端口)运行 Ping 和 TCP Connect 测试。顶部状态栏中的图标指示您是否以及如何 LRAT 已连接。参考[连接通知](#)有关连接状态图标的说明, 并选择适当的 **Interface** (或任何端口) 来自 [Ping/TCP 设置](#)。

默认目标是 `google.com`。打开应用设置  进入一个新的目标。

要开始测试, 请触摸开始。

如果测试次数设置设置为 **Continuous**, Ping/TCP 应用程序对您选择的目标运行测试, 直到您触摸停止。



设备名称: 目标设备的主机名或地址

IPv4 或 IPv6 地址: 目标设备的IP地址

MAC地址: 目标设备的 MAC 地址。两个破折号 -- 表示设备未提供 MAC 地址。

端口:用于 TCP 连接测试的端口号。此字段不会出现在 Ping 测试结果中。

端口:这个LRAT运行测试的测试或管理端口结果

- 已开始:测试开始的时间
- 状态:最近的测试状态
- 发送:发送到目标的 Ping 或 TCP SYN 数据包数
- 接收:从目标返回的 Ping 或 TCP SYN/ACK 数据包的数量
- 丢包:未从目标返回的 Ping 或 TCP 数据包数

响应时间图:以毫秒为单位绘制目标设备的响应时间。如果设备保持链接,该图表最多可保存和显示过去 24 小时的数据。

要平移和缩放图形,您可以轻扫、双击和移动滑块。参考[趋势图](#)图形控件概述的主题。

相应:电流、最小值、最大值和平均响应时间测量的表格显示

限制这个超时阈值从 Ping/TCP 应用程序的设置



抓包应用

数据包捕获是记录网络流量的过程。数据包的形式作为数据流来回。数据包捕获可以帮助您分析网络问题、调试客户端/服务器通信、跟踪应用程序和内容、确保用户遵守管理策略并验证网络安全。

在LRAT, 捕包过程使用 [有线测试端口](#)。

您可以从主屏幕或使用来自其他应用程序的链接打开 **Capture** 应用程序, 例如 [自动测试](#) 或者 [发现](#)。

注意: 此应用程序仅适用于 **LinkRunner AT 4000**。

抓包设置

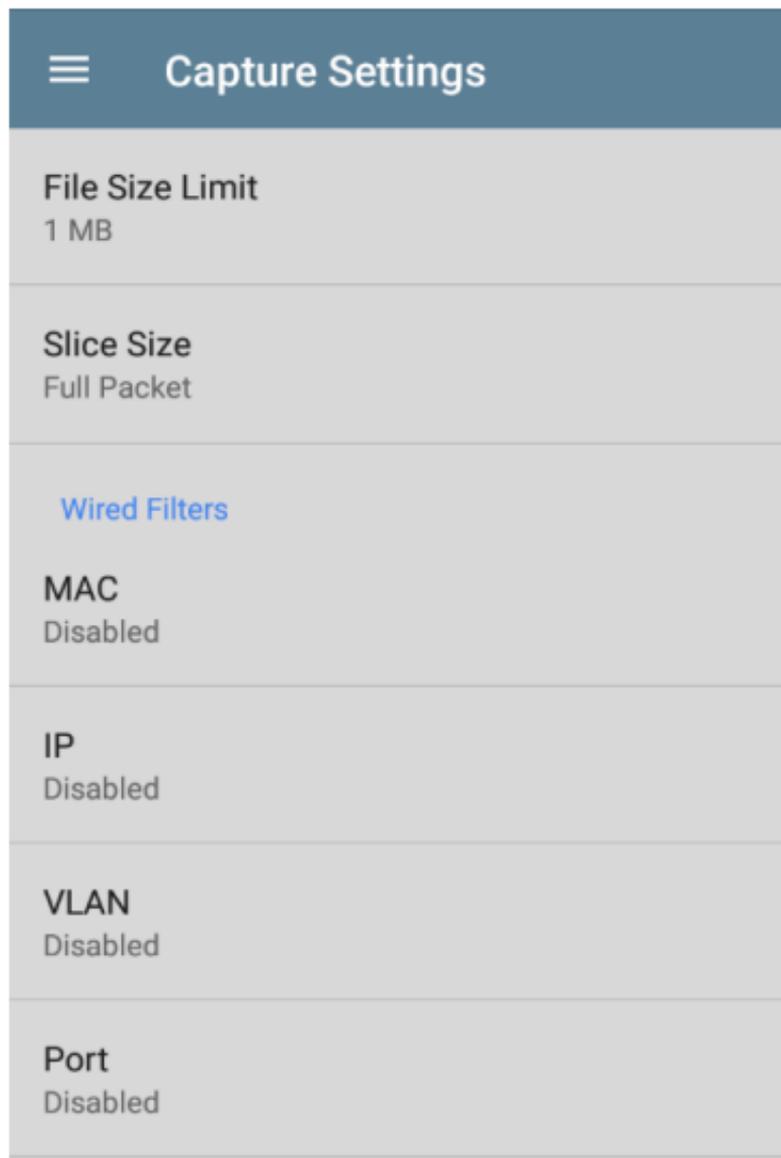
Capture 应用程序设置允许您指定文件和切片大小,并应用过滤器以仅捕获和分析某些数据包类型。例如,您可以设置过滤器以仅捕获与特定应用程序相关的数据包(基于 IP 地址和端口号)。

当您打开 Capture from Home 并且不配置任何过滤器时,来自交换机的所有数据包都会被捕获。默认抓包保存所有从本地交换机发送到交换机的数据包 LRAT。

如果您从另一个打开 Capture 应用程序 NetAlly 测试应用程序,自动应用捕获过滤器。可以从其他应用程序应用的过滤器包括有线 IP 和 MAC。

捕获设置会一直保存,直到您清除过滤器或打开应用了新过滤器的应用程序。

触摸设置图标  在捕获屏幕中配置捕获设置。



文件大小限制: 触摸此字段以指定捕获文件的大小。默认大小为 **1 MB**, 允许的最大大小为 **1 GB (1,024 MB)**。当捕获的文件达到此大小时, 捕获停止。当捕获运行时, 捕获屏幕会在捕获数据时显示当前文件大小。

切片大小:触摸此字段可选择特定的帧切片大小或输入自定义值。**Slice Size** 设置限制了每个数据包的捕获量。当您对数据包的标头感兴趣但不需要查看所有有效负载数据时,较小的切片大小很有用。默认为完1,518 bytes。

有线过滤器

默认情况下，所有过滤器都处于禁用状态，除非您从其他应用程序打开 **Capture**。触摸下面的字段以启用和输入过滤器值。

MAC:输入主机的 MAC 地址，仅捕获包含主机 MAC 地址作为源或目标的数据包。

IP:输入主机的 IP 地址以仅捕获进出主机的流量。您可以指定 IPv4 或 IPv6 地址。

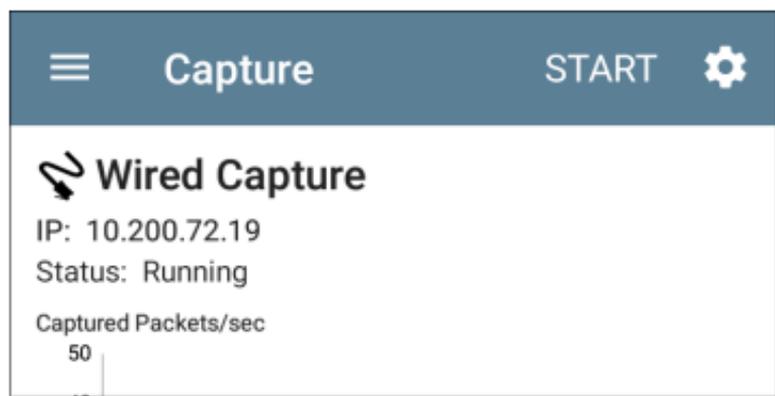
VLAN:输入 VLAN 编号以仅捕获为该 VLAN 标记的流量。

端口:指定端口号以仅捕获来自该 UDP 或 TCP 端口的流量。例如，选择端口 80 以仅捕获 HTTP 流量。

NOT:触摸切换开关以启用此设置，它会指示 **LRAT** 不要捕获您在上述过滤器中输入的值。例如，如果您设置了一个过滤器来捕获端口 80 上进出 IP 10.250.0.70 的流量，并且您启用了 **NOT**，则所有流量都会被捕获除了在端口 80 上进出 10.250.0.70 的流量。

运行和查看抓包

要开始捕捉，请轻点开始在应用程序屏幕的顶部。



捕获的当前状态和任何应用的过滤器显示在捕获类型下。上图表明该应用程序仅捕获 IP 10.200.72.19 的流量。

在捕获运行时查看捕获的实时状态。

有线图绘制了捕获运行时捕获的数据包的类型和数量，包括单播、广播和多播数据包类型。



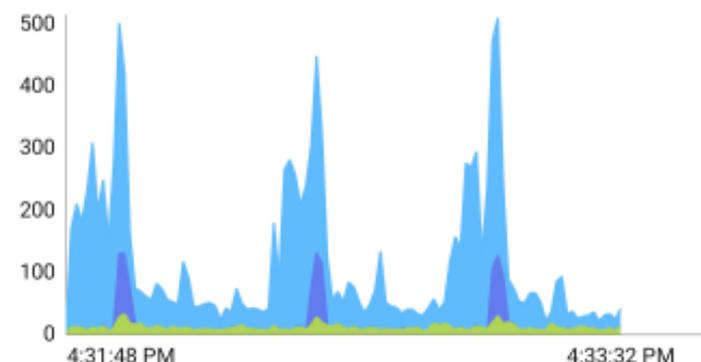
Capture

STOP

Wired Capture

Status: Running

Captured Packets/sec



Packet Type

Captured

Unicast	10.3 K
Broadcast	816
Multicast	1.2 K
All	12.3 K

Capture Size

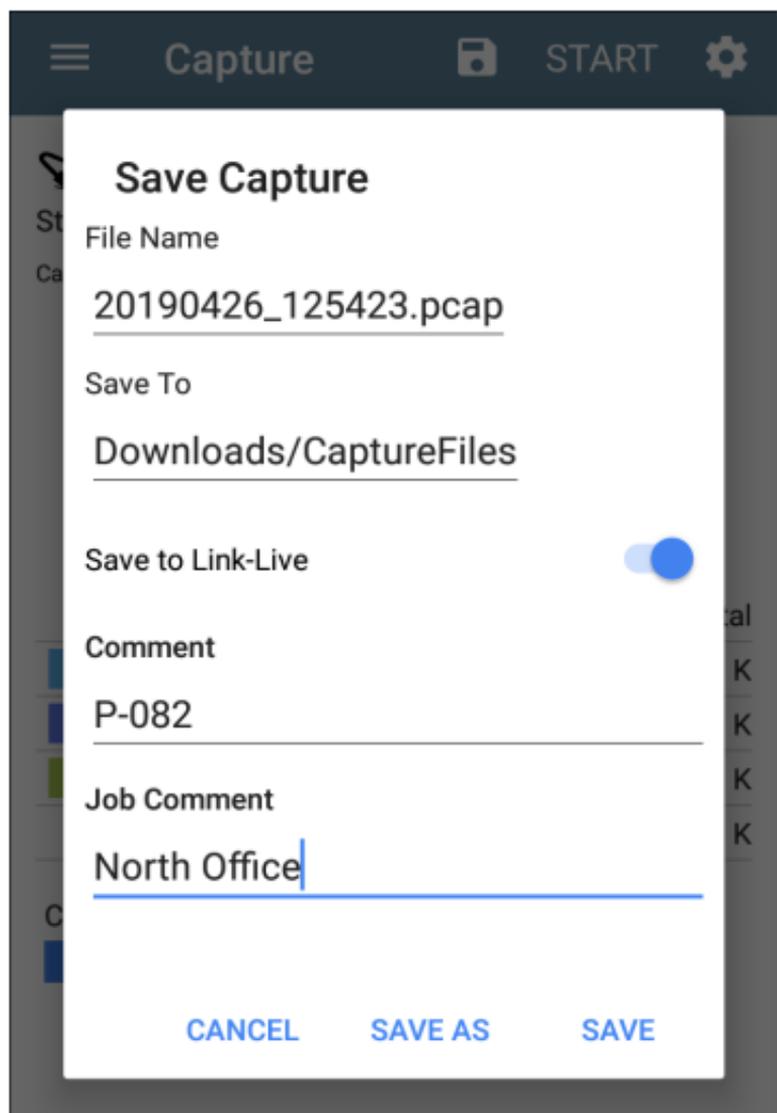
3.7 MB of 10 MB

- 如果您离开 Capture 应用程序，捕获过程将继续在后台运行，直到达到文件大小限制(请参阅 [捕获设置](#))。

- 要平移和缩放图表,您可以滑动、双击和移动滑块。请参阅 [趋势图](#) 来获取有关图形控件的信息。
- 点击 **STOP** 在达到文件大小限制之前停止正在运行的捕获。

捕获完成后,保存抓包对话框自动出现。

点击保存图标  重新打开此对话框。



捕获保存为 .pcap 文件。触摸对话框中的任何字段以输入更改。

文件名:捕获文件使用日期和时间自动命名。触摸此字段以输入自定义名称。

保存到：默认情况下，捕获文件保存在 **Downloads** 文件夹，该文件夹在 LRAT 文件系统中。您还可以将它们保存到 USB 存储设备，或点击 **保存到** 字段来选择一个不同的文件夹。请参阅 [管理文件](#)。

保存到 Link-Live：您也可以将捕获文件上传到 [Link-Live](#) 然后将它们下载到 PC 上进行分析。捕获 (.pcap) 文件出现在上传的文件中  [Link-Live](#) 中的页面。

注解：当您的捕获文件上传到 [Link-Live](#) 时，此注解将附加到您的捕获文件中。

测试注解：这是固定的 [测试注解](#) 将所有测试结果和文件上传到 [Link-Live](#)，直到您对其进行更改。在此处更改工作评论会在您的整个单元中更改它。



发现应用

这发现应用程序创建网络上的设备清单及其属性:设备类型、名称、地址、接口、VLAN、资源和其他连接或关联的设备。该应用程序允许您识别和分析网络设备,并作为使用其他应用程序进行进一步分析的起点,例如 路径分析和连接测试。

注意:此应用程序仅适用于 LinkRunner AT 4000。

发现章节内容

本章介绍了 Discovery 进程和应用程序屏幕的工作方式，显示了 Discovery 数据的示例，并详细说明了 Discovery 设置。

发现简介

主发现列表屏幕

发现详细信息屏幕

设备类型

设备名称和授权

发现设置

问题设置

TCP 端口扫描设置

发现简介

发现使用以太网和光纤查找、分类并显示网络组件的详细信息。Discovery 提供的信息可以包括以下内容：

- IP、BSSID 和 MAC 地址
- 设备名称
- 设备连接
- SNMP数据
- 网络问题
- 接口详情和统计

通过 ARP 和 Ping 扫描发现设备；SNMP、DNS、mDNS 和 netBIOS 查询；和被动交通监控。发现对每个设备进行分类。最多可报告 2,000 台设备。

Discovery 应用程序还可以检测 **问题** 发现设备，包括 **警告** 和 **失败** 条件。

这 LRAT 的发现过程在设备通电时开始。一旦网络连接 (**测试或管理**) 建立，主动发现过程开始。

发现通知图标  指示主动发现的进度。这个图标  表示当前没有可用于主动发现的

链接,可能是因为没有启用用于发现的端口连接或因为 AutoTest 正在运行。

Discovery 应用程序始终如一地监控网络流量,但默认情况下,主动发现过程每 90 分钟重新运行一次。您可以在[发现设置](#)。

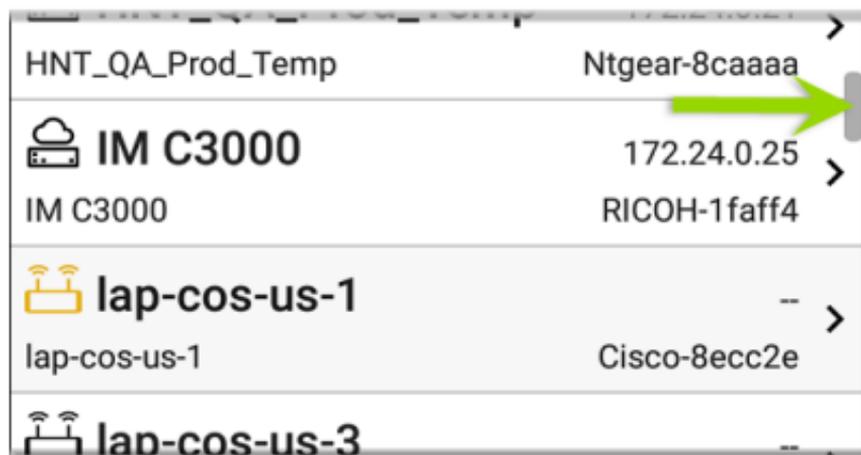
主发现列表页

主发现屏幕列出了所有设备LRAT发现了。

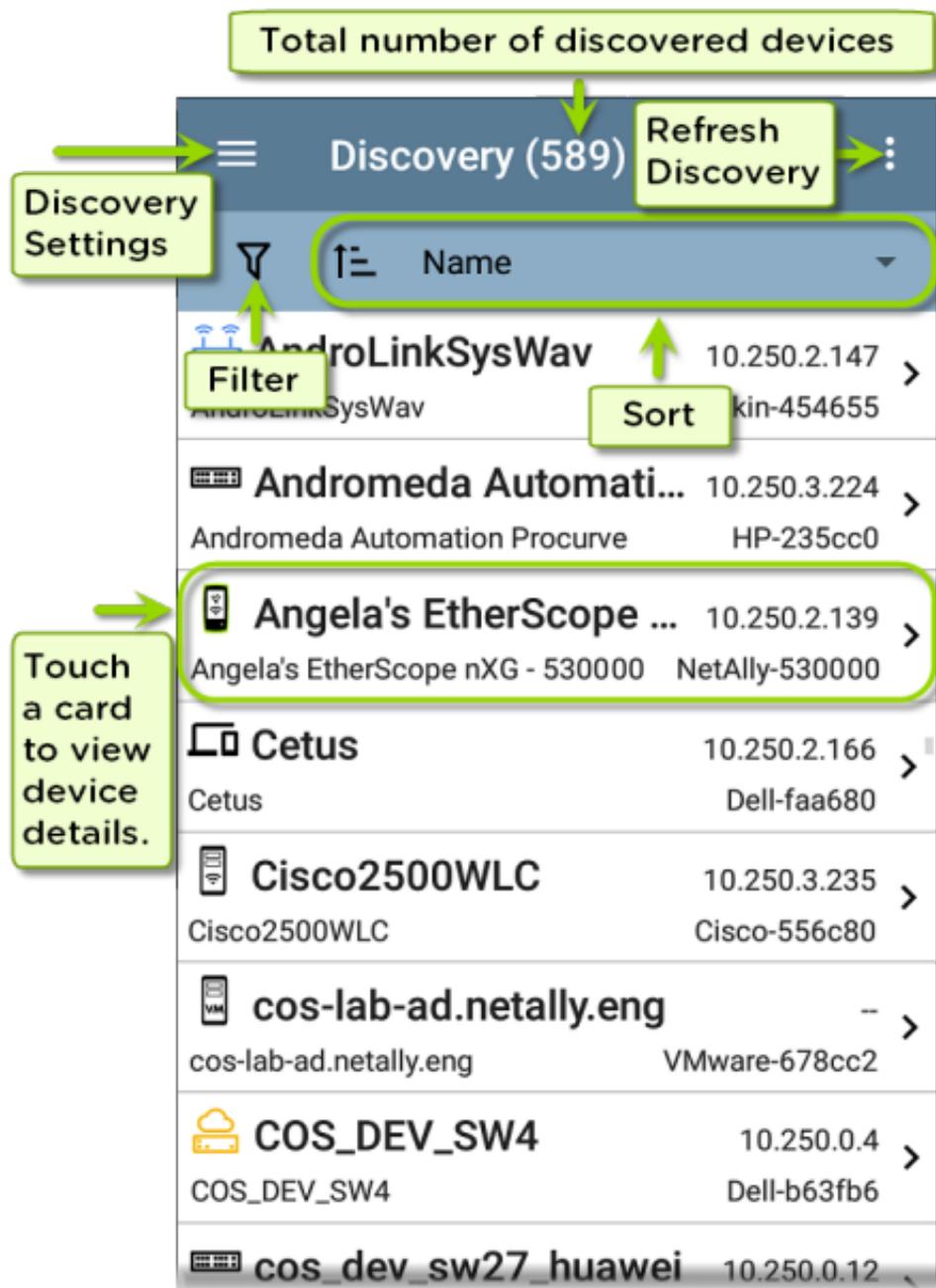
Discovery (182)		
Filter	Name	
LinkRunner_AT_5600a4	BizLinkK-1bddcf	
 LinkRunner_AT_5600a4 10.250.3.12 >	LinkRunner_AT_5600a4	NetAlly-5600a4
 LinkRunner_AT_5600a7 10.250.2.189 >	LinkRunner_AT_5600a7	NetAlly-5600a7
 LinkRunner_AT_5600a8 10.250.3.98 >	LinkRunner_AT_5600a8	NetAlly-5600a8
 LinkRunner_AT_5600ab 10.250.2.117 >	LinkRunner_AT_5600ab	EdimaxTe-cfb342
 LinkRunner_AT_5600ab 10.250.2.103 >	LinkRunner_AT_5600ab	NetAlly-5600ab
 LinkRunner_AT_5600ae 10.250.2.125 >	LinkRunner_AT_5600ae	TRENDnet-14b8f6
 LinkRunner_AT_5600ae 10.250.2.111 >	LinkRunner_AT_5600ae	NetAlly-5600ae

就像在 AutoTest 和其他 LRAT 屏幕上，Discovery 中的图标会改变颜色以指示警告 or 失败状况。Discovery 还显示设备图标蓝色指示不构成警告或故障的问题相关信息，以及 Green 表示先前的问题已解决。（见问题设置调整启用的问题和阈值。）

Discovery 屏幕和其他带有长列表的应用程序屏幕支持快速滚动。触摸并拖动列表右侧的滚动条手柄可快速上下滚动。

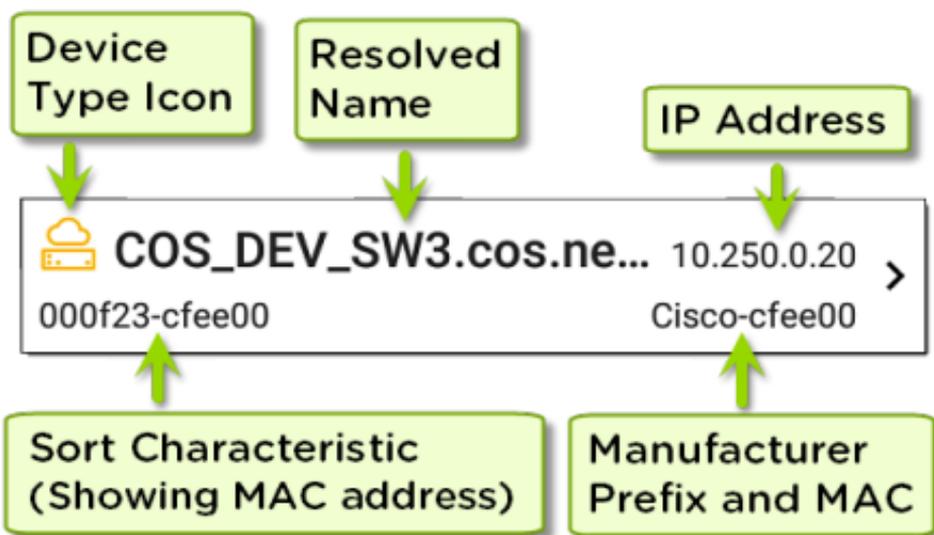


在发现主屏幕中，您可以对列出的设备进行过滤和排序，打开左侧导航以配置设置，并触摸设备的卡片以查看其详细信息。



发现列表卡

每个设备卡上显示的信息取决于所选的 Sort 元素和数据 LRAT 能够发现。

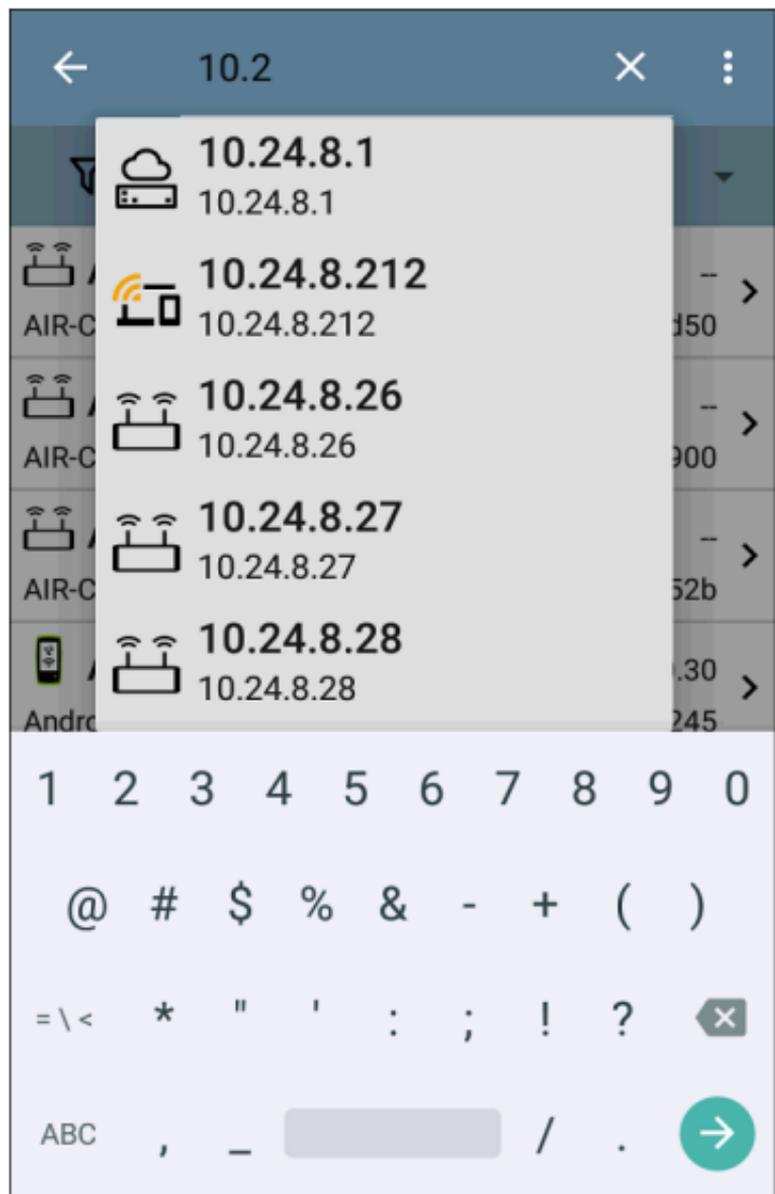


左下方的字段显示发现列表当前排序所依据的特征。在上图中，列表按 MAC 地址排序。看[发现排序](#)在本主题中了解有关排序的更多信息。

🔍 搜索发现列表

主发现屏幕提供搜索功能。点按搜索图标

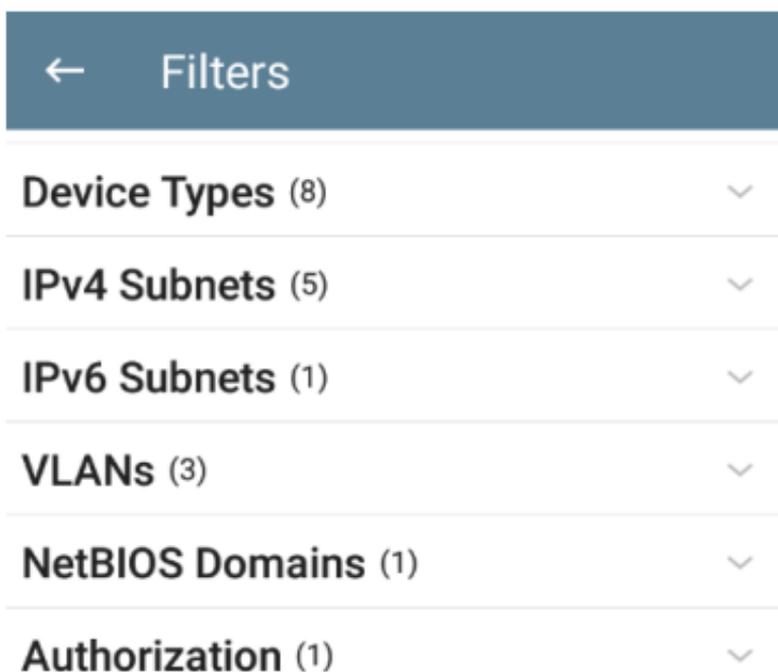
🔍 在屏幕顶部搜索发现的设备。



过滤发现列表

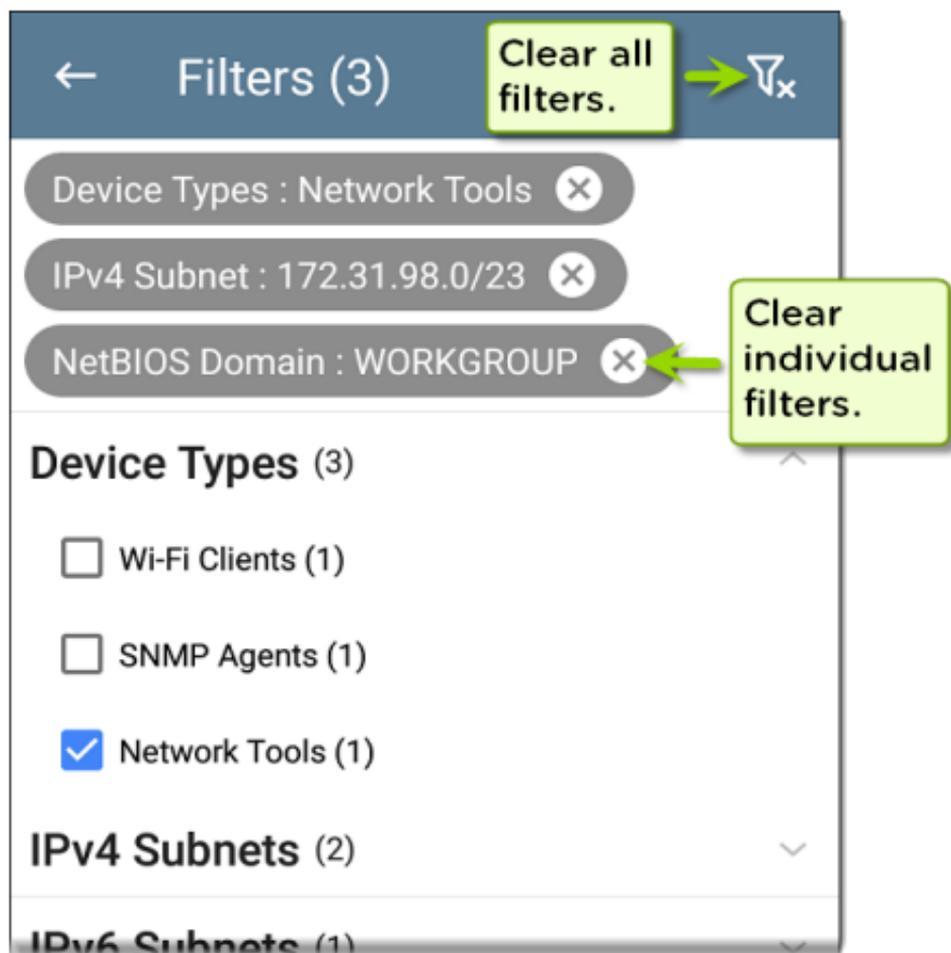
触摸过滤器按钮  在主发现屏幕的左上角附近设置过滤器，控制哪些设备显示在列表

中。



过滤器屏幕显示为每个类别发现的设备或域的数量。触摸类别名称以通过选中复选框来选择过滤器。主发现屏幕仅显示属于您选择的过滤器参数的那些设备或 ID。

选择过滤器后，这些活动过滤器将显示在“过滤器”屏幕的顶部。



- 轻触 **X** 每个过滤器右侧的按钮以清除它。
- 触摸右上角的清除过滤器图标可清除所有过滤器。

选择过滤器后，过滤器屏幕也会针对该特征进行过滤。例如，在上图中，用户选择了“网络工具”设备类型。因此，只有那些子网、地址、等与发现的网络工具在过滤器列表中保持可选。



返回主发现屏幕，屏幕标题显示已发现设备总数中已过滤设备的数量(在上图中，总共1308台设备中有152台已过滤设备)。

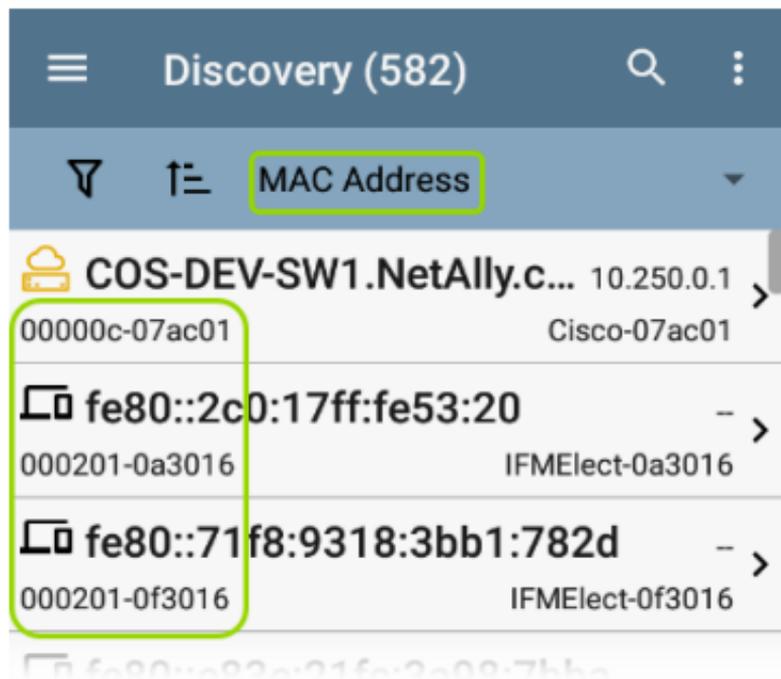
活动过滤器的数量显示在过滤器图标的左侧(上图中的3个活动过滤器)。

排序发现列表

点击排序栏或向下箭头打开排序下拉菜单。

Discovery (227)			
		Name	
Aruba335 ap nar		Problem	061 >
 Cisco37		Device Type	- >
Cisco3702_Erik			af0
 craigo		IP Address	105 >
craigo			57b
 DEMO_k		IPv6 Address	.23 >
DEMO_KIT_SW_		Mfg-MAC Address	547
 dns.goo		MAC Address	8.8 >
dns.google			-
 dns.goo		SSID	4.4 >
dns.google			-
 HNT_QA		Authorization	.21 >
HNT_QA_Prod_Temp			Ntqear-8caaaa

选择排序选项以根据您选择的特征对设备进行排序。



选定的排序选项显示在设备列表上方的排序栏中，每个设备的排序特征显示在设备类型图标下。在上图中，所有设备均按 MAC 地址排序。

点按排序顺序图标  在正常和反向之间切换排序顺序。

设备按组排序。已解析名称的设备出现在顶部(按正常顺序)，然后只有 IPv4、IPv6 和 MAC 地址的设备分别出现在下面。反转正常排序顺序会反转组内的设备，但不会更改组的顺序。

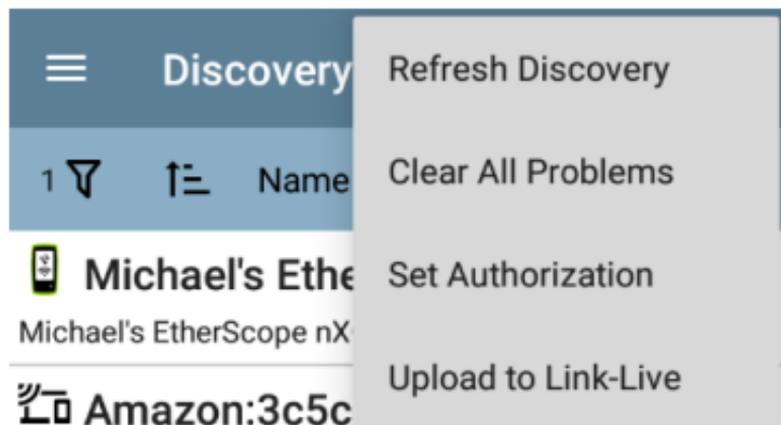
安全审计——批量授权

批量授权允许用户扩展LRAT 3000-4000的过滤将设备组织到以下安全类别中：

- 已授权:对于获准在您的网络上使用的设备
- 相邻设备:对于邻近组织拥有和控制的设备
- 标记:为特定设备提供可见性
- 未知:对于尚未识别或分类的设备
- 未经授权:对于不应该在网络上并且可能存在安全风险的设备
- 未指定:默认未分配授权状态

分类后，通过根据授权类型进行过滤，很容易立即识别网络上的任何新设备。新设备被标识为未指定。

要使用批量授权功能，请创建一个过滤器来标识要分类的设备。例如，您可以过滤建筑物中其他办公室使用的IP地址。过滤发现的设备列表后，选择溢出菜单。



选择**设置授权**查看这些设备当前的分类方式以及每个类别中的设备数量。在下面的示例中，38台设备属于其他办公室并且具有未指定的授权。

Set Authorization

38 of 226 devices selected

- Authorized (0)
- Neighbor (0)
- Flagged (0)
- Unknown (0)
- Unauthorized (0)
- Unspecified (38)

CANCEL

OK

注意：此屏幕上的初始选择默认为计数最高的类别。如果其他类别的计数不为零，则选择**确定**将所有设备的授权设置更改为所选类别。

选择适当的安全类别。如示例中所示，如果这些设备属于其他办公室，请选择：邻居，然后点击**确定**按钮。

Set Authorization

38 of 226 devices selected

- Authorized (0)
- Neighbor (38)
- Flagged (0)
- Unknown (0)
- Unauthorized (0)
- Unspecified (0)

CANCEL **OK**

您现在可以对发现的设备列表进行排序并清楚地识别设备的安全类别。来自其他办公室的设备被标识为：邻居

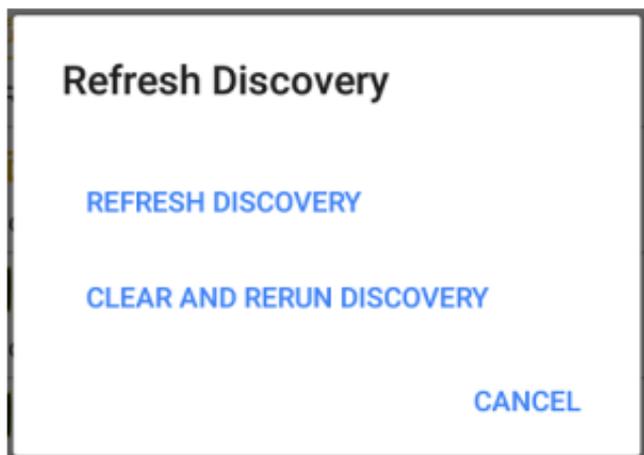
您可以[过滤](#)列表，方法是点击过滤器图标 ，点击[授权](#)，然后点击[邻居](#)，以仅显示邻居设备。您还可以[按授权对列表进行排序](#)，以显示已发现的设备，并明确标识邻居类别。

Discovery (79/276)		🔍	⋮
1	🔍	📏	Authorization
	AIR-CAP3702I-CO	-	>
Neighbor		Cisco-000d53	
	AirCheck_G3_5500c4	10.250.2.236	>
Neighbor		TRENDnet-eb8c72	
	BlackForestMist-Garage	-	>
Neighbor		Mist-dd6dd2	
	den-colspr-ap2	-	>
Neighbor		ExtremeN-01bae5	
	AmazonTe:dc91bf-938721	-	>
Neighbor		AmazonTe-938721	
	Apple:6c7e67-d13251	-	>
Neighbor		Apple-d13251	
	Apple:88665a-496103	-	>
Neighbor		Apple-496103	

注意:批量授权在设备的默认 MAC 地址上运行。如果设备有多个 MAC,则仅在默认 MAC 地址上设置授权。没有发现 MAC 地址的设备,例如未知交换机和网外设备,不能有授权设置。

刷新发现

轻触操作溢出图标在主发现屏幕的右上角,然后选择刷新刷新正在发现的过程。



刷新发现重新启动主动发现过程而不清除已发现的设备。

清除并重新运行发现清除累积的结果并重新启动发现过程。

将发现结果上传到 Link-Live

触摸操作溢出图标在主发现屏幕的右上角，然后选择上传到 **Link-Live** 将当前发现结果发送到分析页面在 Link-Live.com 上。



Link-Live

by NetAlly



Discovery Snapshot Name

20190802_131842

Comment

1st Floor

Job Comment

Psych Building



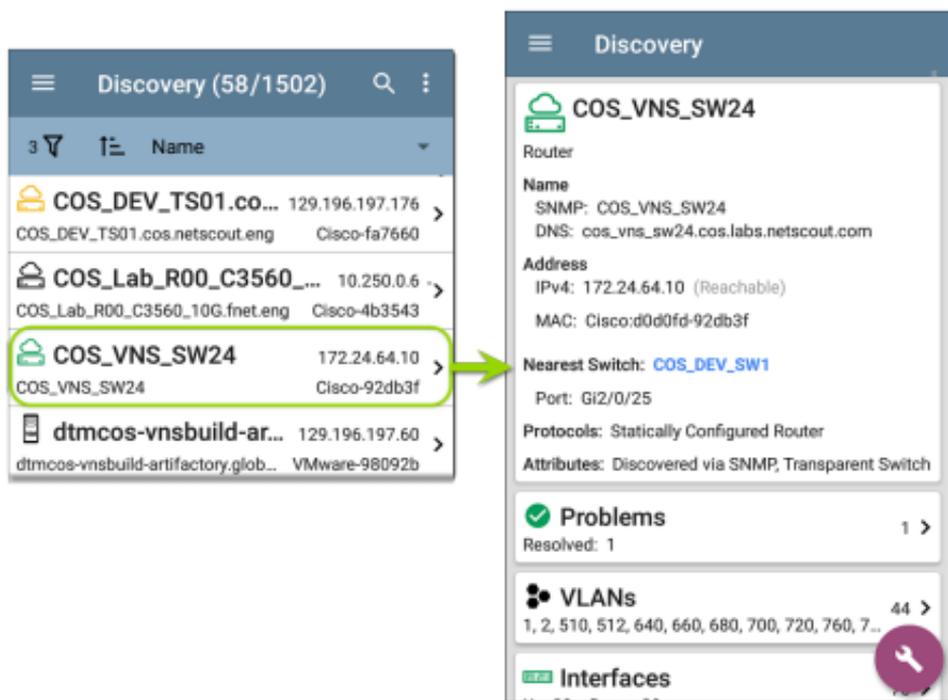
SAVE TO ANALYSIS FILES

参考[Link-Live 章节](#)获取更多信息。

发现详细信息

点击主发现列表屏幕上的任何设备卡以查看设备详细信息。

下面的示例调出路由器卡及其详细信息屏幕。



详细信息屏幕上可用的数据和操作因设备类型，连接方式和 LRAT 可以发现的数据而异。换句话说，只有每个设备的可发现信息才会显示在“详细信息”屏幕上。

 **Discovery**

 **123.136.196.236**
Switch
Address
IPv4: 123.136.196.236 (Reachable)
IPv6: fe80::7ad2:94ff:fec0:e607
MAC: Ntgear:78d294-c0e607
Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 2 >
IPv4: 1 IPv6: 1 MAC: 1

 **VLANs** 3 >
1, 2, 3

 **Interfaces** 15 >
Up: 2 Down: 13

 **SNMP** >
Uptime: 11 weeks 1 day 5 hours 14 minutes



详细信息屏幕上的可用数据和操作因设备类型、连接和数据的不同而有很大差异。LRAT能够发现。换言之，“详细信息”屏幕上仅显示每个设备的可发现信息。

Discovery

 **123.136.196.236**

Switch

Address

IPv4: 123.136.196.236 (Reachable)
IPv6: fe80::7ad2:94ff:fec0:e607
MAC: Ntgear:78d294-c0e607

Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 2 >

IPv4: 1 IPv6: 1 MAC: 1

 **VLANs** 3 >

1, 2, 3

 **Interfaces** 15 >

Up: 2 Down: 13

 **SNMP** >

Uptime: 11 weeks 1 day 5 hours 14 minutes



对于上面显示的交换机屏幕，Discovery 能够找到 IP 地址，但无法找到交换机的名称。

每个详细信息屏幕显示有关所选设备的附加信息、检测到的任何问题LRAT, 并为其他连接或相应的网络元素计数。

每个“详细信息”屏幕还具有一个 FAB 按钮, 可让您执行其他操作或在设备上运行其他应用程序。可用的操作和应用程序取决于设备类型和可用的连接。请参阅 [发现应用程序浮动操作菜单](#) 以获取更多信息

参考[设备类型](#)有关不同设备的详细信息LRAT可以发现。

顶部详细信息卡

详细信息屏幕顶部的卡片总结了所选设备的发现数据。

卡片顶部显示设备类型和图标(带有警告上例图像中的状态)。

显示在顶部详细信息屏幕卡上的其余字段取决于设备类型和LRAT可以发现设备。

在发现详细信息屏幕上, 您可以触摸任何[蓝色链接的姓名或地址](#)打开发现链接设备的屏幕。

注意:非下划线链接在同一个应用程序中打开(在本例中为 Discovery),以及[下划线链接](#)在不同的应用程序中打开。

最近的交换机链接打开这些设备的发现应用程序详细信息屏幕。

顶部详细信息卡上的数据字段

根据设备类型和信息,以下字段可能会出现在设备详细信息屏幕的顶部卡片上LRAT能够发现:

名称:发现设备的主机名。此部分可以显示用户定义的 DNS、mDNS、SNMP、NetBIOS、AP 和已发现的虚拟机名称。

地址:发现设备的 IPv4、IPv6、和/或 MAC 地址。此部分显示每种类型的默认(首次发现)地址。如需更多地址,请选择[地址](#)卡时可用。

授权:此字段显示用户分配的设备授权状态。看[为设备分配名称和授权](#)。

最近的交换机:标识为最接近设备的开关的名称或地址

端口:设备连接的物理端口

VLAN ID:设备所在VLAN的ID

协议:路由协议,通过数据包分析发现,在设备或网络上运行

服务:本设备提供的网络服务,如 DHCP 或 DNS

属性:其他发现的关于设备的属性

管理程序:运行虚拟机的管理程序的名称

虚机:虚拟机名称

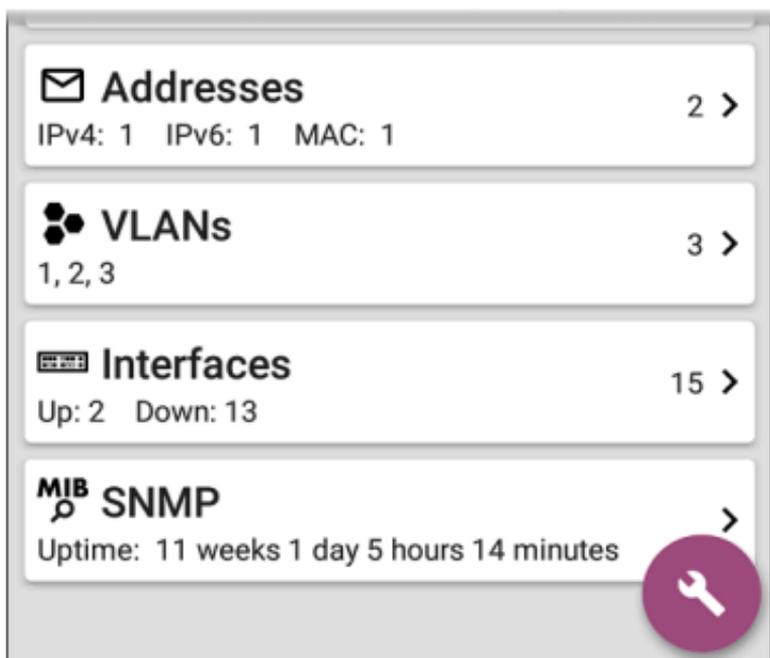
来宾操作系统:运行在虚拟机上的操作系统

内存预留:为虚拟机保留的内存量

上次看到:时间LRAT最近检测到的设备

设备详细信息中的下方选项卡

点击设备详细信息屏幕上任何下方的选项卡, 查看更多发现的特征并“深入”到所选设备的特定问题、地址、接口等。



带有列表的屏幕(例如下面显示的地址)也提供排序选项。

Addresses (3)		
↑	Address	▼
IPv4 10.250.0.1 10.250.0.120	BSSID	/22 549 >
IPv6 2001:c001:c0de 2001:c001:c0de	IP Address	... 549 >
IPv6 fe80::1618:77ff:fe80::1618:77ff	IPv6 Address	549 >
	Mfg-MAC Address	549 >
	MAC Address	

本主题的其余部分提供了每种类型的“详细信息”屏幕和其他分析选项的示例。

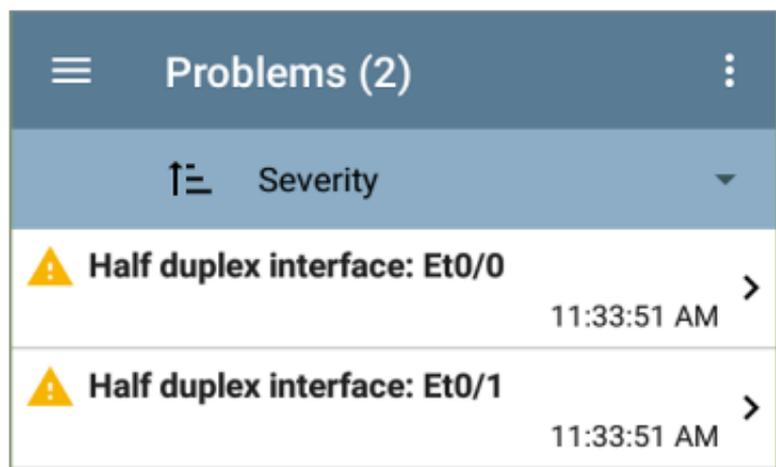
请记住，您可以使用向右的箭头触摸任何卡片 ➤ 以打开包含有关设备或特性的更多信息的新页面。

问题

问题卡显示最严重问题的图标颜色, 以及检测到的问题数量**警告**, **失败或错误**, **信息**, 和**解决**设备或网络组件的条件。

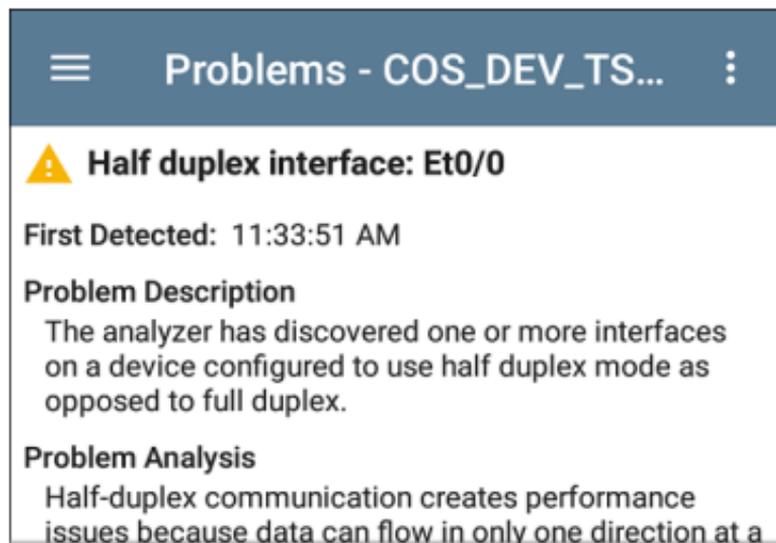


点击问题卡以查看问题列表屏幕(除非仅检测到 1 个问题, 在这种情况下, 将打开详细的问题描述, 跳过列表屏幕)。



点按排序字段以对列表进行排序严重性或者到问题出现的时候首次检测。

在问题列表屏幕上, 触摸问题所在的行以阅读详细说明。



☰ Problems - COS_DEV_TS... ☰

⚠ Half duplex interface: Et0/0

First Detected: 11:33:51 AM

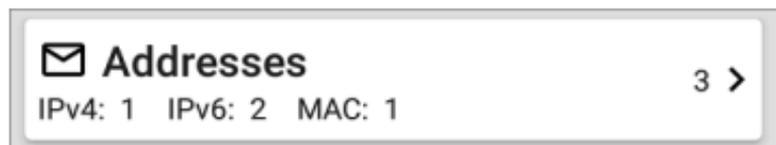
Problem Description
The analyzer has discovered one or more interfaces on a device configured to use half duplex mode as opposed to full duplex.

Problem Analysis
Half-duplex communication creates performance issues because data can flow in only one direction at a

触摸动作溢出按钮  在问题列表或描述屏幕的右上角清除问题。

参考[问题设置](#)选择您的设备检测和显示哪些问题。

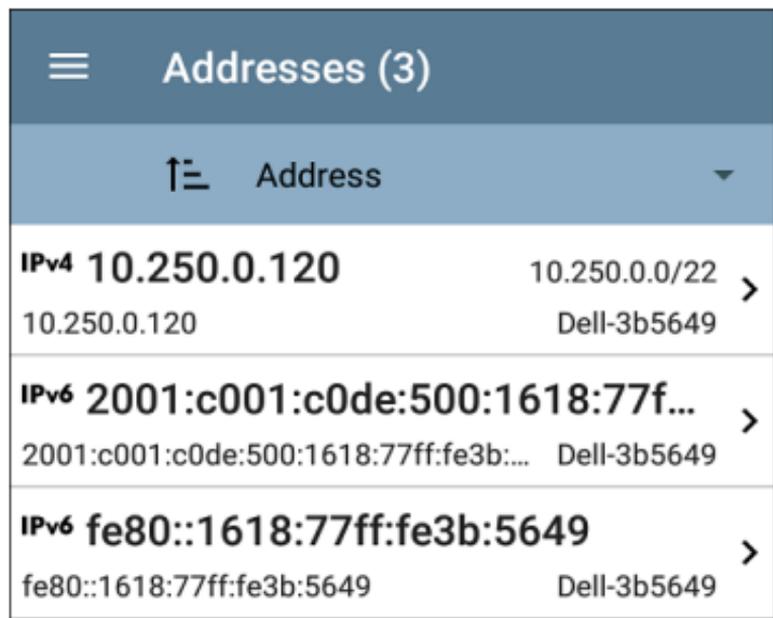
地址



 **Addresses** 3 >

IPv4: 1 IPv6: 2 MAC: 1

地址卡显示发现的每种地址类型的数量：IPv4、IPv6、MAC 和/或。点击查看地址和相关信息。

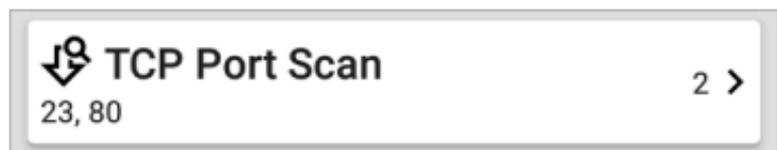


Addresses (3)		
↑	Address	▼
IPv4	10.250.0.120	10.250.0.0/22 >
	10.250.0.120	Dell-3b5649
IPv6	2001:c001:c0de:500:1618:77f...	>
	2001:c001:c0de:500:1618:77ff:fe3b:...	Dell-3b5649
IPv6	fe80::1618:77ff:fe3b:5649	>
	fe80::1618:77ff:fe3b:5649	Dell-3b5649

在地址列表屏幕中，您可以对列表顺序进行排序并点击任何发现的地址以进一步调查该地址。

TCP端口扫描

如果您运行了 TCP 端口扫描(从[发现FAB](#)) 在设备或 IP 地址上, TCP 端口扫描卡会出现在设备的详细信息屏幕上。



此卡片列出开放端口号并显示开放端口总数。点击卡片打开TCP 端口扫描屏幕。

您也可以从[发现浮动操作菜单](#)。



☰ TCP Port Scan START ⚙️

📄 HNT_QA_Prod_Temp

IP Address: 172.24.0.21
 Interface: Wired Port
 Scan List: 1-2049, 3268-3389, 3535, 5000-6005, 8008-8443

Results
 Status: Completed

Port	Description
23	telnet
80	www-http

🔧

TCP 端口扫描结果屏幕的顶部显示被测设备的名称或 IP 地址以及以下字段：

IP地址：被扫描设备的IP地址

界面：运行测试的测试或管理端口，在[TCP 端口扫描设置](#)

扫描列表：测试的端口号列表

结果

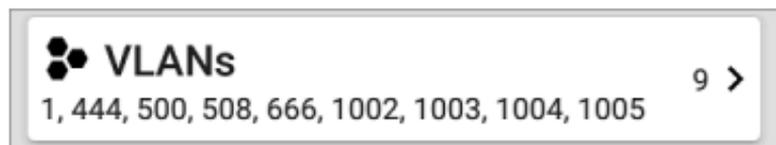
状态: 端口扫描的当前状态

端口/描述: 所有检测到的开放端口及其描述的列表

参考[TCP 端口扫描设置](#)。

VLANs

VLAN 卡显示此设备正在使用或为其配置的 VLAN ID。



如果未检测到或配置 VLAN, 则不会出现此卡。点击卡片以打开 VLAN 屏幕。



COS_DEV_SW33

VLAN	Description
1	default
444	VLAN0444
500	VLAN0500
508	LabWiFi
666	VLAN0666
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

VLAN 详细信息屏幕还显示每个 VLAN ID 的描述。

端口

使用 SNMP 发现接口。

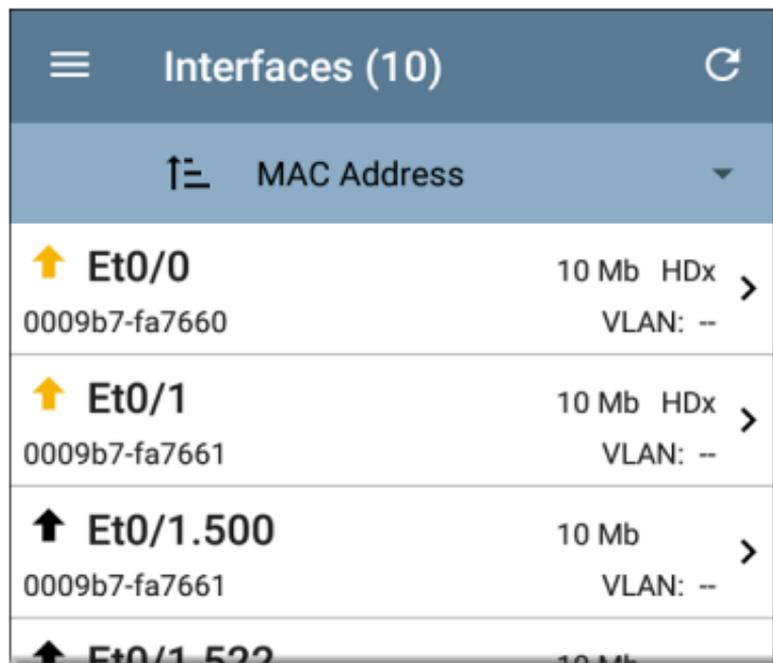
	Interfaces	171 >
Up: 20	Down: 151	

接口卡在右侧显示了 Up 和 Down 接口的数量以及接口总数。

点击卡片以查看接口列表。

Interfaces (171)		↻
↑	Interface Status	▼
↑	VLAN-1002	0 b >
Status: up	VLAN: 1002	
↑	VLAN-1003	0 b >
Status: up	VLAN: 1003	
↑	VLAN-1005	0 b >
Status: up	VLAN: 1005	
↓	Fa1	100 Mb >
Status: down	VLAN: --	
↓	Gi1/3	1 Gb FDx >
Status: down	VLAN: 1	

与其他 Discovery 列表屏幕一样，Interfaces 列表提供了许多排序选项，所选的排序选项会影响显示的信息类型。上图显示了按状态(向上或向下)排序的接口。下图显示了按 MAC 地址排序的接口，因此显示了每个接口的 MAC 地址。



Interfaces (10)			
↑ MAC Address			
↑ Et0/0	10 Mb HDx		>
0009b7-fa7660	VLAN: --		
↑ Et0/1	10 Mb HDx		>
0009b7-fa7661	VLAN: --		
↑ Et0/1.500	10 Mb		>
0009b7-fa7661	VLAN: --		
↑ Et0/1.522	10 Mb		>

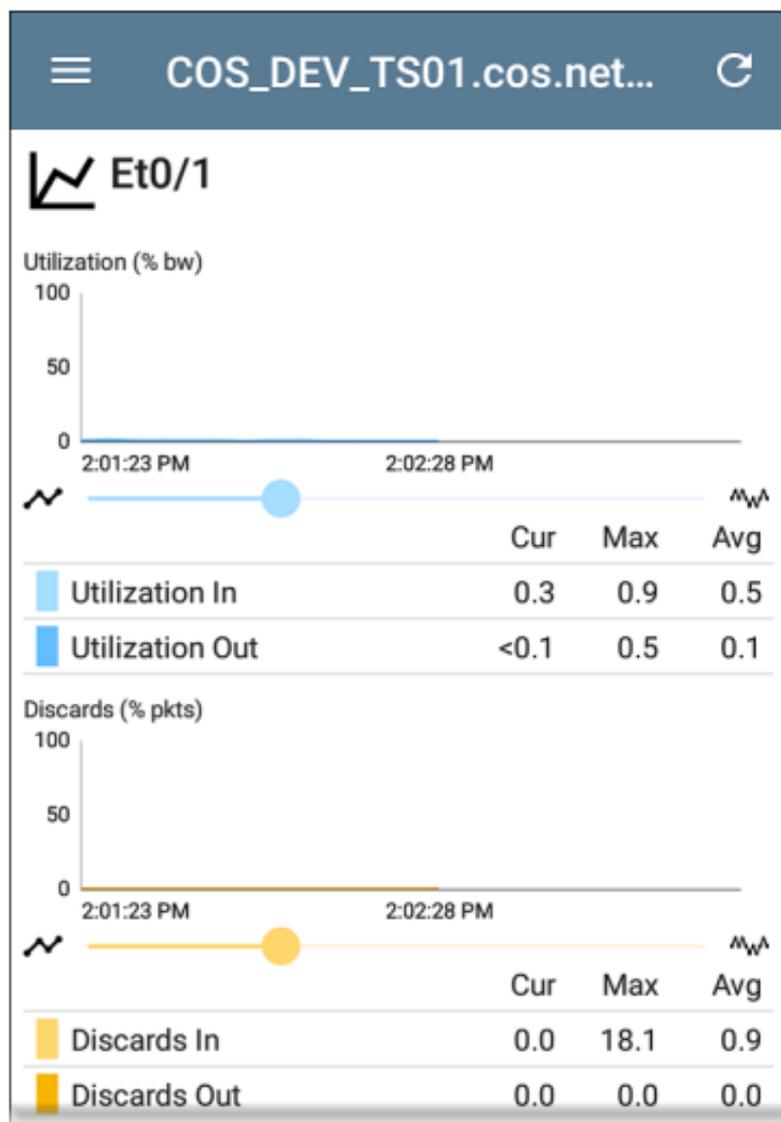
触摸接口行会打开所选接口的新发现详细信息屏幕。

The screenshot shows a mobile application interface for a network device. At the top, there is a blue header bar with a hamburger menu icon on the left, the text "COS_DEV_TS01.cos.net..." in the center, and a refresh icon on the right. Below the header, the main content area is divided into three sections. The first section is titled "Et0/1" with an orange upward-pointing arrow icon. It contains the following text: "DOT1Q Trunk to CISCO_3750_PoE COS_DEV_SW2 f...", "Status: up", "Speed: 10 Mb", "Duplex: HDx", "MTU: 1500", "Connected Device: COS_DEV_SW1", "Port: Gi2/0/30", "Address", and "MAC: Cisco:0009b7-fa7661". The second section is titled "Devices" with a square icon and a right-pointing arrow, followed by the number "0". The third section is titled "Statistics" with a line graph icon and a right-pointing arrow, followed by the text "Util: 0.3 % Discards: 0.0 % Errors: 0.0 %".

接口详细信息屏幕包含接口的描述以及有关其状态、连接的设备 and 端口以及地址的信息。

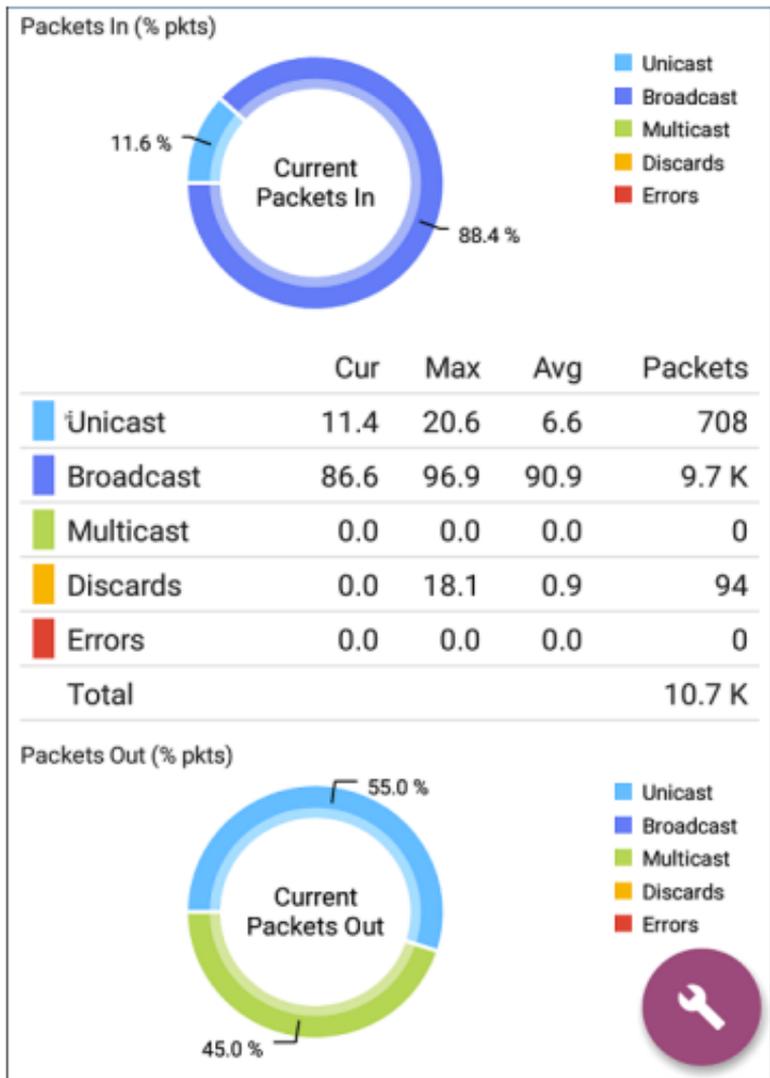
MTU: Maximum Transmission Unit, 接口端口配置的最大包帧大小

在此屏幕上, 您可以触摸下方的卡片以查看任何发现**VLANs** 和设备用于接口以及接口图统计信息。



统计屏幕显示利用率、数据包丢弃、数据包错误的实时趋势图。参考[趋势图](#)有关图形平移和缩放控件概述的主题。

趋势图下方是进出接口的数据包传输的饼图。



SNMP

MIB SNMP

Uptime: 5 weeks 6 days 2 hours 57 minutes



SNMP card 显示 SNMP 正常运行时间。触摸卡片以获取 SNMP 详细信息。

☰
COS_DEV_SW34

MIB SNMP

SNMP System Group
 Uptime: 5 weeks 6 days 2 hours 58 minutes
 Manufacturer: Cisco
 Model: cat4500e
 Serial Number: FOX1407GRJA
 HW Version: V02
 SW Version: 15.2(2)E7
 Description:
 Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICES-M), Version 15.2(2)E7, RELEASE SOFTWARE (fc3)
 Technical Support:
<http://www.cisco.com/techsupport>
 Copyright (c) 1986-2017 by Cisco Systems, Inc.
 Compiled Wed 12-Jul-17 14:36 by

SNMP
 Type: SNMP v1/v2/v3
 Engine ID: 80000009030068efbd6f4b80
 Communication: SNMP v2
 Using: Default Community String: public

SNMP 系统组: 这些数据字段是从系统组和其他关键设备版本信息中收集的。

SNMP: 设备支持的 SNMP 版本、引擎 ID(适用于 v3) 以及 LRAT 当前正在与设备通信以及凭据, 包括正在使用的社区字符串

连接的设备

已连接设备卡出现在详细信息屏幕上 **未知开关**。虽然 LRAT 可能无法直接识别连接的交换机，连接到它的设备提供有关交换机运行位置的线索。



Connected Devices

8 >

已连接设备卡显示已发现的连接到未知交换机的设备的数量。触摸该卡会打开一个包含已连接设备的发现列表屏幕。

☰ Connected Devices (8)		
↑☰	IP Address	▼
 10.250.2.143		-- >
10.250.2.143	NetAlly-02506e	
 10.250.2.177		-- >
10.250.2.177	TRENDn-af1e30	
 10.250.3.32		-- >
10.250.3.32	NetAlly-02506e	

资源

 **Resources**
>

CPU: 28% Memory: 35%

资源卡显示设备上 CPU、内存和存储使用的百分比。此信息是通过 SNMP 收集的。

触摸卡片以查看当前和最大资源利用率测量值。

☰
COS_DEV_SW34

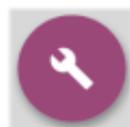


Resources

	Cur	Max
CPU %	12	12
Memory %	60	60

Last Update: 1:44:22 PM

默认，LRAT 显示 **警告** 如果 CPU、内存或存储利用率高于 90%。您可以在 Wired 中调整问题检测和阈值 [问题设置](#) 从发现导航抽屉访问。



发现应用程序浮动操作菜单

浮动操作按钮(FAB)在详细信息屏幕上提供额外的操作，具体取决于设备类型和可用连接。

开启其他NetAlly应用程序，例如，从“详细信息”页面自动使用设备的名称和/或地址填充新应用程序。用这种方式发现应用程序提供了有用的快捷方式，并避免让您在其他测试应用程序中重新输入目标地址或主机名。

- 轻触 TCP 端口扫描打开 TCP 端口扫描屏幕在发现应用程序中。
- 选择浏览打开 Google Chromium。
- 轻触添加测试目标创建与当前所选设备匹配的新 AutoTest 目标。首先显示一个对话框以选择测试类型，然后 AutoTest 应用程序打开，显示新添加的目标设置，您可以在其中进一步自定义它。
- 对于具有 MAC 地址的设备，触摸名称和授权打开一个对话框，您可以在其中分配自定义用户名和授权状态。

- 轻触更多打开附加浮动操作按钮的辅助列表。轻触返回返回到原始列表。
 - 轻触更多打开附加浮动操作按钮的辅助列表。轻触返回返回到原始列表。
 - **Telnet or SSH** 打开 JuiceSSH 应用程序。
 - 点击返回返回主 FAB 列表。

自动填充设备地址

从 FAB 打开另一个应用程序时，显示在 FAB 上的默认地址和名称 [顶部详细信息卡](#) 目标是否已填充。

例如，下面详细信息屏幕中显示的路由器具有多个 IPv4 和 MAC 地址(可以通过触摸地址卡进行查看)。

 **Discovery**

 **Rack5SW1.fnet.eng**
Router

Name
SNMP: Rack5SW1.fnet.eng

Address
IPv4: 10.250.3.207 (Reachable)
MAC: Cisco:00141c-8945c1

Nearest Switch: [COS_DEV_SW1](#)
Port: Gi2/0/39

Protocols: Statically Configured Router

Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 6 >
IPv4: 6 MAC: 5

 **VLANs** 66 >
1, 2, 21, 42, 78, 85, 154, 202, 236, 378, 478, 5...

 **Interfaces** 
Up: 12 Down: 30

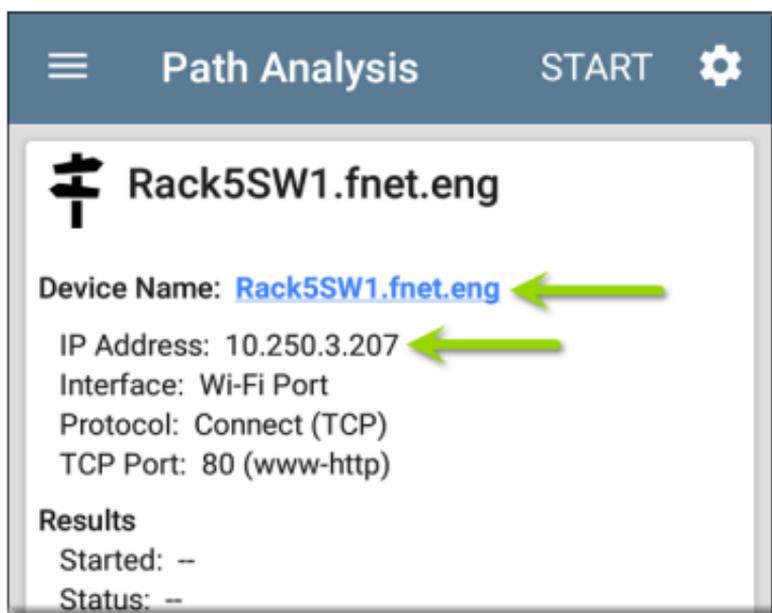
当您打开 FAB 并选择不同的应用程序(例如路径分析)时,路径分析应用程序中只会填充详细信息屏幕顶部列出的地址和名称。



 **Rack5SW1.fnet.eng**
Router

Name
SNMP: Rack5SW1.fnet.eng ←

Address
IPv4: 10.250.3.207 (Reachable) ←
MAC: Cisco:00141c-8945c1



☰ **Path Analysis** START ⚙️

 **Rack5SW1.fnet.eng**

Device Name: [Rack5SW1.fnet.eng](#) ←

IP Address: 10.250.3.207 ←

Interface: Wi-Fi Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)

Results
Started: --
Status: --

要打开具有不同地址的另一个屏幕或应用程序，请打开地址卡，然后选择另一个地址以查看其详细信息页面。

设备类型

Discovery 应用程序列出并分析了本节中介绍的设备类型。不同的数据可能提供给 LRAT 取决于设备类型、发现方式以及您配置的设置。

参考 [发现设置 for SNMP 配置](#) 和 [通过其他设备发现的设备](#) 选项。

有关不同详细信息卡和屏幕的说明，请参阅 [发现详情](#)。

本节其余部分中的图像代表 Discovery 可能为每种设备类型显示的数据示例。

路由器

LRAT通过监控流量和查询主机来发现 IP 路由器。

Discovery

 **COS_DEV_SW34**
Router

Name
SNMP: COS_DEV_SW34

Address
IPv4: 10.250.0.34 (Reachable)
MAC: Cisco:68efbd-6f4bbf

Nearest Switch: [Rack5SW1.fnet.eng](#)
Port: Gi1/0/11
VLAN ID: 500

Protocols: Statically Configured Router

Attributes: Discovered via SNMP, Transparent Switch

 **VLANs** 17 >
1, 244, 500, 801, 803, 804, 805, 806, 825, 830...

 **Interfaces** 171 >
Up: 20 Down: 151

 **SNMP** >

交换机

交换机也可以通过监控流量和查询主机来发现。

 **Discovery**

 **cos-dev-sw18-poe**

Switch

Name
SNMP: cos-dev-sw18-poe

Address
IPv4: 10.250.3.216 (Reachable)
MAC: Cisco:503de5-220c43

Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 2 >

IPv4: 2 MAC: 2

 **VLANs** 37 >

1, 11, 196, 500, 502, 504, 508, 510, 511, 518, ...

 **Interfaces** 38 >

Up: 9 Down: 29

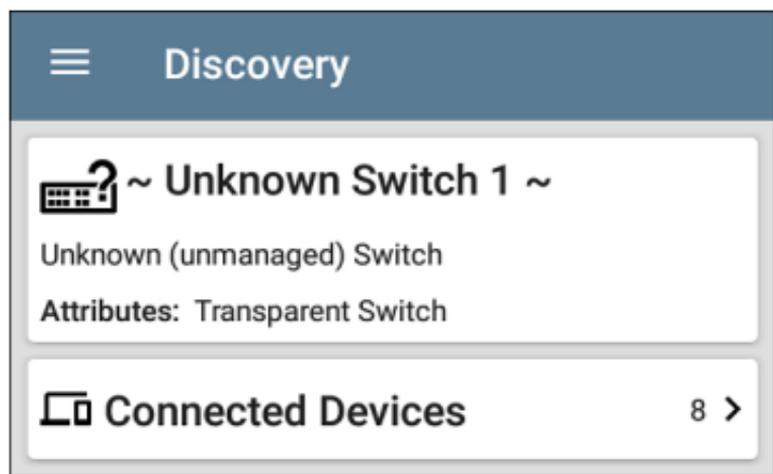
 **SNMP** 

Uptime: 27 weeks 2 days 7 hours 25 minutes

未知交换机

基于对通过周围交换机的流量的分析，间接检测到未知交换机。虽然LRAT无法识别交换机本身，它可以通过该空间中的设备MAC地址感知交换机在网络上的哪个位置处于活动状态。

未知交换机由LRAT当他们被发现时。这些数字可能会在下次运行发现过程时发生变化。



Unknown Switches Details 屏幕显示连接到交换机的设备数量，并允许您通过点击[连接的](#)设备卡片。连接的设备提供有关未知开关可能位于何处的线索。

网络服务器

网络服务器包括 NetBIOS、DHCP 和 DNS 服务器。

☰
Discovery



Compass.netally.eng

Network Server

Name
 Virtual Machine: [Compass.netally.eng](#)
 DNS: [compass.fnet.eng](#)
 NetBIOS: COMPASS

Address
 IPv4: 10.250.3.221 (Reachable)
 IPv6: 2001:c001:c0de:500:d1f5:d8e0:a81:3397
 MAC: VMware:000c29-13235b

Nearest Switch: ~ [Unknown Switch 4](#) ~

Hypervisor: [COS-PNT-VM.fnet.eng](#)
 10.250.3.251

Virtual Machine
 Guest OS: Windows Server 2008 Standard Edition,
 32-bit Service Pack 2 (Build 6003)
 Memory Reservation: 2,048MB

Services: DNS, Virtual Machine



 **Addresses**

IP 1 1 IP 6 8 MAC 8

虚拟机管理程序

VMware 管理程序是通过 SNMP 发现的。必须为管理程序启用管理程序的 SNMP 代理 LRAT 发现它并将其归类为管理程序。

☰
Discovery



COS-PNT-VM.fnet.eng

Hypervisor

Name
SNMP: COS-PNT-VM.fnet.eng

Address
IPv4: 10.250.3.251 (Reachable)
IPv6: fe80::1618:77ff:fe34:db2a
MAC: Dell:141877-34db2a

Nearest Switch: ~ Unknown Switch 4 ~

Hypervisor
Product Name: VMware ESXi
Product Version: 6.7.0
Product Build: 13644319
Memory: 98207MB
CPUs: 2
Virtual Machines: 16

Services: Hypervisor

Attributes: Port Aggregation



Addresses



IPv4: 1 IPv6: 1 MAC: 1

虚拟机

VMware 虚拟机是从启用 SNMP 的 VMware 管理程序中的 VMware 客户端表中发现的。如果设备具有 VMware MAC, 则它们也被归类为虚拟机。



Discovery



Cisco ACS 5.8 Linux

Virtual Machine

Name

Virtual Machine: Cisco ACS 5.8 Linux

Address

IPv4: 10.250.0.59 (Reachable)

IPv6: 2001:c001:c0de:500:20c:29ff:fe0b:e61c

MAC: VMware:000c29-0be61c

Nearest Switch: ~ Unknown Switch 4 ~

Hypervisor: [COS-PNT-VM.fnet.eng](#)

10.250.3.251

Virtual Machine

Guest OS: Linux 2.6.32-431.20.3.el6.x86_64 Red Hat Enterprise Linux Server release 6.4 (Santiago)

Memory Reservation: 4,096MB

Services: Virtual Machine



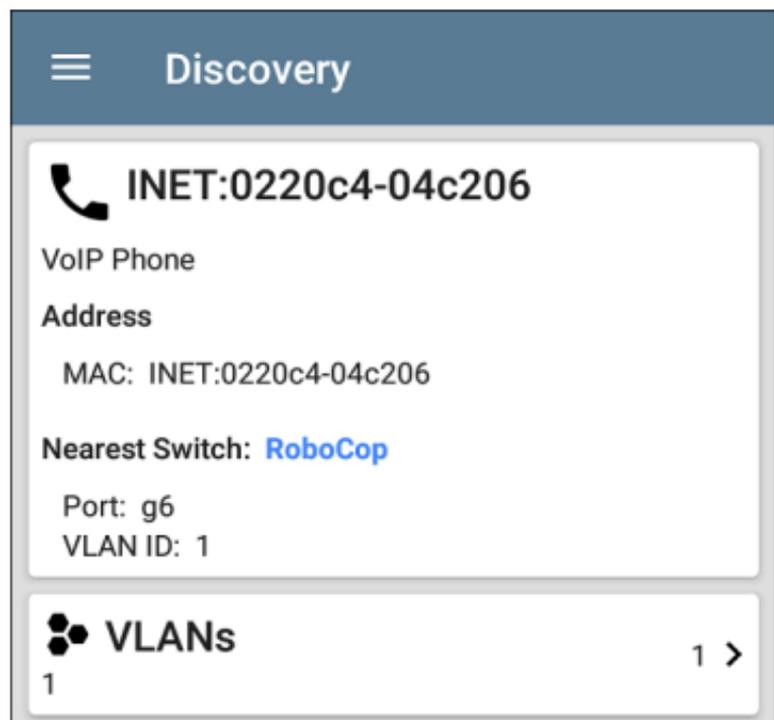
Addresses

IPv4: 1 IPv6: 2 MAC: 1



VoIP电话

VoIP 发现提供对网络的 VoIP 和第 2/3 层配置的可见性。



The screenshot shows a mobile application interface with a dark blue header containing a hamburger menu icon and the word "Discovery". Below the header is a white card with a grey border. The card displays a VoIP phone icon, the text "INET:0220c4-04c206", and the label "VoIP Phone". Underneath, the "Address" section shows "MAC: INET:0220c4-04c206". The "Nearest Switch" is listed as "RoboCop" in blue text. Below that, the "Port" is "g6" and the "VLAN ID" is "1". At the bottom of the card is a section titled "VLANs" with a cluster of three dots icon, the number "1", and a right-pointing arrow.

Discovery

 **INET:0220c4-04c206**

VoIP Phone

Address

MAC: INET:0220c4-04c206

Nearest Switch: [RoboCop](#)

Port: g6
VLAN ID: 1

 **VLANs** 1 >

打印机

这个LRAT通过 SNMP 打印机 MIB 和 IPX 打印机通过诊断请求和查询识别 IP 打印机。

 **Discovery**

 **TOSHIBA e-STUDIO3005AC**
Printer
Name
SNMP: TOSHIBA e-STUDIO3005AC
mDNS: MFP12073521
NetBIOS: MFP12073521
Address
IPv4: 143.131.143.43 (Reachable)
IPv6: fe80::280:91ff:feb8:3a31
MAC: Tokyo:008091-b83a31

 **Problems** 1 >
Warnings: 1

 **Addresses** 3 >
IPv4: 1 IPv6: 2 MAC: 1

 **Interfaces** 2 >
Up: 2 Down: 0

 **SNMP**



SNMP 代理

SNMP 使用 SNMP 查询发现代理。看 [SNMP 配置](#)。

注意：如果 LRAT 无法发现设备上的 SNMP 代理，它们可能连接到另一个子网，例如管理子网。通过将子网添加到解决此问题 [扩展范围](#)。



The screenshot shows a 'Discovery' interface with a blue header. Below the header is a card for 'LAB Sensor 1'. The card contains the following information:

- SNMP Agent**
- Name**: SNMP: LAB Sensor 1
- Address**: IPv4: 10.250.0.76 (Reachable)
MAC: HWServ:000a59-022933
- Nearest Switch**: [JuniperEX2200](#)
- Port**: ge-0/0/23

Below the card is a section for 'MIB SNMP' with a right-pointing arrow and the text 'Uptime: 6 days 4 hours 29 minutes'.

参考 [SNMP 详细信息](#)。

NetAlly网络工具

此LRAT还可以识别其他NetAlly网络测试员，包括LRATs、AirCheck G2、OneTouch、LinkRunner(AT和G2)和测试附件。

Discovery (122/708)		
1	Device Type	
 fe80::2c0:17ff:fe53:138	EtherScope nXG	NetAlly-530138
 fe80::2c0:17ff:fe53:146	EtherScope nXG	NetAlly-530146
 10.250.3.147	AirCheck G2	NetAlly-350593
 NetAlly:00c017-353246	AirCheck G2	NetAlly-353246
 10.250.2.117	LinkRunner G2	NetAlly-c50070
 10.250.2.132	Test Accessory	NetAlly-330e87

上图显示了几个NetAlly工具，因为它们出现在主发现列表中。

LRAT在“详细信息”屏幕上显示它可以收集的
有关每个工具的所有信息。



Discovery

 **10.250.2.240**

LinkRunner G2

Address

IPv4: 10.250.2.240 (Reachable)
IPv6: fe80::2c0:17ff:fec5:88
MAC: NetAlly:00c017-c50088

Nearest Switch: [PV_Mike_NetgearGS110TP](#)

Port: g6
VLAN ID: 500

 **Addresses** 2 >

IPv4: 1 IPv6: 1 MAC: 1

 **VLANs** 1 >

500

主机/客户

通过流量监控和查询发现其他主机和客户端。如果无法将主机识别为属于其他类别之一(交换机、路由器、VoIP设备等),则将其归类为主机/客户端。

 **Discovery**

 **ubuntu**

Host/Client

Name
mDNS: ubuntu

Address
IPv4: 10.250.2.109 (Reachable)
IPv6: 2001:c001:c0de:500:b844:4388:4fb7:4506
MAC: ORICO:f01e34-1fbaa4

Nearest Switch: [PV_Mike_NetgearGS110TP](#)
Port: g3
VLAN ID: 500

 **Addresses** 4 >
IPv4: 1 IPv6: 3 MAC: 1

 **VLANs** 1 >
500

注意：一个MAC以 LocalAdm 开头的地址表示该地址已在本地随机化以防止未经授权的跟踪。

☰ Discovery

 localAdm:227367-a99246

Wi-Fi Client

Address

MAC: [localAdm:227367-a99246](#)

802.11

Channels: 48

Type: --

AP: [localAdm:decbac-51a778](#)

SSID: ngenius&sniffer

Security: WPA2-E

设备名称和授权

为设备分配名称和授权

发现应用程序提供了分配名称和授权给任何发现的具有 MAC 地址的设备的选项。

分配用户名和/或授权状态不会改变实际设备上的任何信息，只会改变显示在 LRAT 上的已指定名称和授权的设备信息。

对于具有多个地址的设备，您只需为一个 MAC 地址分配名称和/或授权。名称和授权保存在内部 `authname.txt` 文件中，并在设备关闭和打开时保持设置。

此功能可让您快速识别已知设备并根据以下状态对其进行分类：

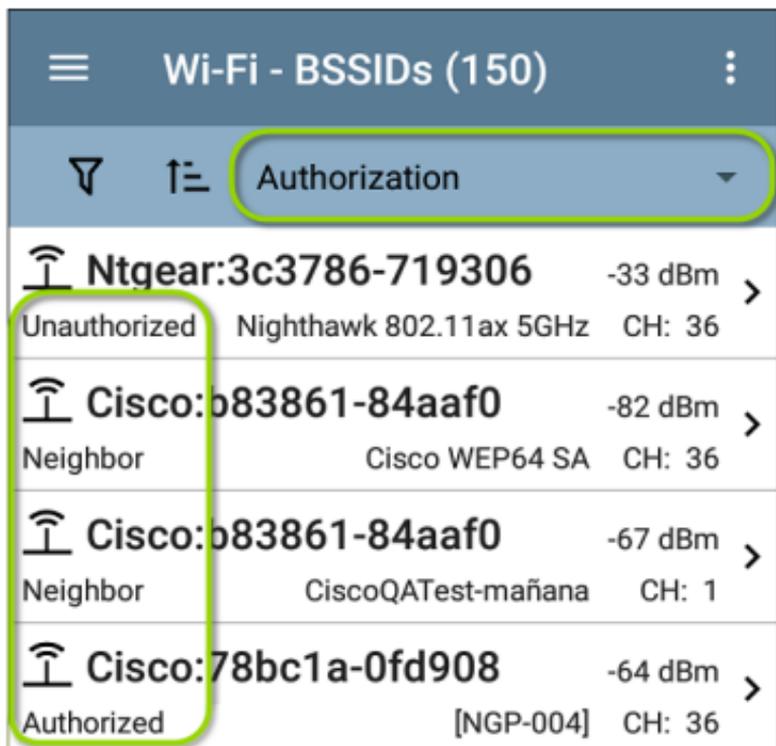
- 已授权：对于经批准可在您的网络中使用的设备。
- 邻居：适用于邻近组织拥有和控制的设备。
- 已标记：使特定设备可见。
- 未知：对于尚未识别或分类的设备。

- 未授权:对于不应接入网络且可能存在安全风险的设备。
- 未指定:默认未分配授权状态。

虽然授权状态的设计具有这些预期含义,但您可以根据自己的目的随意使用它们。

设置后,自定义用户名将显示在其他 NetAlly 显示设备信息的应用程序中。授权显示在发现应用程序中。

您可以在发现应用程序中按分配的授权进行排序和筛选。当列表按授权排序时(按正常排序顺序),具有最高关注授权的设备将显示在顶部。下图显示了按此方式排序的列表页面:

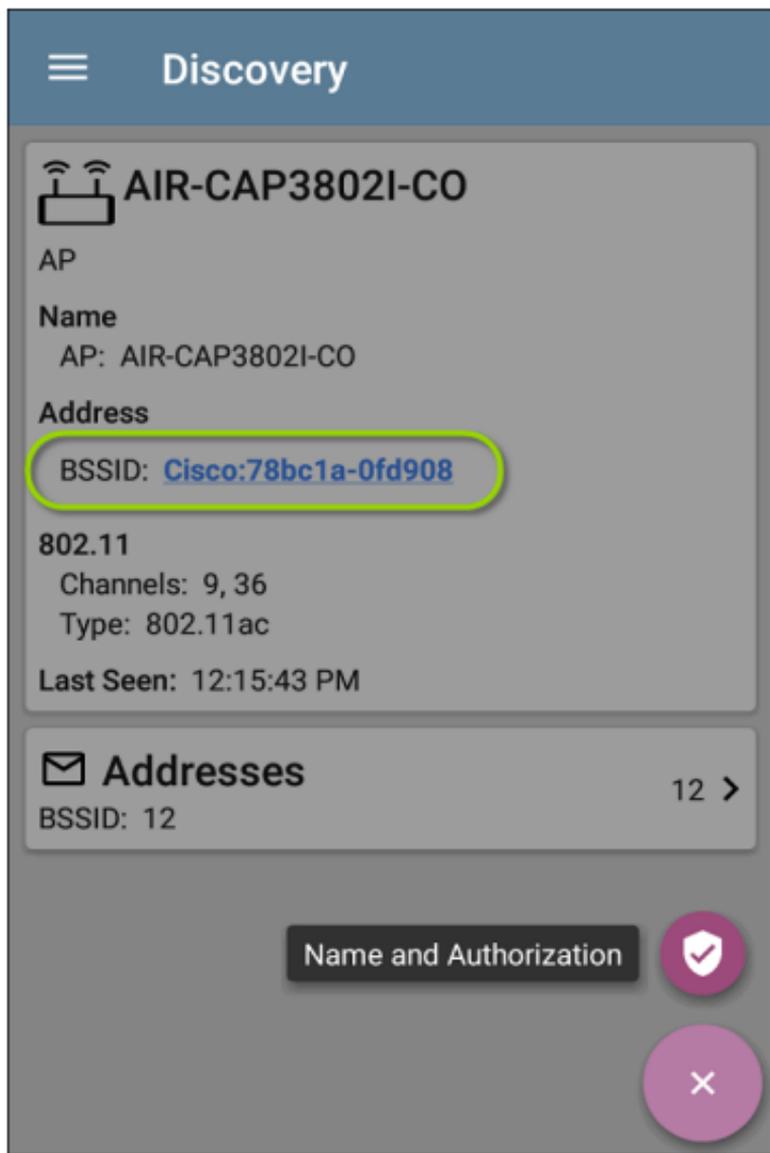


申请名称和/或授权

访问名称和授权功能，该功能在浮动操作菜单  上，该菜单位于 [发现详情页面](#)。

注：当将授权应用于具有多个 MAC 地址的设备，授权状态仅适用于显示在“详细信息”页面上的 MAC 地址，如本节所示。

1. 点击 [FAB](#)，它在发现页面上，适用于有被发现的 MAC 的设备。



上面的例子显示了 Discovery 应用程序中 AP 的详细信息页面。

2. 选择 名称和授权 打开对话框。

Name and Authorization

MAC Address: Cisco:78bc1a-0fd908

User Name: Conference Room AP

Authorization

Authorized

Neighbor

Flagged

Unknown

Unauthorized

Unspecified

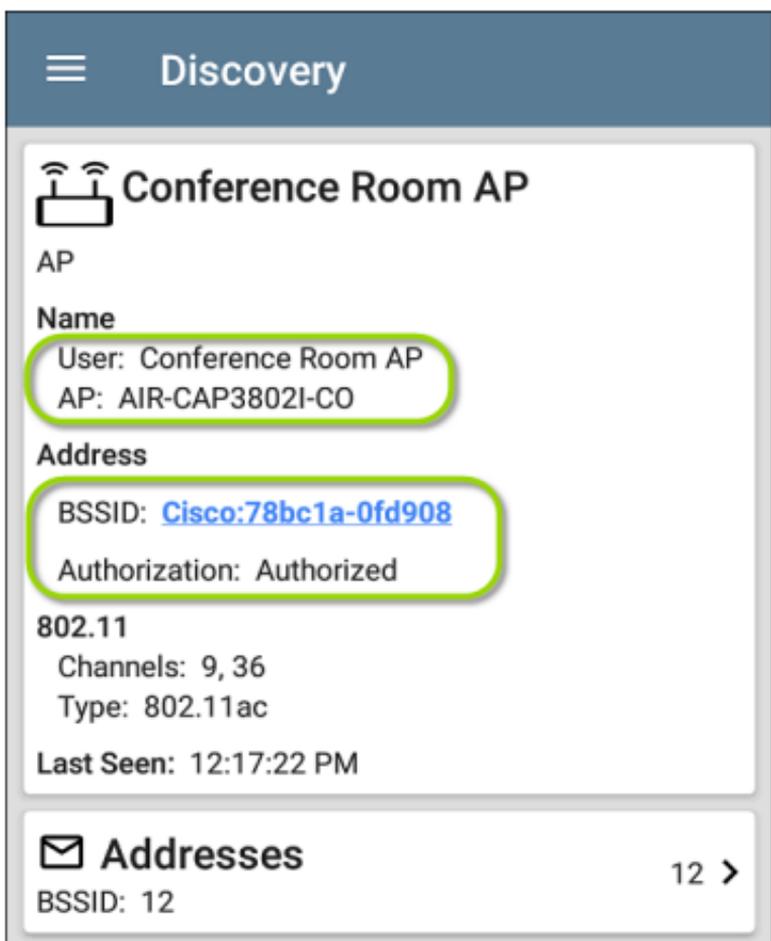
CANCEL OK

3. 在名称和授权对话框中，点击用户名如果需要，可以在字段中输入自定义名称。在上图中，用户输入了名称“Conference Room AP”。

注意：可以选择输入用户名或选择授权。您不必同时执行这两项操作。

4. 选择单选按钮以按需要分配 授权状态。
5. 点击**OK**以应用

一旦应用,用户名和授权将显示在发现详细信息信息屏幕上。



The screenshot shows a mobile application interface titled "Discovery". At the top left is a hamburger menu icon. Below the title, there is a card for a device named "Conference Room AP", represented by a Wi-Fi router icon. The card contains the following information:

- AP**
- Name**
 - User: Conference Room AP
 - AP: AIR-CAP3802I-CO
- Address**
 - BSSID: [Cisco:78bc1a-0fd908](#)
 - Authorization: Authorized
- 802.11**
 - Channels: 9, 36
 - Type: 802.11ac
- Last Seen: 12:17:22 PM

At the bottom of the card, there is a section titled "Addresses" with an envelope icon, showing "BSSID: 12" and a count of "12" with a right-pointing arrow.

注:如果为在同一设备上不同的MAC地址分配了不同的授权状态,最受关注的授权出现在设备的详细信息页面上。

更改或删除用户名或授权

再次打开名称和授权对话框，针对同样的 *MAC地址* 来重新分配或删除已分配的用户名或授权。如果名称或授权几分钟后没有按预期更新，则您可能已将它们分配给同一设备的多个地址。

要查看设备的所有已分配授权，请打开设备的发现页面来查看设备地址 页面。然后，按授权排序。

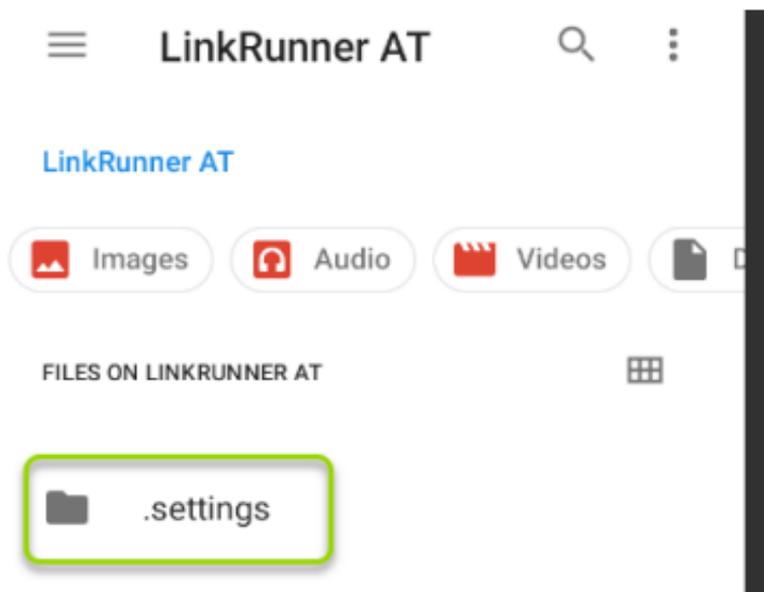
Addresses (14)		
Authorization		
 Cisco:b83861-84aaf3	CH: 36	>
Flagged	Cisco WEP128 OA	
 Cisco:b83861-84aaf1	CH: 1	>
Neighbor	Cisco WEP64 OA	
 Cisco:b83861-84aafc	CH: 1	>
Authorized	Cisco WEP128 OA	
 Cisco:b83861-84aaf0	CH: 1	>
Neighbor	Cisco WEP64 OA	

要将设备的用户名和/或授权重置为未分配的默认值，请打开名称和授权对话框，清除

用户名字段并将其留空，然后选择 **未指定** 授权。然后，点击 **OK**。

修改或导入 **authname.txt**

自定义名称和授权存储在 **authname.txt** 文件，该文件在 LRAT 的内部存储 **.settings** 文件夹中，可从 **文件** 应用程序进入。



如果需要，您可以在 LRAT 单元手动编辑这个文件，或者您可以在 PC 上创建一个新的 **authname.txt** 文件并将其导入到单元的同文件夹位置。（您也可以从 **Link-Live** 推送 **authname.txt** 文件到您的测试单元。）

注意:您的LRAT 3000-4000可以解析 `authname.txt` 文件中的 ? 通配符(尽管不允许使用 * 通配符)。

您的设备上的默认 `authname.txt` 文件包含有关如何格式化您的名称和授权条目的说明:

- 每行定义一个 MAC, 使用以下格式:
MAC, [授权] [, 自定义名称]
- 授权不区分大小写, 可以是以下字符串之一:
 - 已授权
 - 邻居
 - 已标记
 - 未授权
 - 未知
 - 未指定(或空白)
- 您可以用问号 ? 替换 MAC 数位, 以匹配该数字的任意值。

示例 `authname` 文件可能如下所示:

```
00c017-330ea3, Authorized, iPerf3-server
bc:e9:2f:41:df:b4, Authorized, HP-Deskjet
b827eb-???????, Unauthorized, Raspberry-PI
7c:10:c9:??:??:??, Neighbor, ASUS-AP
```

要编辑 authname.txt 文件 LRAT, 第三方应用程序, 如 QuickEdit 文本编辑器, 可从 [NetAllyApp Store](#)  获取。

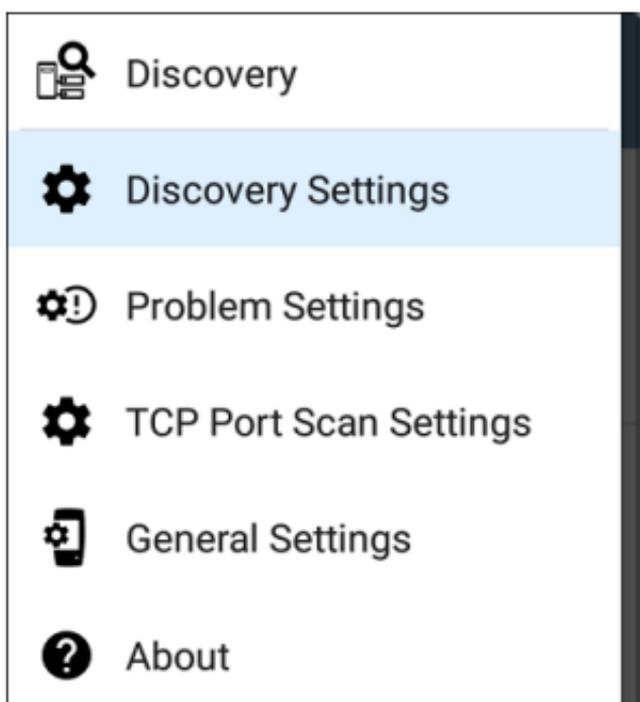
有关导入文件的帮助, 请参阅[管理文件](#) 主题。

注意: 导入并覆盖 authname.txt 文件后, NetAlly 建议在 Discovery 应用程序中 [更新发现](#) 或重新启动您的设备。

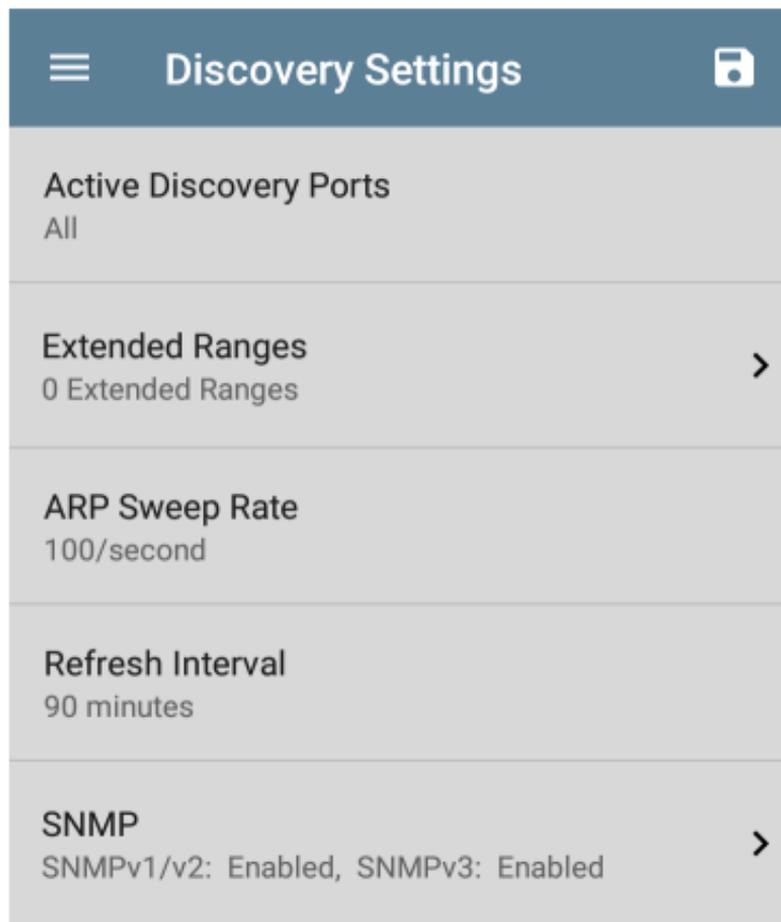
发现设置

发现配置包括 SNMP 设置、社区字符串及其使用顺序、凭据集、端口、扩展范围和处理间隔。

通过滑出左侧导航抽屉或点击菜单图标访问 Discovery 设置屏幕 , 并选择发现设置。



(触摸此处可跳至 [问题设置](#), [TCP 端口扫描](#), 或回到 [常规设置](#).)



要调整发现设置：

1. 在发现设置屏幕，根据需要触摸本主题中描述的每个字段，以选择或输入所需的配置元素。
2. 完成配置后，点击返回按钮回到主要发现列表屏幕。

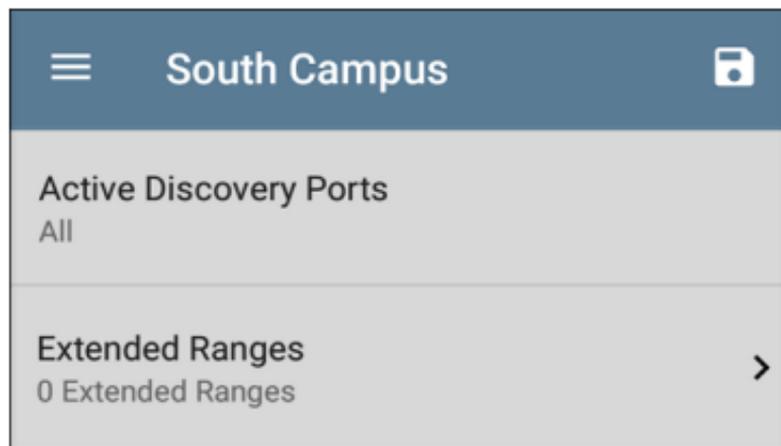
3. 然后，刷新发现从动作溢出菜单应用新配置。

您可以通过触摸保存按钮加载、保存、导入和导出配置的 Discovery 设置在这个屏幕上。

- 加载打开之前保存的 Discovery 配置。
- 另存为使用现有名称或新的自定义名称保存当前配置。
- 导入：导入以前导出的设置文件。
- 导出选定项或全部导出：创建当前设置的导出文件，并将其保存到内部或连接的外部存储。

参考[管理测试应用程序设置](#)更多说明。

保存配置后，您输入的自定义名称将出现在“发现设置”页面的标题中。在下图中，用户保存了一个名为“南校区”的自定义配置，该配置替换了“发现设置”屏幕标题。



主动发现端口

轻触 **Active Discovery Ports** 以选择 **Discovery** 用于收集数据的端口。(默认情况下,发现使用所有的端口。取消选中它们以限制使用的端口。) 如果活动网络链接可用,则发现仅通过启用的端口运行。请参阅[选择端口](#)获取对不同端口的解释。

扩展范围

Extended Ranges 页面允许您输入要在其上运行发现过程的非本地子网的地址。

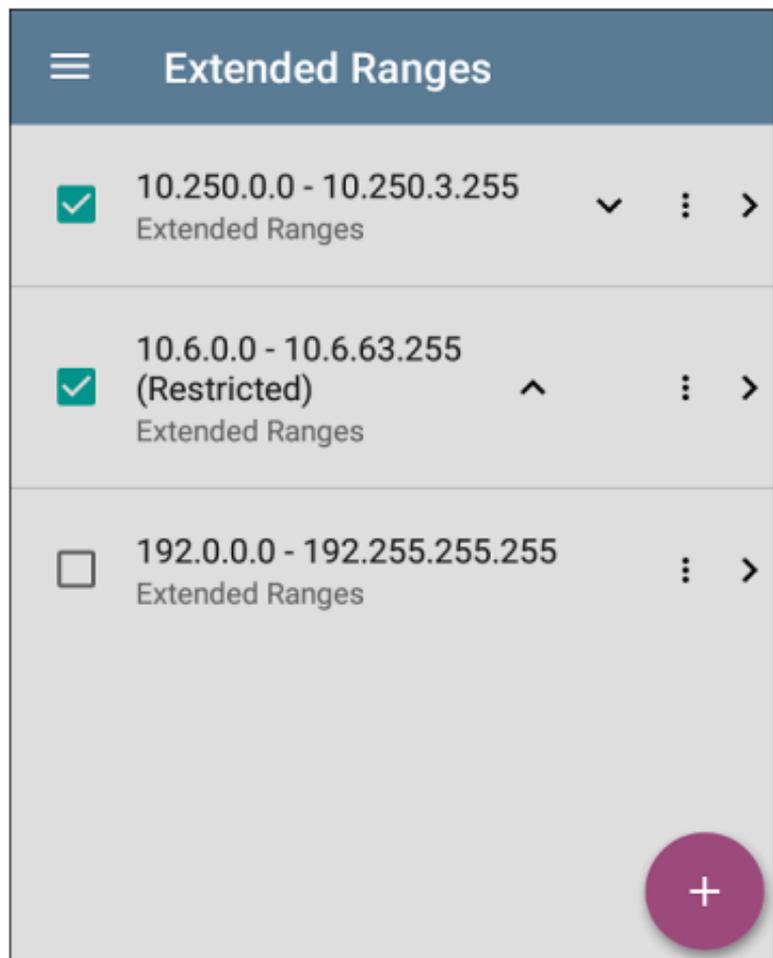
Discovery 会扫描所有已启用的设备扩展范围,无论是直接连接还是离线。这个 **LRAT** 对未直接连接的子网执行 **Ping** 扫描,对连接的子网执行 **ARP** 扫描。

当 SNMP 代理位于与主机(PC 和服务 器)子网分开的子网上时,必须为发现配置其他网络:

- 要发现的远程子网的网络地址,即主机(PC 和服务 器)网络。
- 远程子网中交换机和路由器 SNMP 代理的网络地址,例如一个管理子网。

配置两个 SNMP 凭证集和扩展范围以确保 LRAT 无论您的网络端口连接如何,始终发现管理子网。

轻触该字段以打开扩展范围列表屏幕。



- 选中或取消选中这些框以在当前发现配置中包括或排除扩展范围。未选中的扩展范围不会影响当前配置中的默认发现行为,但它们可能用于其他发现配置(如社区字符串和凭据)。
- 触摸任何扩展范围的行以编辑其地址和子网。

- 触摸 FAB  添加新的扩展范围。

☰ **Range**

Active
Subnet will be included in Discovery

Address
10.250.0.0

Subnet Mask
255.255.252.0 /22

活动子网与受限子网

对于每个配置的扩展范围，您可以点击切换按钮从**Active to**受限的。发现是在活动范围上执行的。将范围设置为受限的禁用该网络或子网上的发现过程，这意味着LRAT不会与限制范围内的设备进行通信。

10.6.0.0 - 10.6.63.255
(Restricted)

Extended Ranges

^ ⋮ >

- 受限范围优先, 无论它们在“扩展范围”屏幕上的列出顺序如何。
- 您可以限制配置的活动扩展范围的一部分。
- 您还可以限制单个设备, 无论它是否属于活动范围的一部分。要输入您不想被发现的单个设备, 请在地址字段中输入其 IP 地址, 并将子网掩码字段设置为 255.255.255.255。

地址

轻触地址字段以输入或选择 IP 地址范围。

点击下拉菜单以选择以前发现的子网。地址字段会自动填充您的选择。

子网掩码

触摸此字段以选择子网掩码。如果您选择已发现的子网, 子网掩码也会预先填充。

ARP扫描率

触摸 ARP 扫描速率字段以选择每秒 5 到 100 个 ARP 请求之间的速率。

此设置可以防止LRAT关闭检测到太多 ARP 发送的端口。

刷新间隔

此设置控制发现进程运行之间的时间。默认情况下,发现每 90 分钟运行一次。触摸刷新间隔字段以选择不同的时间间隔,最多 8 小时。

这个手动选项关闭常规自动发现,并且只有在您选择时才会刷新进程刷新发现从主发现列表屏幕。

SNMP 配置

SNMP 管理设备的 MIB(管理信息库)包含设备配置、接口配置和统计信息、SNMP 表(如主机资源和路由表)和 VLAN 详细信息等信息。通过探索过程,LRAT 询问 MIB 以确定设备类型、端口、连接的子网和其他数据。

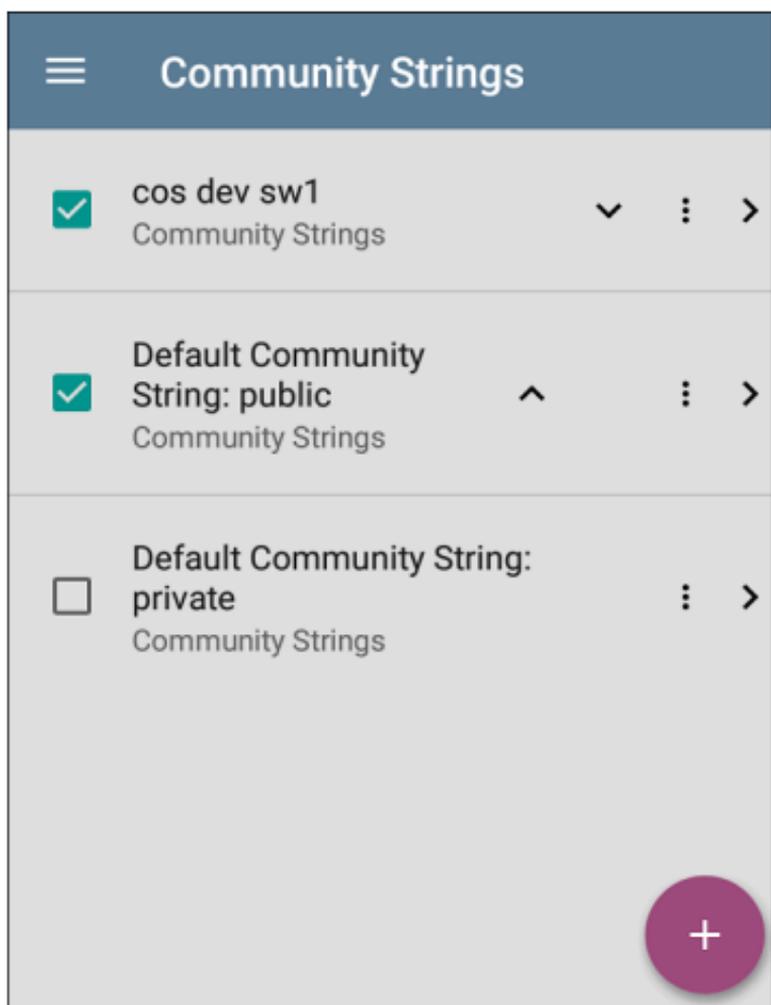
需要 SNMP 凭据才能与互连设备(例如交换机和路由器)上的 SNMP 代理进行通信。发现设置允许您输入 SNMP 社区字符串和凭据设置 LRAT 用于与这些设备进行通信。

SNMPv1/v2

触摸切换按钮以启用或禁用 SNMPv1 和 v2 查询。默认情况下启用此设置并使用在下一个设置中配置的社区字符串。

字符串

轻触此字段可打开社区字符串列表屏幕并添加、编辑或删除社区字符串。



这个LRAT按照此屏幕上显示的顺序使用选中的字符串。如果使用一个字符串未收到来自被查询设备的响应，则发送下一个字符串。

注意:此屏幕和 Discovery 设置中的其他屏幕的操作与[自动测试配置文件组屏幕](#)。

在社区字符串屏幕上,您可以执行以下操作:

- 选中或取消选中这些框以在当前 Discovery 配置中包含或排除使用的字符串。
- 点击向上和向下箭头  改变顺序 LRAT 使用字符串查询设备。
- 触摸操作溢出图标  到复制或删除一个字符串

警告:删除字符串时,会将其从所有已保存的 Discovery 配置中删除。要从当前发现配置使用的字符串中删除字符串,只需取消选中它。

- 轻触 FAB  添加新的社区字符串。
- 触摸任何社区字符串的行以编辑字符串及其说明。

提示:为了最大限度地减少发现时间,请取消选中或删除所有未使用的社区字符串,因为每个失败的查询都会延长发现时间。您还可以按照最常用的顺序排列社区字符串。

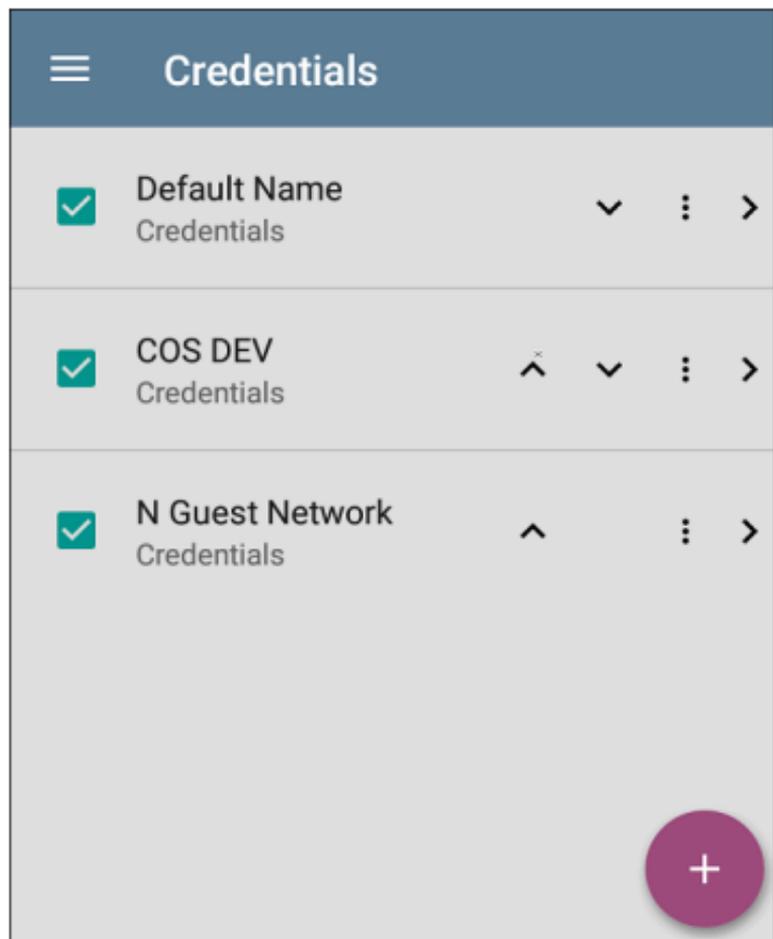
SNMPv3

轻触切换按钮以启用或禁用 SNMPv3 查询。默认情况下启用此设置并使用在下一个设置中配置的凭据。

注：如果启用此设置，但未配置 SNMPv3 凭据，则 LRAT 发现所有 SNMPv3 代理的引擎 ID。这是发现设备是否支持 SNMPv3 的好方法。

证书

轻触此字段可打开凭据列表屏幕。



此屏幕界面的工作方式类似于上面的社区字符串屏幕。LRAT按所示顺序使用凭据。

- 选中或取消选中复选框以在当前发现配置中包含或排除一组凭据。
- 触摸一行以编辑其凭据。
- 触摸 FAB  添加新凭据。



Credential Sets	
Name	Default Name
Username	
Authorization Type	None
Authorization Password	
Privacy Type	None
Privacy Password	

在凭据集屏幕上，点击每个字段以选择或输入所需的凭据。

名称

轻触名称字段以输入凭据集的自定义名称。

用户名

轻触以输入 SNMPv3 用户名。

授权类型和密码

Discovery 支持两种 SNMPv3 授权类型：HMAC-SHA 和 HMAC-MD5。如果需要授权，请输入适当的密码。

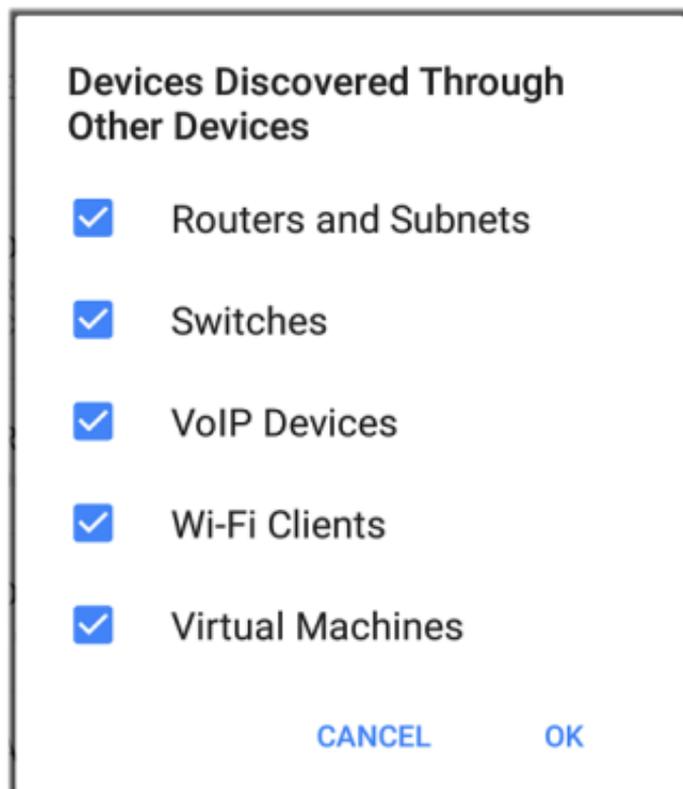
SNMP 查询延迟

此功能控制您的 LRAT 在对可能导致 SNMP 代理中 CPU 峰值的关键表(包括 ARP 缓存、IP 地址表、路由表和 FDB 表)的 SNMP 查询之间等待。

默认 SNMP 查询延迟为无延迟。查询关键大表时，LRAT 收到响应后立即请求更多数据。如果需要，您可以选择 1 或 5 秒的延迟。

通过其他设备发现的设备

默认 LRAT 从其他设备的 SNMP 表中发现设备。如果您不希望 Discovery 从此处列出的设备类型的 SNMP 表中自动查找设备，您可以取消选中它们的复选框。



路由器和子网

启用路由器和子网复选框后，任何发现的路由器都包含在发现结果中。此外，如果 Discovery 对已发现的路由器具有 SNMP 访问权限，则会读取其路由表，并将下一跳路由器添加到 Discovery 列表中。如果路由表中有任何本地子网可用，它们也会添加到子网列表中。此过程将继续，直到为添加的路由器尝试了所有可用的 SNMP 凭据。

注意:发现不会扫描每个发现的子网;发现的子网只会添加到子网列表中。要在特定子网中执行发现,请参阅扩展范围以上。

如果另一个站点有您想要使用此过程发现的路由器,但没有来自该站点的本地下一跳链接,您可以将该站点的其中一个路由器添加到发现中。然后,该过程从该路由器运行,并在该站点上查找路由器。将路由器的子网或仅路由器的 IP 地址(掩码为 /32)添加到扩展范围。

交换机

启用交换机复选框后,发现会将它在其他设备的 SNMP 邻居表中找到的任何交换机添加到发现列表。

例如,当LRAT正在读取一台交换机的 CDP 和 LLDP 缓存,它包含其他交换机。如果启用此选项,则LRAT添加那些其他开关,即使它们不在发现范围内。

注意:要发现另一个站点的交换机,请将该站点的交换机之一添加到 Discovery Extended Ranges。

VoIP 设备

启用 VoIP 设备复选框后，发现会添加它在其他设备的 SNMP 表中找到的任何 VoIP 设备，而不管子网如何。这些通常可以在交换机的 LLDP-MED 表中找到。启用 Switches 选项提供了找到所有 VoIP 设备的最佳机会。

虚机

启用虚拟机复选框后，发现会添加它在其他设备的 SNMP 表中找到的任何虚拟机。这些通常可以在 ESX 主机中找到。SNMP 表。将 ESX 主机的子网添加到扩展范围有助于查找虚拟机。

设备健康间隔

Discovery 会自动运行一组网络运行状况测试来搜索网络问题，例如所有已发现接口和设备资源上的高利用率、丢弃或错误。

选定的时间刷新闻隔是每次运行设备运行状况测试之间的最短时间。触摸该字段以禁用设备运行状况测试或将间隔从默认的 10 分钟更改为 30 或 60 分钟。

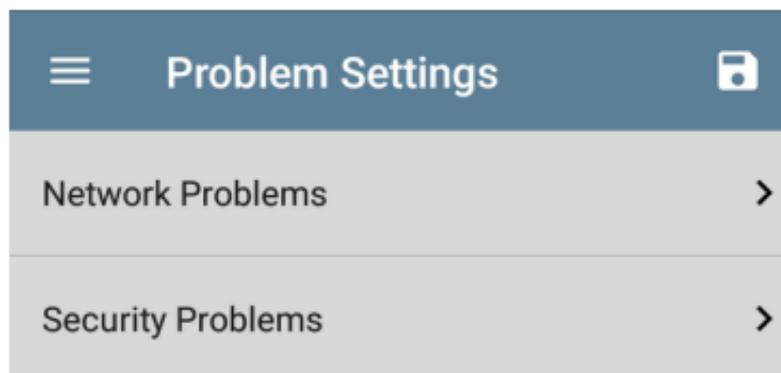
禁用设备健康测试会影响发现可以检测到的问题类型。

也可以看看 [电缆测试设置](#).

问题设置

问题设置确定检测和显示哪些问题 发现应用程序 以及已启用问题的阈值, 例如数据包丢弃和利用率。

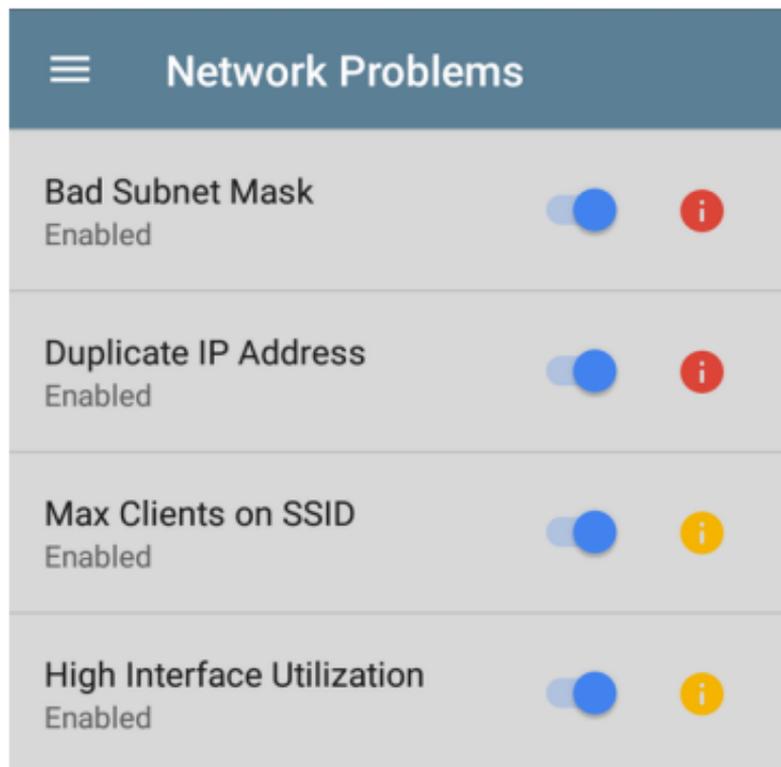
通过滑出左侧导航抽屉或点击菜单图标访问问题设置屏幕  在 Discovery 应用程序中, 然后选择问题设置。



问题被归类为有线或 Wi-Fi。

您可以通过触摸保存按钮来保存、加载、导入和导出配置的问题设置  在这个屏幕上。看 [管理测试应用程序设置](#) 更多说明。

点击每个行以启用或禁用问题类型并在适用的情况下设置阈值。



默认情况下启用所有问题类型。点击右侧的切换按钮以禁用每个按钮。

- 轻触红色 ，黄色的 ，或蓝色  每个问题右侧的信息图标以阅读详细说明和建议的操作。
- **红色** 图标表示故障条件。
- **黄色** 指示警告条件。
- **蓝色** 图标只是提供信息。

轻触红色 ，黄色的 ，或蓝色  每个问题右侧的信息图标以阅读详细说明和建议

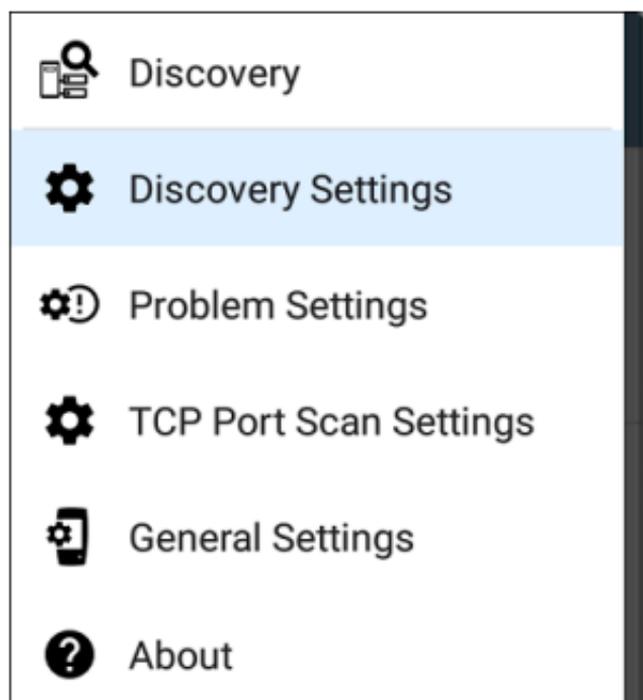
的操作。**红色**图标表示故障条件和**黄色**指示警告条件。**蓝色**图标只是提供信息。

完成配置后，点击返回按钮返回主发现屏幕。

TCP 端口扫描设置

TCP 端口扫描功能检查当前设备上的开放端口。要运行扫描，请点击“发现详细信息”屏幕上的 FAB，然后点击“TCP 端口扫描”。这个 LRAT 同时扫描多个端口并报告开放端口的编号。

通过滑出左侧导航抽屉或点击菜单图标访问 TCP 端口扫描设置  在里面 [发现应用](#)。



选择 TCP 端口扫描设置。

TCP Port Scan Settings	
Interface	Any Port
Scan List	1-2049, 3268-3389, 3535, 5000-6005, 8008-8443
Timeout Threshold	1 s

接口: 点击该字段可选择运行端口扫描的端口。(有关不同端口的说明, 请参阅选择端口。)

扫描列表: 此设置包含在端口扫描期间测试的端口号。点击该字段以输入不同的端口号或范围, 以逗号分隔。

超时阈值: 这个阈值控制了多长时间LRAT等待来自每个端口的响应。一旦扫描列表中的所有端口都有足够的响应时间, 扫描就会结束, 并且 TCP 端口扫描结果屏幕会列出在阈值内响应的端口。

参考[TCP 端口扫描结果卡和屏幕](#)。



路径分析应用

路径分析追踪连接点, 包括中间路由器和交换机之间 LRAT 3000-4000 和一个目标 URL 或 IP 地址。您可以使用路径分析来识别问题, 例如接口过载、设备资源过载和接口错误。它还显示了网络内的设备(和网外设备)如何沿路径相互连接。

所有交换机都是通过 SNMP 查询预先发现的。测量完成后, LRAT 显示到目标设备的跳数。最多可以有 30 跳报道。

注意: 此应用程序仅适用于 LinkRunner AT 4000。

路径分析简介

路径分析结合了第 3 层和第 2 层测量。

这第 3 层测量结合了经典的第 3 层 IP (UDP、ICMP、或 TCP) traceroute 测量, 并查看通过的路径 二层交换机。

第 2 层测量通过向所有发现的交换机发送 SNMP 查询, 在交换机转发表中查找路由器的 MAC 地址, 从而发现路由器跃点之间的交换机。测量完成后, 路径中找到的开关将显示在路由器跃点之间。

当您使用 SNMP 凭据配置 Discovery 应用程序时, 路径分析最有效。参考[在 SNMP 配置中发现设置](#)主题了解如何使用。

路径分析设置

路径分析源设备始终是您的LinkRunner AT 4000。默认目标是 www.google.com。

从另一个应用程序填充路径分析

像其他LRAT测试应用程序，当您从另一个应用程序打开路径分析时，例如[发现](#)，您在上一个应用程序中查看的网络组件的地址已预先填充为路径分析目标。

手动配置路径分析

打开应用程序设置以配置自定义目标并选择接口和协议。要打开，从路径分析应用程序屏幕，触摸设置图标，或打开左侧导航区域并选择路径分析设置。

Path Analysis Settings	
Device Name	10.250.2.166
Interface	Any Port
Protocol	Connect (TCP)
TCP Port	80 (www-http)

在路径分析设置屏幕上，根据需要触摸每个字段以配置您的目标：

设备名称：轻触输入路径目的地的 IP 地址或 DNS 名称。默认为 `www.google.com`。

界面：此设置决定运行路径分析的设备端口。点击该字段来选择一个端口。（请参阅[选择端口](#)了解对不同端口的解释。）

LRAT 必须在所选端口上有活动的网络链接才能运行路径分析。如果选择了任意端口，可用链接按照接口选择对话框中显示的顺序使用。

请参阅[测试和管理端口](#) 获取有关不同端口及其链接方式的解释。

协议: 点击为路径分析选择连接 (TCP)、Ping (ICMP) 或 Echo (UDP/7) 协议。

TCP 端口: 此字段仅在您选择了连接 (TCP) 协议时出现。点击以输入要运行路径分析的端口号。(您可能需要输入特定的端口号, 因为路由可能因端口号而异和/或可能被防火墙阻止。)

运行路径分析

轻触开始按钮开始路径分析。

注意：LRAT必须在应用程序设置中选择的接口(端口)上链接。看[测试和管理端口](#)求助。

 **Path Analysis** START 

 **www.google.com**
21 ms, 34 ms, 32 ms
Device Name: www.google.com
IP Address: 172.217.11.228
Interface: Any Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)
Results
Started: 5:56:45 PM
Status: Destination reached in 8 hops
[UPLOAD TO LINK-LIVE](#)

 **Thomas's LinkRunner 10G - ...** 
Out: Wired Port 100 Mb FDx

 **Layer 2 Path**
No layer 2 devices discovered

 **modem.domain** 
17 ms, 20 ms, 18 ms Hop: 1

与 AutoTest 一样，路径分析结果也显示在卡片上。顶部卡片显示主要测试详细信息，第二张卡片显示源设备的信息(您的 LRAT 3000-

4000), 下面的卡片显示了路径中的第 2 层和第 3 层跃点, 它们是按顺序排列的。

轻触任意 [蓝色链接的姓名或地址](#) 在路径分析结果屏幕中打开 [发现 app](#) 并进一步检查链接的元素。

路径分析结果和来源 LRAT 卡

 **google.com**
10 ms, 6 ms, 11 ms

Device Name: [google.com](#)

IP Address: 172.217.1.206
Interface: Any Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)

Results
Started: 2:26:58 PM
Status: Destination reached in 11 hops

[UPLOAD TO LINK-LIVE](#)

顶部路径分析结果卡在顶部显示路径的目标地址, 然后是 TCP Connect、Ping 或 Echo 测试的三个响应时间。

设备名称: 在设置中输入的目的地的解析 DNS 名称或 IP 地址

IP 地址: 目标目的地的 IPv4 地址

端口:在设置中选择的接口选项

协议:在设置中选择的协议(TCP、Ping 或 Echo)

TCP 端口:用于 TCP 连接协议的端口号。(Ping 或 Echo 协议结果不会出现此字段。)

结果

已开始:路径分析开始的时间

状态:路径分析测试的当前状态,包括任何错误消息

上传到 **LINK-LIVE**:触摸此链接将您的结果上传到 Link-Live 帐户。参考[将路径分析结果上传到 Link-Live](#)稍后在本主题中。

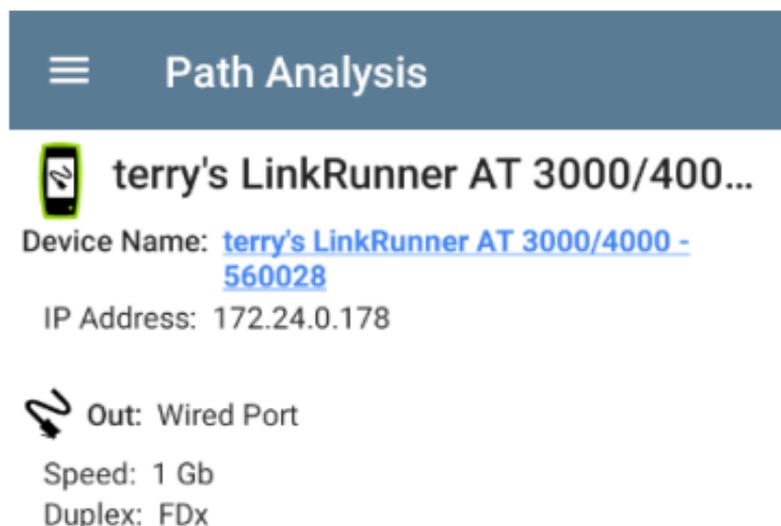
源LRAT 卡



来源 这个LRAT卡显示运行路径分析的端口。

注意:此卡和屏幕仅显示您的自定义名称LRAT如果你有[向 Link-Live 注册它](#)。

触摸卡片以查看更多详细信息。下图显示了有线路径分析中的源 LRAT 卡，其中显示了链路速度和双工。



☰ Path Analysis

 terry's LinkRunner AT 3000/4000...

Device Name: [terry's LinkRunner AT 3000/4000 - 560028](#)

IP Address: 172.24.0.178

 Out: Wired Port

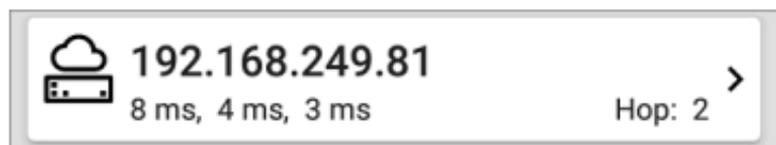
Speed: 1 Gb

Duplex: FDx

(LinkRunner AT 4000 仅有的) 在 LRAT 源卡下，跳跃卡显示确定位于路径中的第 2 层和第 3 层设备。

3层跳

每个第 3 层跃点卡显示设备类型图标、DNS 名称(如果发现)和 IP 地址。



 192.168.249.81

8 ms, 4 ms, 3 ms

Hop: 2 >

在名称(或 IP)下方,每个 Connect (TCP)、Ping (ICMP) 或 Echo (UDP/7) 的响应时间以毫秒为单位显示。右侧是该设备在路径中的路由器跳数。

触摸卡片以查看跃点详细信息屏幕。

 **Path Analysis**

 **192.168.249.81**
8 ms, 4 ms, 3 ms Hop: 2

Router: [192.168.249.81](#)

IP Address: 192.168.249.81

无回复

有时路径分析会显示带有“无回复”的跳卡(如下所示)。此结果意味着该路径部分中的设备未发送 ICMP TTL 超时响应。

Path Analysis		START	⚙️
	No Reply -, -, -	Hop: 5	>
	4.34.62.118 23 ms, 22 ms, 18 ms	Hop: 6	>
	ae-6.pat1.nez.yahoo.com 47 ms, 40 ms, 46 ms	Hop: 7	>
	Split Route 41 ms, 25 ms, 34 ms	Hop: 8	>
	Split Route 38 ms, 45 ms, 31 ms	Hop: 9	>
	Split Route 48 ms, 28 ms, 47 ms	Hop: 10	>
	slb8-1-flk.ne1.yahoo.com 39 ms, 41 ms, 38 ms	Hop: 11	>
	www.yahoo.com 35 ms, 61 ms, 46 ms	Hop: 12	>

拆分路线

Path Analyzes 可能会得到“Split Route”结果 (如上所示), 这意味着同一跳内的两个或三个不同的路由器响应了三个请求。

点击拆分路由卡以查看响应路由器的 DNS 名称和 IP 地址。

☰ Path Analysis



Split Route

41 ms, 25 ms, 34 ms

Hop: 8

Response 1: et-0-0-0.msr1.ne1.yahoo.com

IP Address: 216.115.105.25

Response 2: et-0-0-0.msr2.ne1.yahoo.com

IP Address: 216.115.105.179

Response 3: et-19-1-0.msr2.ne1.yahoo.com

IP Address: 216.115.105.181

三层接口和统计

可以识别和测量第 3 层设备上的接口统计信息，如果 LRAT 具有 SNMP 访问权限。



COS_DEV_SW1

13 ms, 12 ms, 13 ms

Hop: 3 >

In: Gi1/0/47

1 Gb FDx

触摸跳卡以查看界面详细信息和统计信息的摘要(如果可用)。

参考[二层交换机接口和统计](#)

路径分析中的网络问题

Hop 卡还可以显示基于[问题设置](#)在 Discovery 应用程序中，并以相应的颜色显示设备类型图标。

上图中的黄色开关图标表示[警告](#)状态。

☰
Path Analysis



COS_DEV_SW1

13 ms, 12 ms, 13 ms

Hop: 3

Router: [COS_DEV_SW1](#)

IP Address: 192.168.249.82

 **In:** [Gi1/0/47](#)

Speed: 1 Gb

Duplex: FDx

Statistics

Util: 0.3 % Discards: 0.0 % Errors: 0.0 %

点击[蓝色链接](#)开关名称打开一个[发现详情](#)屏幕对于开关，用户可以在其中调查警告的原因。

二层设备

第 2 层设备可以是交换机或 AP。

二层交换机

下图显示了本地广播域中设备的路径分析示例，在路径的第 2 层部分有两个交换机。

☰
Path Analysis
START

Interface: Any Port
 Protocol: Connect (TCP)
 TCP Port: 80 (www-http)

Results
 Started: 3:41:34 PM
 Status: Destination reached in 1 hop

[UPLOAD TO LINK-LIVE](#)

LinkRunner AT 3000/4000 >
 Out: Wired Port 1 Gb FDx

COS_DEV_SW1 >
 In: Gi1/0/13 VLAN: 500 1 Gb FDx
 Out: Gi2/0/24 VLAN: 500 1 Gb FDx

cos-dev-sw18-poe >
 In: Gi0/1 VLAN: 500 1 Gb FDx
 Out: Gi0/7 VLAN: 500 1 Gb FDx

Cetus >
 6 ms, 4 ms, 6 ms Hop: 1

这个LRAT能够识别这些第2层交换机及其接口,因为它具有配置的SNMP访问交换机。

交换卡显示输入和输出接口ID、VLAN ID以及接口的链路速度和双工(如果检测到)。

触摸第2层卡会打开设备的详细信息屏幕。

 **Path Analysis**

 **COS_DEV_SW1**

Switch: [COS_DEV_SW1](#)

IP Address: 10.250.0.1

 In: [Gi1/0/13](#)

Speed: 1 Gb

Duplex: FDx

VLAN: 500

Statistics

Util: <0.1 % Discards: 0.0 % Errors: 0.0 %

 Out: [Gi2/0/24](#)

Speed: 1 Gb

Duplex: FDx

VLAN: 500

Statistics

Util: <0.1 % Discards: 0.0 % Errors: 0.0 %

第 2 层详细信息屏幕在顶部显示设备名称和 IP 地址。

注意:上图中的黄色开关图标表示警告状态。参考[路径分析中的网络问题](#)稍后在本主题中。

二层交换机接口和统计

路径分析中的第 2 层交换机详细信息屏幕显示接口统计信息的摘要(如下所述)。要查看这些接口的所有可用信息,请点击它们的蓝色链接以打开一个[接口详情](#)Discovery 应用程序中的屏幕。

可以识别和测量第 2 层交换机上的接口统计信息,如果 LRAT 具有 SNMP 访问权限。

进/出:表示接口类型和名称。接口名称通常包含交换机连接到网络的物理端口号。

使用率:正在使用的总接口容量的百分比

丢弃:已被丢弃的总数据包的百分比

错误:包含错误的数据包百分比

未发现第 2 层设备



Layer 2 Path

No layer 2 devices discovered

在某些情况下，LRAT不会在第 3 层设备之间发现第 2 层设备。可能没有任何第 2 层设备，或LRAT可能无法通过 SNMP 访问这些交换机。

第 2 层卡也可能会显示“未找到交换机”的结果，这表明 Discovery 未找到任何具有 SNMP 访问权限的交换机，以确定这些交换机是否在路径中。如果这是意外结果，请检查并验证您的 [SNMP 配置](#) 和 [扩展范围](#) 在 Discovery 应用程序设置中。

将路径分析结果上传到 Link-Live

轻触上传到 **LINK-LIVE** 顶部卡片上的链接打开 [Link-Live](#) 路径分析结果共享屏幕：

Link-Live

by NetAlly

Path Analysis Name

20190419_131047

Comment

Conference Room B

Job Comment

Union Hall

SAVE TO ANALYSIS FILES

路径分析结果上传到分析页面  在 Link-Live 上。



反射器应用

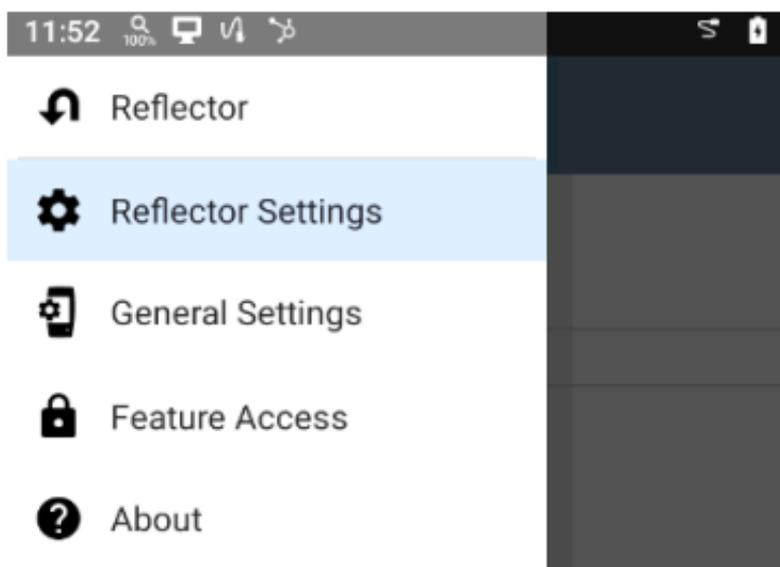
反射器应用能将您的 LinkRunner AT 3000/4000 转变为性能测试反射器。

您可以将反射器应用与使用性能或LANBERT应用的其他NetAlly测试设备配合使用。它还可以用作通用的数据包反射器。您的设备接收来自其他设备的数据包；将源和目标的MAC地址和IP地址交换；然后将数据包发送回该设备。发送设备可以比较发送到反射器的数据包数量与从反射器接收到的数据包数量。该应用程序可用于网络端点的部署前测试，并确保网络性能能够支持特定应用程序。

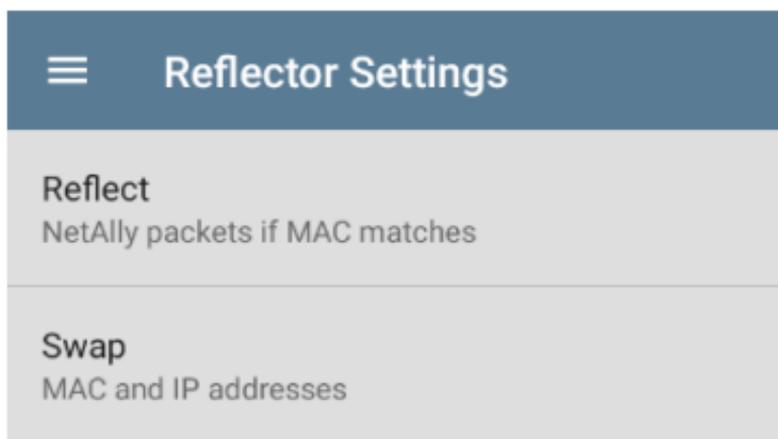
反射器设置

要选择基本的反射器设置：

1. 从反射器的主屏幕上，点击导航菜单图标  或从左侧滑动栏向右滑动以显示导航菜单。



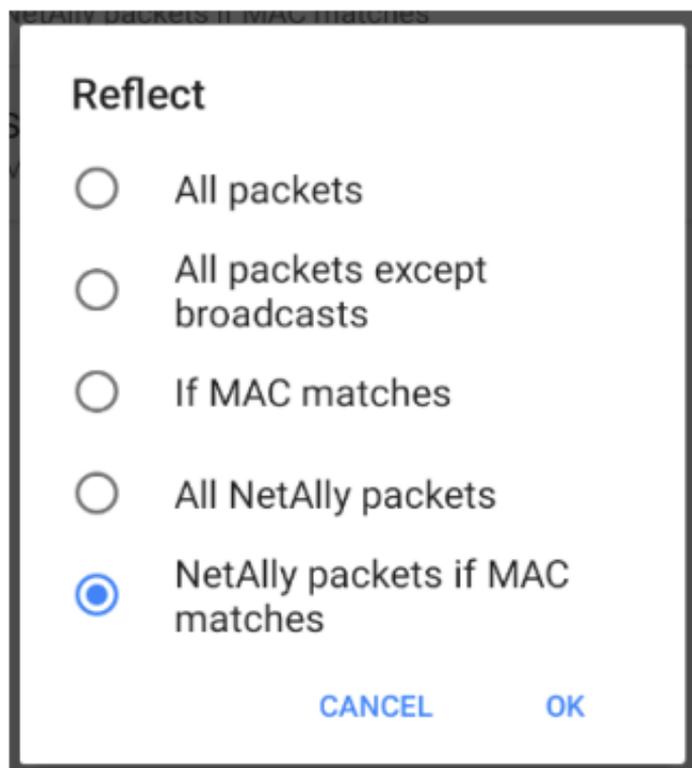
2. 点击 **反射器设置** 以显示设置选项。



3. 根据需要，点击下面描述的每个字段来配置反射器。更改的设置将自动应用。配置完成后，点击返回按钮  以返回到反射器的主屏幕。

反射

点击此字段以选择要反射的数据包：

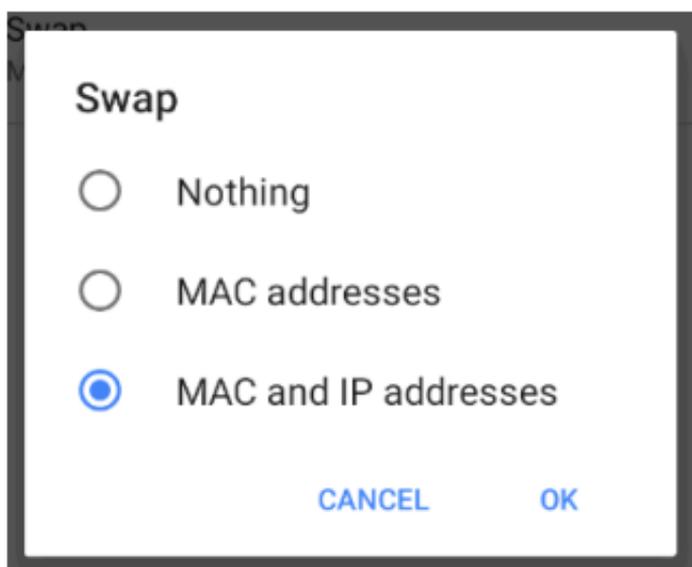


- 一般来说，NetAlly推荐在MAC匹配的情况下，选择 **NetAlly数据包** 的默认值，以避免在您的网络上出现任何不必要的流量。
- 如果您将反射器与运行性能测试应用的NetAlly测试设备一起使用，使用反射的默认值，**当MAC匹配时，即为NetAlly数据包**，并设置交换的默认值为 **MAC地址和IP地址**。

- 如果您将反射器与LANBERT应用的NetAlly测试设备一起使用，设置反射值为**除了广播以外的所有数据包**，并设置交换的值为**MAC地址**。

交换

点击此字段以选择要交换选项：



- 一般来说，NetAlly 推荐设置为默认值，以避免在您的网络上出现任何不必要的流量。
- 如果您将反射器与运行性能测试应用的NetAlly 测试设备一起使用，使用交换的默认值，即**MAC地址和IP地址**，并并使

用 Reflect 的默认值，当 **MAC 匹配** 时，即为 **NetAlly 数据包**。

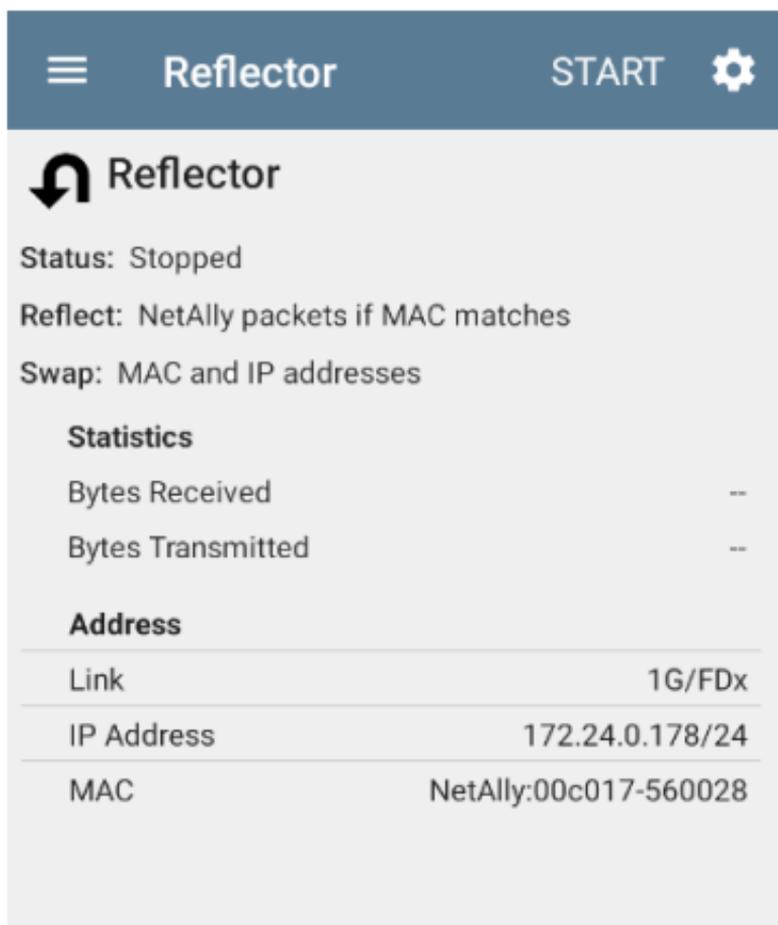
- 如果您将反射器与 LANBERT 应用的 NetAlly 测试设备一起使用，设置交换值为 **MAC 地址**，并设置反射值为 **除了广播以外的所有数据包**。

运行反射器

在您根据需要调整了反射器的设置，设置了所需的反射和交换设置之后，您可以将您的 LinkRunner AT 3000/4000 作为反射器运行。

1. 要打开反射器的主屏幕，只需在 LinkRunner AT 3000/4000 主页上点击 Reflector 图标即可。
2. 确保您的 LinkRunner AT 3000/4000 通过 [有线测试端口](#) (顶部的 RJ-45 或光纤端口) 连接到活动网络。
3. 运行一个 [有线自动测试配置文件](#)，以成功建立端口上的连接。
4. 点击 [开始](#) 以启动反射器测试。该状态说明测试正在运行。

注意：LinkRunner AT 3000/4000 的 IP 地址显示在屏幕底部。请记录该地址以设置发起测试的主设备。



Reflector

Status: Stopped

Reflect: NetAlly packets if MAC matches

Swap: MAC and IP addresses

Statistics

Bytes Received --

Bytes Transmitted --

Address

Link	1G/FDx
IP Address	172.24.0.178/24
MAC	NetAlly:00c017-560028

5. 请按照设备的说明设置发送数据包的主设备，然后开始测试。
 - 在运行过程中，反射器屏幕会显示接收和反射的字节数。
 - 只要测试正在运行，您的 LinkRunner AT 3000/4000 会保持开启。

- 如果从反射器应用的主屏幕导航离开，测试将停止。只要两个设备仍在运行，您可以恢复测试。
6. 当您收集到足够的信息后，点击 **停止** 按钮以停止反射器应用程序。屏幕上将显示接收和发送的字节数。

Reflector		START
 Reflector		
Status: Running		
Reflect: NetAlly packets if MAC matches		
Swap: MAC and IP addresses		
Statistics		
Bytes Received	9,224,813	
Bytes Transmitted	9,134,525	
Address		
Link	1G/FDx	
IP Address	172.24.0.178/24	
MAC	NetAlly:00c017-560028	

请查阅主设备的用户文档，以获取有关查看结果的信息。



iPerf 测试应用程序

iPerf 是一种标准化的网络性能工具，用于测量 UDP 或 TCP 吞吐量和丢失。

iPerf 应用程序运行 iPerf3 性能测试到 NetAlly 测试附件或 iPerf 服务器端点。

注意：此应用程序仅适用于 LinkRunner AT 4000。



The NetAlly测试附件运行网络连接测试, 将结果上传到[Link-Live 云服务](#), 并作为 iPerf 服务器端点, 用于由其他人运行的 iPerf 测试NetAlly手持测试仪。

了解更多关于测试附件的信息

[NetAlly.com/products/TestAccessory](https://www.netally.com/products/TestAccessory).

如果您使用安装在 PC 或其他设备上的 iPerf 服务器作为端点, 则需要 iPerf 版本 3 才能运行LRATiPerf测试。您可以从以下网址下载 iPerf 服务器软件<https://iperf.fr>.

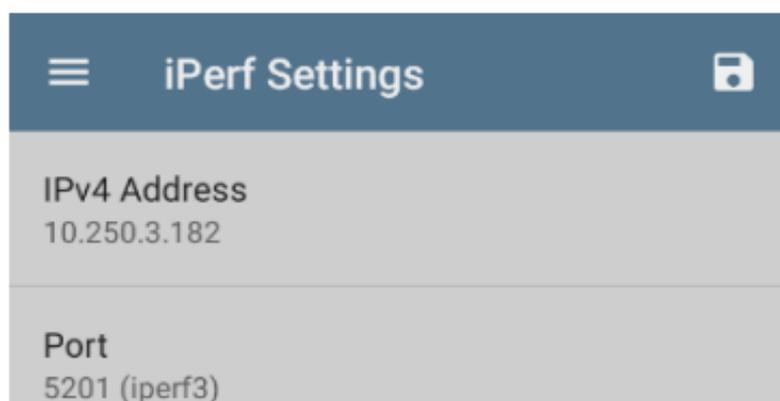
iPerf 设置

要运行 iPerf 测试，您必须配置您的 LRAT 单元与您的 iPerf 端点进行通信。您可以手动输入 iPerf 服务器地址，或选择一个 NetAlly 在 iPerf 设置中测试附件的地址。

保存自定义 iPerf 设置

iPerf 应用程序允许您稍后将用于运行 iPerf 测试的设置配置保存到同一端点。

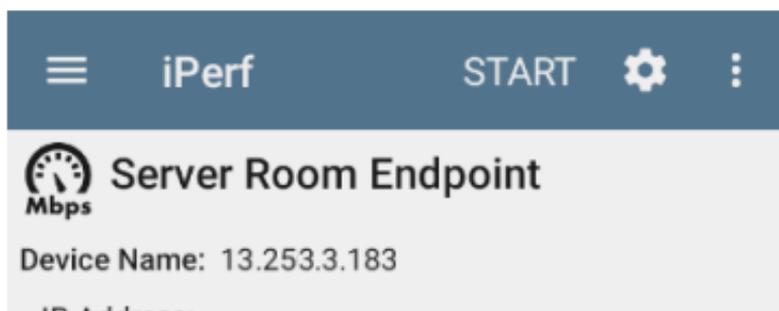
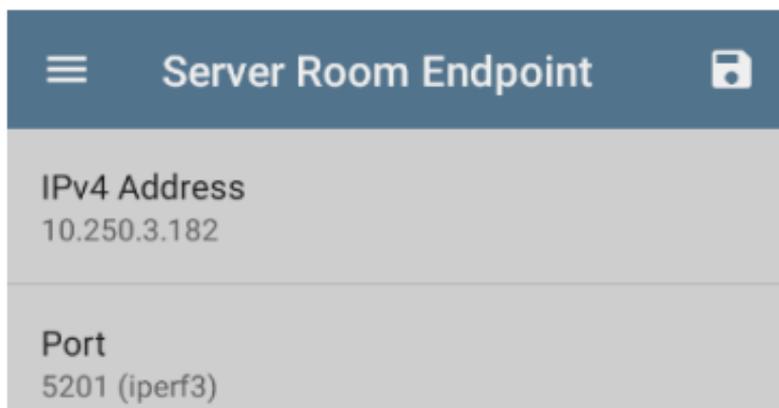
iPerf 应用程序允许您保存设置配置，以便稍后在同一端点运行 iPerf 测试。



触摸保存图标  加载、保存、导入和导出配置的设置。参考 [保存应用程序设置配置](#) 更多说明。

保存设置配置后，您输入的自定义名称会出现在 iPerf 设置和结果屏幕的顶部。在此处

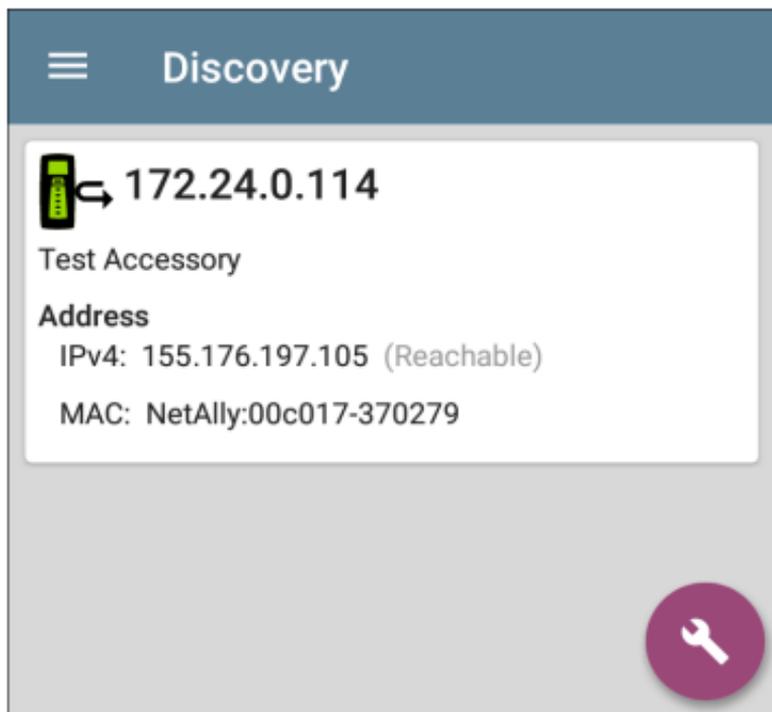
的示例图像中，用户保存了一个名为“服务器机房端点”的自定义 iPerf 配置。



发现中的测试配件

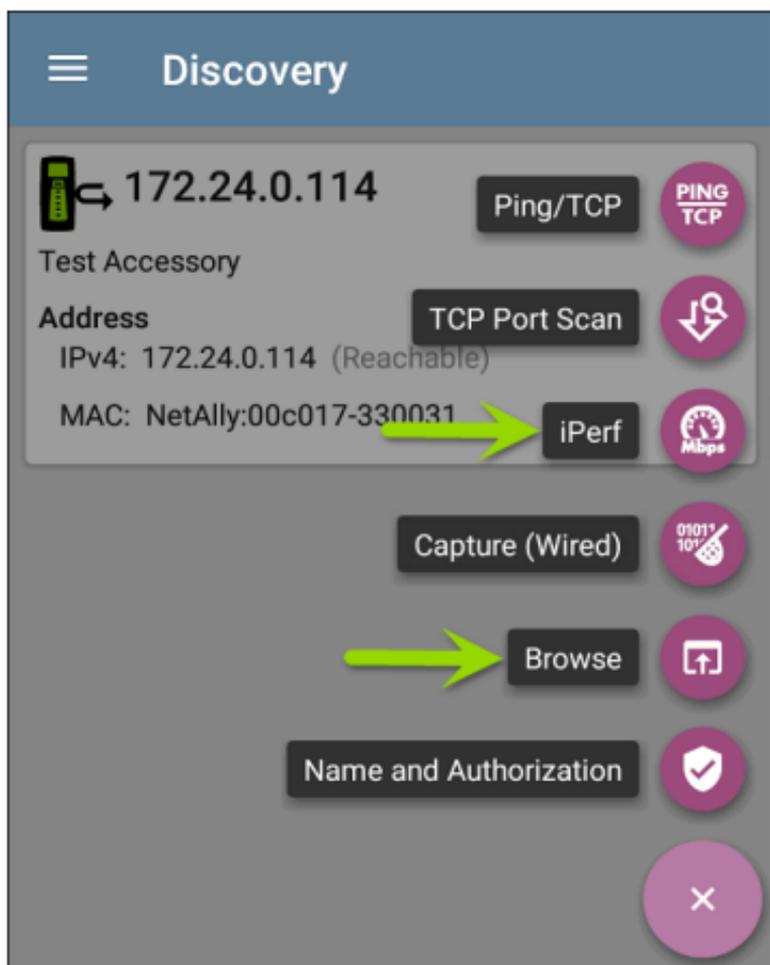
您可以从测试附件的详细信息屏幕开始 iPerf 测试。[发现应用](#)使用浮动操作按钮

1. 打开 **Discovery** 应用程序，然后选择一个活动测试配件从主发现列表打开其详细信息屏幕。



2. 打开浮动操作按钮(**FAB**) 菜单。





3. 然后，选择 **iPerf** 应用按钮。iPerf 应用程序打开时使用从 **Discovery** 中的测试附件填充的 IP 地址。

注意：您可以选择浏览在浮动操作菜单中打开测试附件的 Web 界面，您可以在其中查看其状态并配置其设置。

配置 iPerf 设置

要手动配置 iPerf 测试设置，请打开设置  在 iPerf 屏幕上。

轻触每个字段以根据需要输入或修改选择。更改的设置会自动应用。完成配置后，点击返回按钮  返回 iPerf 测试屏幕。

IPv4地址：触摸该字段以输入或选择目标 iPerf 服务器的 IPv4 地址。iPerf 测试只允许使用 IPv4 地址。



IPv4 地址对话框中的下拉列表显示所有测试附件 LRAT 通过发现 [发现过程](#)，以及声称具有相同功能的任何测试附件 [Link-Live](#) 组织作为您的 LRAT。

注意:清除对话框中的地址字段以查看发现的测试附件地址的完整列表。

端口:默认 iPerf3 端口号为 5201。点击该字段以输入不同的端口号。

注意:此处输入的 iPerf 端口号必须与 iPerf 服务器使用的端口号匹配。如果需要,请参阅测试附件用户指南 (NetAlly.com/products/TestAccessory)。

持续时间:此设置是 iPerf 测试的一个方向(上游或下游)的时间长度。如果下面的方向设置同时设置为上游/下游,则总测试时间是此处设置值的两倍。点击该字段以选择新的持续时间或输入自定义值。默认值为 10 秒。

协议:TCP 是默认协议。点击 UDP 选择器切换到 UDP。

注意:运行 TCP 协议的 iPerf 测试会以尽可能快的速度自动运行。运行 UDP 协议测试时,iPerf 应用程序会尝试以选定的带宽运行。

方向:您可以运行 iPerf 测试上游、下游或两者。默认值为上游和下游。触摸此字段以仅设置一个方向的测试。

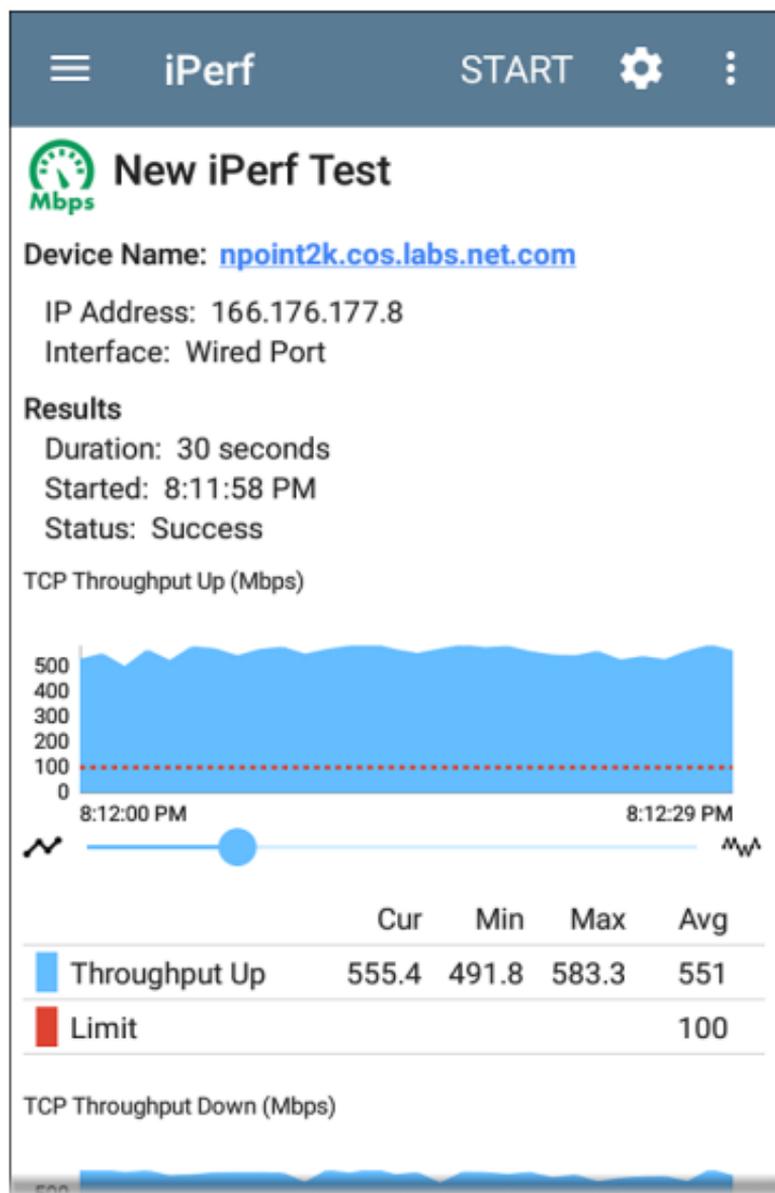
上行和下行带宽:这些字段仅在**UDP**协议被选中。它们使用 **UDP** 协议为 iPerf 测试指定所需的目标带宽。

上游和下游阈值:阈值是LRAT用于将测试评分为**通过**或**失败**。iPerf 阈值是吞吐率。默认值为 10 Mbps。点击阈值字段以选择不同的值或输入自定义值。

运行 iPerf 测试

确保您在接口上有一个活动链接([测试或管理端口](#)) 从中运行 iPerf 测试。有线测试端口要求运行自动测试有线配置文件([自动运行](#)) 以建立链接。

轻触开始 iPerf 主屏幕上的按钮开始测试。



测试特性和状态显示在 iPerf 结果屏幕的顶部，而屏幕的下部显示 TCP 或 UDP 上传和/或下载速度的实时图表。

要平移和缩放图形，您可以滑动、双击和移动滑块。参考[趋势图](#)图形控件概述的主题。

设备名称: iPerf 服务器或测试附件的主机名或地址

IP地址: iPerf 服务器的 IPv4 地址

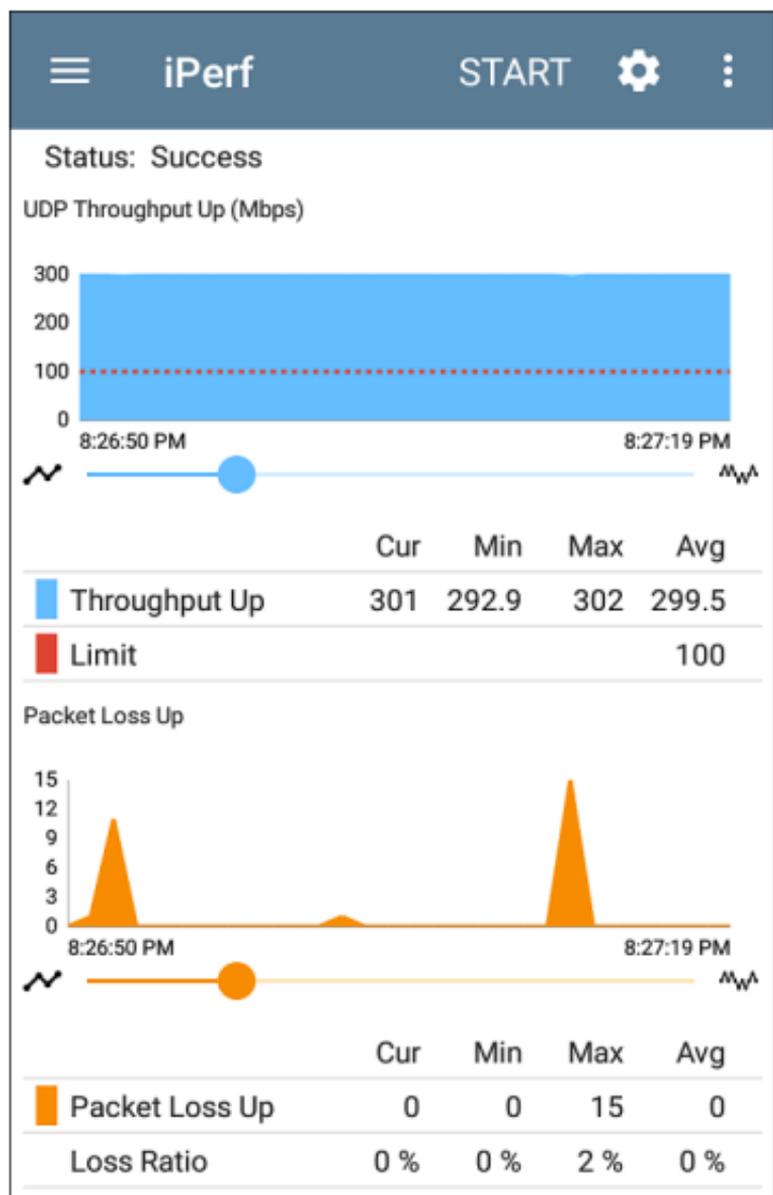
端口: 这个LRAT运行测试的测试或管理端口
结果

- **持续时间:** 从 iPerf 设置配置的持续时间
- **已开始:** 测试开始的时间
- **状态:** 测试的成功或失败状态

TCP/UDP 吞吐量上升和下降图: iPerf 图表以 Mbps 为单位绘制(向上)或从(向下) iPerf 服务器的吞吐率。

每个图表下方的表格显示当前、最小、最大和平均速率。

限制: 这是阈值来自 iPerf 应用程序的设置。阈值也在图形上显示为红色虚线。



UDP 数据包丢失向上和向下图:运行UDP协议测试时, iPerf结果还会显示数据包丢失的图形和表格。丢失数据包的数量和百分比值显示在图表下方的表格中。在上游测试

结束时从 iPerf 服务器收到结果之前，Packet Loss Up 图形和表格不会显示测量结果。

请注意，Packet Loss Up 数可能远小于 Packet Loss Down 数。

将 iPerf 结果上传到 Link-Live

将您的 iPerf 结果发送到 [Link-Live](#) 网站，触摸操作溢出按钮  在 iPerf 屏幕右上角，然后点击上传到 **Link-Live**。

**Link-Live**
by NetAlly



Iperf Result Filename
20190619_134743

Comment
Room 302

Job Comment
Union Hall

 **SAVE TO LINK-LIVE**

这个 [Link-Live 分享屏幕](#) 打开并允许您修改自动生成的文件名并将注释附加到 iPerf 结果中，该结果显示在结果中  [Link-Live.com](#) 上的页面。



Link-Live 云服务

The screenshot displays the Link-Live web interface. The top navigation bar includes the Link-Live logo, a search bar, and a user profile for 'Ken's Organization'. The main content area is titled 'Shared ACK-G3-E - 550078' and shows a list of test results on the left and detailed test data on the right.

Test Results List:

- Shared ACK-G3-E - 550078 (1/23/23 1:43 PM)
- Cobertura - 53022C (2:15 PM)
- ACK-G3-E - 550078 (2:50 PM)
- ACK-G3-E - 550078 (2:45 PM)
- inOffice IPv6 Connect to ArubaSwitch02 (2:15:02)
- EtherScope nRG - 530209 (2:09 PM)
- EtherScope xRG - 530228 (2:07 PM)
- Office ACKG3 - 55089G (1:40 PM)
- Office ACKG3 - 55089G (1:30 PM)
- inOffice IPv6 Connect to ArubaSwitch02 (1:15:02)
- inOffice IPv6 Connect to ArubaSwitch02 (1:15:02)

Test Details for Shared ACK-G3-E - 550078:

- Test:** Shared ACK-G3-E - 550078
 - MAC: 99C817-550878
 - Device: AirCheck G3
 - Type: Wireless
 - Profile: InOffice IPv6 Connect to LRG
 - Firmware: 2.2.0.43
 - Wired Management IP: 10.24.8.331
 - WiFi Management IP: 10.24.8.191
- Link:**
 - PHY Rate: 400 Mbps
 - Retry Rate: 0 %
 - Signal: -34 dBm
 - Noise: -90 dBm
 - SNR: 56 dB
 - Success
- Access Point:**
 - 10.24.8.29
 - SSID: LRG
 - BSSID: Sonicwall/10b169-c844ef
 - 802.11 Types: a, ac, n
 - Channel: 149
 - Channel Util (%): 5
 - Non-802.11 Util (%): 0.5
- DHCP:**
 - IP: 10.24.8.247
 - Server: 10.24.8.1
 - Subnet: 255.255.254.0
 - DHCP Total: 3417 req
 - Local IP: 168-200:1791:565:78
- DNS:**
 - DNS1: 127.0.0.1
- Gateway:**
 - 10.24.8.1

Link-Live 云服务是一个免费的在线系统，用于收集、跟踪、组织、分析和报告您的测试结果。在您领取 LRAT 3000-4000 后，自动测试结果将自动上传。

综合的LRAT 3000-4000在 Link-Live 中提供比以前的测试仪更多的功能来分析您的网络。确认LRAT to Link-Live.com访问这些功能：

- 检查软件更新并更新您的LRAT 3000-4000软件。
- 从第三方应用程序下载NetAlly [App Store](#)用于您的LRAT.
- 自动上传[自动测试](#)每次运行 AutoTest 时都会得到结果。
- 附上测试和[工作](#)Link-Live 上传的评论，并自动将您的结果和文件分类到 Link-Live 中的文件夹中。
- 上传测试、发现和分析结果NetAlly应用程序，包括 [发现](#)、[路径分析](#)、和 [iPerf](#)。看 [Link-Live](#) 和 [测试应用程序](#)有关上传的更多信息。

Link-Live 云服务入门

首先, 在以下位置创建一个用户帐户 [Link-Live.com](https://link-live.com), 然后登录。您可以在LRAT的网络浏览器来创建和管理您的帐户。

注册设备

在Link-Live.com

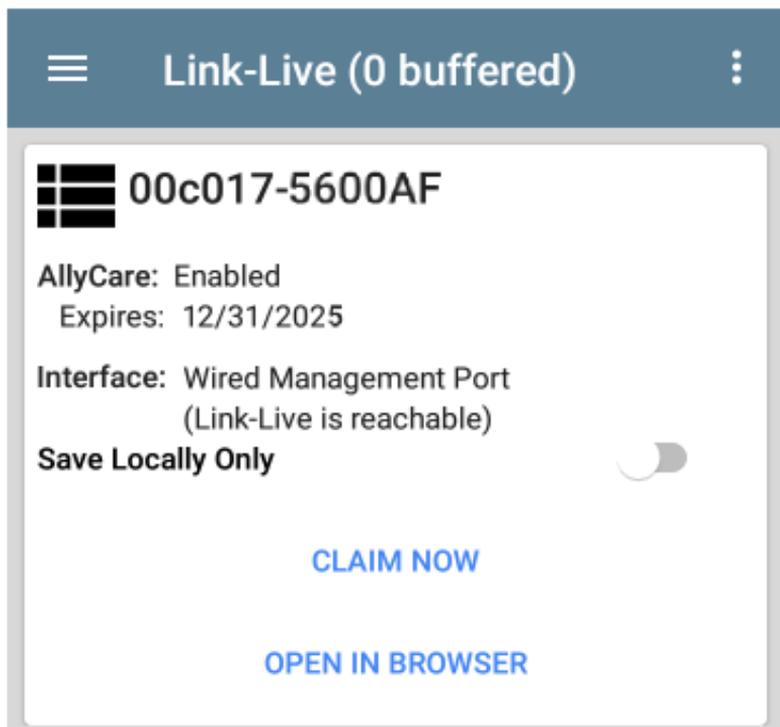
1. 首次登录 Link-Live.com 时, 会出现一个弹出窗口, 提示您注册设备。

如果您已经有一个用户帐户和其他设备声明为 Link-Live, 请导航到**Units** 左侧导航区域的页面, 然后单击注册设备按钮  在屏幕的右下角。

2. 然后选择LRAT 3000-4000图像, 并按照 Link-Live 网站上的声明说明进行操作。

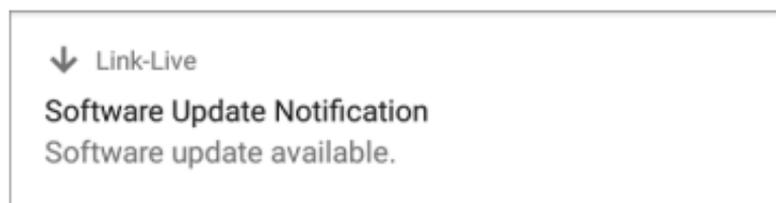
在LRAT 3000-4000设备上

1. 打开 Link-Live 应用程序。显示您设备的 MAC 地址。



2. 点击[注册](#)在 Link-Live 应用程序屏幕上。
3. 当 Link-Live 网站上的说明提示时，输入 MAC 地址。

在您注册您的 LRAT 3000-4000 到 Link-Live，可能会有软件更新。如果是这样，状态栏中会显示通知 。打开[顶部通知面板](#)，然后选择通知以更新您的设备。



参考[更新软件](#)想要查询更多的信息。

注册后

一旦你的LRATLink-Live 云服务声称,它会在您每次运行 AutoTest 时自动上传您的 AutoTest 结果。您还可以使用 AutoTest 上传测试评论和带有测试结果的图片 [有线有线测试结果](#)。您可以使用测试和自动将结果分类到 Link-Live 中的文件夹中 [工作注释](#)。

如果你的LRAT未连接到活动网络,任何测试结果、评论或图像都存储在内存中(缓冲)并在建立连接后上传。

有关如何使用的更多信息 [Link-Live.com](#) 网站,单击或触摸导航菜单图标  在 Link-Live.com 页面的左上角,然后选择  Support

取消注册

如果您不想再向 Link-Live.com 发送任何信息,您可能需要从 Link-Live 取消认领您的设备以将其转移给其他用户。

取消注册您的LRAT从您设备的 Link-Live 中,打开 [关于Link-Live](#) 应用程序左侧导航栏的屏幕,点击取消注册。



About



LinkRunner AT Tester

Model: LRAT-3000

Serial: 2405171LR3

MAC Addresses

Wired: 00c017-5600af

Wired Management: 782d7e-14c548

System Version: 2.5.0.102

Application Version: 2.5.0.104

AllyCare: Enabled

Expires: 3/27/2099

SFP Details

Type: 10GBASE-SR/1000BASE-SX (850 nm)

Vendor: FORMERICA OE

Version:

Model: TAS-A1JH1-P11

Rx Power: --

[EXPORT LOGS](#)

AllyCare 激活码

如果您的设备未绑定，AllyCare 代码按钮将出现在“关于”屏幕底部的“导出日志”按钮旁边。

[ALLYCARE CODE](#)

[EXPORT LOGS](#)

Tap **AllyCare 激活码** 打开对话框以输入 AllyCare 激活码。

私有 Link-Live 设定

仅在您已经部署了私有 Link-Live时使用此设定。请咨询NetAlly以获取更多私有 Link-Live 服务信息。

Link-Live 应用程序功能

您的主 Link-Live 应用程序屏幕LRAT 3000-4000有利于这侧过程, 显示链接的Live相关信息, 并允许您启用或禁用Link-Live.com上传需要。

Link-Live 应用程序屏幕

The screenshot shows a mobile application interface with a dark blue header bar containing a hamburger menu icon and the text "Link-Live (0 buffered)". Below the header is a white card with a grey border. The card displays the following information:

- Ken's LinkRunner 10G - 540024** (with a Link-Live logo icon)
- Organization: My Organization
- E-mail: ken@netally.com
- AllyCare: Enabled
- Expires: 12/31/2023
- MAC: 00C017-530208
- Interface: Wired Management Port
(Link-Live is reachable)
- Enable Link-Live:
- Save Locally Only:
- [OPEN IN BROWSER](#)

LRATLink-Live.com 上显示的设备名称显示在 Link-Live 图标的右侧 。您可以在 Link-Live.com 上更改此名称单位  页面。

组织是声称该单元的 Link-Live 组织。

E-mail是分配给单元的第一个电子邮件地址，它接收测试结果通知电子邮件。

此处显示的组织 and 电子邮件地址是在 Link-Live.com 网站上分配的。显示的字段 LRAT 的 Link-Live 应用程序提供信息。

AllyCare优享服务指示 NetAlly 的可选 AllyCare 服务的状态。参考 [NetAlly.com/Support](https://www.netally.com/support) 想要查询更多的信息。

端口显示 Link-Live 当前正在使用哪个网络接口来发布结果及其状态。

启用 **Link-Live** 切换按钮可打开或关闭 Link-Live 功能。如果此处禁用了 Link-Live，则 LRAT 无法上传测试结果或检查软件更新。这上传到 **Link-Live** 选项不会出现在测试应用程序中。

触摸 [用浏览器打开](#) 链接以打开 Link-Live.com LRAT 的网络浏览器。

Link-Live 屏幕标题中的“(# buffered)”表示当没有可用的活动网络连接时存储在设备内存中的文件数。缓冲文件类型列在主应用程序卡下方。

☰ **Link-Live (2 buffered)**

 **Ken's LinkRunner 10G - 540024**

Organization: My Organization
E-mail: ken@netally.com
AllyCare: Enabled
Expires: 12/31/2024
MAC: 00C017-530208
Interface: Wired Management Port
(Link-Live is reachable)

Enable Link-Live

Save Locally Only

[OPEN IN BROWSER](#)

Discovery Snapshot 
Apr 25, 2023 11:16:24 PM

Wired Snapshot 
Apr 25, 2023 11:16:25 PM

显示的缓冲文件会自动上传到 Link-Live.com。LRAT连接到活动网络。

仅在本地保存

如果您不想将结果发送到 Link-Live 网站，您仍然可以将结果本地保存到您的LRAT作为JSON文件。

轻触仅本地保存Link-Live应用程序中的切换字段以将JSON文件保存到您的设备。

 **Thomas' LinkRunner 10G - 530AB0**

AllyCare: Enabled
Expires: 12/31/2023

Save Locally Only



[SHOW FILES](#)

 **terry's LinkRunner AT 3000/400...**

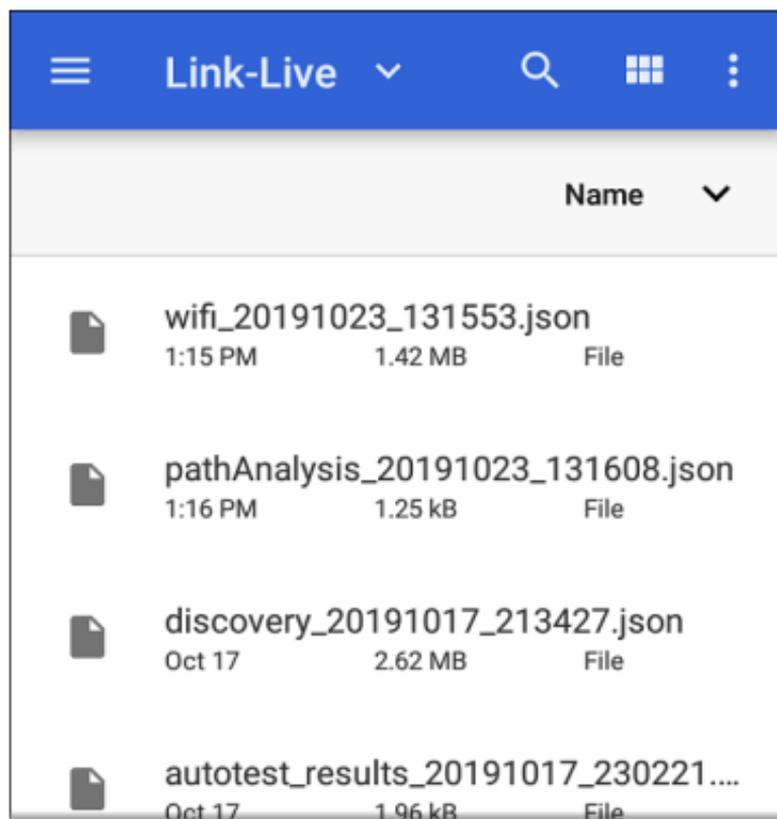
AllyCare: Enabled
Expires: 12/31/2023

Save Locally Only



[SHOW FILES](#)

选择[显示文件](#)打开[文件](#)应用程序。`.json`文件保存在[下载](#)>[测试结果](#)文件夹。



参考[管理文件](#)文件应用程序概述的主题。

您可以将 JSON 文件传输到 PC 进行分析，也可以从 App Store 下载 JSON 查看器应用程序  在你设备上LRAT。

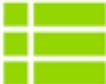
使用仅本地保存已启用，上传或保存到 Link-Live 的选项(在[Link-Live](#)和[测试应用程序](#)下面的部分)仍然显示在NetAlly测试应用程

序。但是，结果会保存到 Link-Live 的内部存储文件夹中，而不是上传到 Link-Live.com。

工作评论

这个[左侧导航区域](#)对于 Link-Live 应用程序，您可以输入或更改工作评论。这工作评论附加到上传到 Link-Live 的所有测试结果和文件，直到您更改或删除它。相比之下，其他注解，就像那些附加到[Wired](#)自动测试配置文件或[发现](#)结果，仅附加到一组测试结果或上传的文件中。

两种评论类型都出现在[Link-Live 共享屏幕](#)像下面的一个：

**Link-Live**
by NetAlly



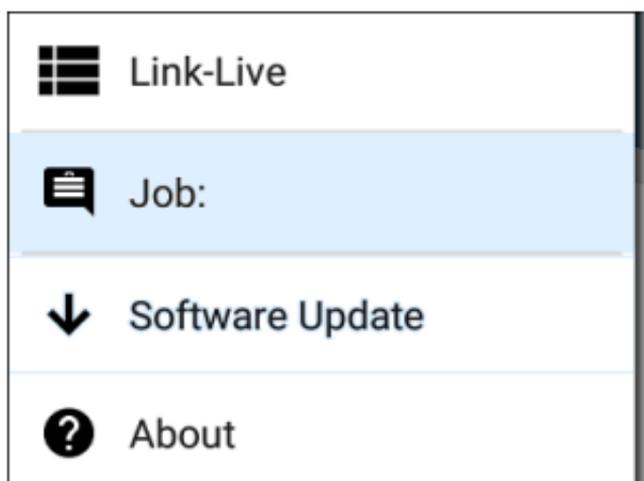
File Name
client1024rsa-new.pem

Comment
Certs

Job Comment
South Campus Wi-Fi

要在 **Link-Live** 应用程序中输入或更改工作评论：

1. 在 **Link-Live** 应用程序打开的情况下，触摸菜单图标  或从屏幕左侧向右滑动。



2. 轻触工作：字段。
3. 在对话框中输入注释。
4. 轻触保存。

请注意，工作评论字段出现在其他 Link-Live 共享屏幕中，允许您从多个位置更改它 LRAT。无论您在何处更改工作评论，它都会在设备上的任何地方更新。

软件更新

Link-Live 应用程序的左侧导航区域还可让您检查和下载任何可用的软件更新。参考[更新软件](#)在软件管理章节。

Link-Live 和测试应用程序

一旦您的设备被认领，Link-Live 应用程序将与多个测试应用程序协同工作，将测试结果、发现和分析数据、评论和图像上传到 Link-Live 网站。Link-Live.com 将不同应用程序上传到相应网页进行分类，如下图：

LINK-LIVE 网页	应用上传
 结果	自动测试、性能、iPerf 和电缆测试结果 保存到测试结果时的图像、连接日志和其他文件
 上传的文件	捕获、图像、连接日志和其他文件类型
 分析	发现和路径分析结果

如果您的设备没有注册 [Link-Live.com](https://link-live.com) 或者，如果应用程序屏幕上禁用了 Link-Live，则不会出现用于在测试应用程序中上传到 Link-Live 的链接和按钮。

Link-Live 共享屏幕

Save to Link-Live



UPLOAD TO LINK-LIVE

每当您选择一个按钮或链接(如上面的那些)以上传、保存或[分享](#)到Link-Live, 出现Link-Live共享屏幕, 其中包含适合数据类型的选项。

例如, Discovery的Link-Live共享屏幕应用程序数据允许您上传到分析  Link-Live.com 上的页面。

**Link-Live**

by NetAlly

**Wi-Fi Snapshot Name**

20190429_122109

Comment

Conference Room B

Job Comment

North Office



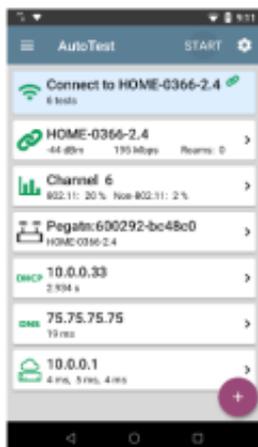
SAVE TO ANALYSIS FILES

屏幕截图或其他图像的 Link-Live 共享屏幕允许您将其附加到最近运行的(自动测试、性能、iPerf 或电缆测试)测试结果上的结果  页面, 或者只是到上传的文件  Link-Live.com 上的页面。



Link-Live

by NetAlly



Comment

Conference Room B

Job Comment

North Office



SAVE TO LAST TEST RESULT



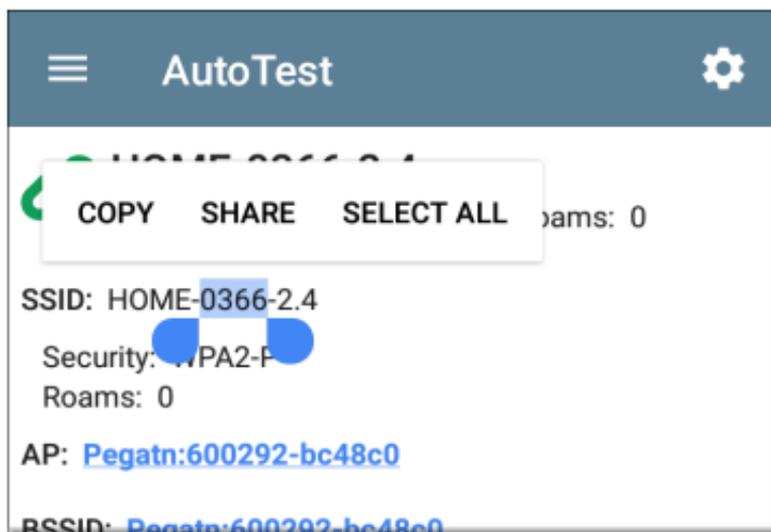
SAVE TO UPLOADED FILES

记住，常规注解字段仅上传到当前结果或文件，而工作注解字段上传所有结果和文件，直到您更改它。

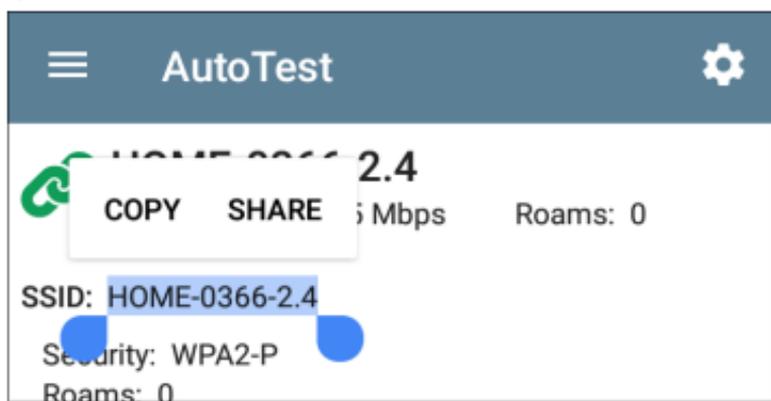
共享文本文件到 Link-Live

您还可以通过以下方式选择和共享文本。长按单元屏幕上的文本。文本文件附在 Link-Live.com 上的最后测试结果中。

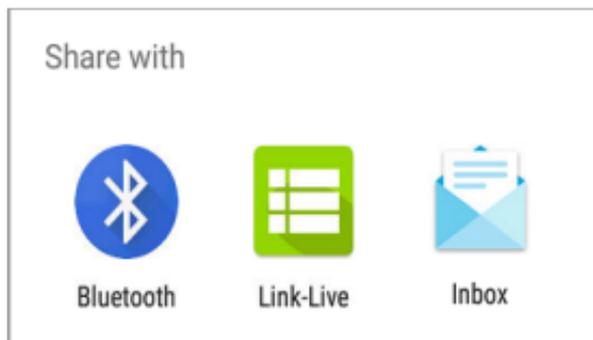
1. 长按文本字符串以选择它。



2. 轻触 全选如果需要的话。



3. 轻触 **SHARE**.



4. 选择 Link-Live 图标以打开 [Link-Live 共享](#) 屏幕。

**Link-Live**
by NetAlly



File Name
20191106_155804

Comment
SSIDs

Job Comment
/Inventory

 **SAVE TO LAST TEST RESULT**

5. 格式化任何**注解**根据需要, 然后触摸保存到上次测试结果.

规格和合规性

本章包含所需的合规信息。

LRAT 3000-4000 规格

规格

尺寸	4.02 in x 7.72 in x 1.65 in (10.2 cm x 19.6 cm x 4.2 cm)
重量	1.06 lbs (0.48 kg)
电池	可充电锂离子电池组 (3.63 V, 9.75 Ah, 36.39 Wh)
电池寿命	一般工作寿命9小时. 一般充电时间为3小时.
显示	带电容式触摸屏的 5.0 英寸彩色 LCD(720 x 1280 像素)
主机端口	RJ-45 Ethernet test port RJ-45 cable test port (1) USB Type-A Port (1) USB Type-C On-the-Go Port
内存	大约 8 GB 可用于存储测试结果和用户应用程序
充电	USB Type-C 65-W 适配器: 交流输入电源 100-240 V, 50-60 Hz; 直流输出电源 15 V (3 A)
PoE 收费	802.3 af/at
支持的 IEEE 标准	Wired: 802.3/ab/i/u/z, 1000 BASE-T PoE: 802.3af/at/bt Class 0-8, UPOE Fiber: 1000BASE-X, SFP SX/LX/ZX
LEDs	1 LED (电池状态指示)

环境指标

操作温度	32°F 到 113°F (0°C 到 +45°C) 注意:如果设备的内部温度高于 113°F (45°C), 电池将不会充电.
工作相对湿度(% RH, 无冷凝)	90% (50°F 到 95°F; 10°C 到 35°C) 75% (95°F 到 113°F; 35°C 到 45°C)
储存温度	-4°F 到 140°F (-20°C 到 +60°C)
冲击和振动	满足 MIL-PRF-28800F 对 3 类设备的要求
安全	IEC 61010-1:2010:污染等级 2
高度	运营:4,000 m; 存储:12,000 m
EMC	IEC 61326-1:基本电磁环境 CISPR 11:第 1 组, A 类

第 1 组:设备有意产生和/或使用传导耦合射频能量, 这种能量对于设备本身的内部功能是必需的。

A 类:设备适用于除家用和直接连接到为家用建筑物供电的低压供电网络以外的所有场所。由于传导和辐射干扰, 在其他环境中确保电磁兼容性可能会有潜在困难。

索引

A

Active

- discovery ports 322
- subnets 325

Adapter

- USB to Ethernet 51

Adding

- profile groups 135
- profiles 129
- test targets 169

Address

- Discovery 326
- extended range 322

Addresses

- Discovery 276
- subnet 323

Apps

- AutoTest 124

- Capture 207, 362
 - configurations, saving 95
 - Discovery 245
 - Files 74
 - Path Analysis 343
 - Ping/TCP 226
 - settings, loading 88
 - settings, saving 92
- ARP sweep rate 326
- Assigning device name 309
- Authname file 316
- Authorization 309
 - batch 259
- AutoTest
 - app 124
 - FTP test 197
 - HTTP test 187
 - importing/exporting profiles 137
 - main screen 139

- periodic 141
- Ping 175
- settings, transferring 99
- TCP connect test 182

B

- Batch authorization 259
- Battery charging 21
- Buttons 18

C

Cable Test

- open cable TDR test 215
- patch cable testing 220
- running 214
- settings 212
- terminated WireView test 218
- toning function 222

Capture

- running 240, 368

- settings 363
 - viewing 240, 368
 - wired filters 239
- Charging and power 21
- charge via PoE setting 59
 - PoE 21
- Chromium browser 71
- Cleaning 25
- Colors, icons 139
- Common
- icons 68
 - tools 71
- Configuring
- iPerf 377
 - saving configuration 92, 95
 - SNMP 327
- Connecting
- devices, Discovery 288
 - TCP Connect test 182

Wi-Fi 40

D

Defaults, app settings 88

Details

Discovery

Discovery 267

Device

discovery 333

health 336

Layer 2 356

names 309

names, assigning 309

types, Discovery 294

VoIP 336

Device types

hosts/clients 306

hypervisors 299

network servers 298

- printers 303
- routers 295
- SNMP agents 304
- switches 296-297
- virtual machines 300
- Wi-Fi controllers 302

DHCP

- test 146-147

Differences between models 16

Discovery

- addresses 276
- app 245
- connected devices 288
- details screens 267
- device types 294
- FAB 290
- filtering list 253
- interfaces 281
- main list screen 249

- notifications 56
 - ports 322
 - problem settings 338
 - problems 275
 - refresh 264
 - resources 289
 - searching list 252
 - security auditing 259
 - settings 319
 - SNMP 286
 - sorting list 256
 - TCP port scan 278
 - Test Accessory 374
 - through other devices 333
 - VLANs 280
- Distance units 63
- DNS
- test 159
 - tests 146

E

Ejecting storage media 78

Ethernet adapter 51

Exporting

- AutoTest profiles 137

- settings 95, 104

Extended ranges 322

External USB adapter 40

F

FAB

- Discovery 290

Factory defaults

- profiles 128

Files

- app 74

- authname 316

- managing 74

- moving and copying 76

text, sharing to Link-Live 405

Filters

Discovery list 253

wired 239

FTP test, AutoTest 197

G

Gateway

test 163

tests 146

Grading test results 160, 164, 178, 183, 191,
201

Graphs, trending 64

Groups, profile 128, 131

H

Hosts/clients, discovery 306

HTTP

test 187

Hypervisors 299

I

Icons

- colors 139

- common 68

Importing

- AutoTest profiles 137

- settings 95, 104

Interfaces, Discovery 281

Interval

- device health 336

- refresh 327

iPerf

- running 380

- settings 373

L

Layer 2 Devices 356

Layer 3 Hops 352

Link-Live

- app 386
- cloud service 386
- features 393
- introduction 386
- job comment 398
- notifications 401
- saving locally only 396
- software updates 400
- transferring settings 99
- uploading results 225, 265, 360, 384

Link-Live Remote

- notifications 57

LinkRunner AT

- feature access 109
- features 18
- models 16

List

- filtering, Discovery 253

- searching, Discovery 252

- sorting, Discovery 256

Loading

- app settings 88

Local save 63

M

Machines, virtual 336

Management

- files 74

- port notifications 56

- ports 49-50

- settings 60

Models, differences between 16

N

Names, device 309

Navigation

- system 29

Network

- servers 298

Notifications

- discovery 56

- Link-Live 401

- Link-Live Remote 57

- management port 56

- panel 33

- system 33

- test and port status 54

- test port 54

- VNC 57

P

- Password, VNC 62

Path Analysis

- app 343

- introduction 344

- Layer 2 devices 356

- Layer 3 hops 352
- manual configuration 345
- populating 345
- results 350
- running 348
- settings 345

Periodic AutoTest 141, 143

Ping

- TCP app 226
- TCP app, running 232
- TCP settings 227
- 测试 175

PoE

- charge battery setting 59
- charging 21, 57
- test PoE before link 59

Ports 18, 49

- Discovery 322
- management 50

- selecting 52

- test 49

Power

- powering on 23

Preferences 63

Printers 303

Problems

- Discovery 275

- settings 338

Profiles

- adding 129

- adding groups 135

- exporting 137

- groups 131

- importing 137

- managing 128

R

Range, extended 322

Refresh

- Discovery 264

Refresh interval 327

Reset

- trending graphs 67

- user name/authorization 316

Resources, Discovery 289

Restricted subnets 325

Results

- Cable Test, uploading 225

- iPerf, uploading 384

- Path Analysis 350, 360

- screen, test target 172

Reverse grading 160, 164, 178, 183, 191, 201

Routers 295, 334

Running

- Capture 240, 368

- iPerf tests 380

- Path Analysis 348

Periodic AutoTest 143

Ping/TCP test 232

S

Saving

app settings 92

configuration 95

locally only 63, 396

Screen

Discovery, main 249

shot 43

Searching, Discovery list 252

Security

auditing, batch authorization 259

auditing, Discovery 259

Selecting, ports 52

Server

network, discovery 298

Settings

- app defaults 88
- Cable Test 212
- Capture app 363
- default 88
- Discovery 319
- exporting 95, 104
- importing 95, 104
- iPerf 373
- management 60
- managing 88
- Path Analysis 345
- periodic AutoTest 141
- Ping/TCP app 227
- preferences 63
- problems, discovery 338
- test app 88
- transferring 99
- VNC 61

- wired filters 239

- wired, general 59

Sharing

- screen shot 43

- screens, Link-Live 401

- text files, Link-Live 405

Show internal storage 32

SNMP

- agents 304

- configuration 327

- Discovery 286

- query delay 333

Software

- manual updates 83

- updates 400

- updating 81, 83

Sorting

- Discovery list 256

SSH 71

Static IP test 147

Status

- bar 33

- notifications 54

Storage, media 78

Subnet

- addresses 323

- mask 326

Subnets 334

- active v. restrictive 325

Sweep rate, ARP 326

Switches 296-297, 335

System

- navigation 29

- notifications 33

- status bar 33

T

Targets

- addresses 172
- test results 172

TCP

- connect test 182
- port scan, Discovery 278
- test app 226

Telnet/SSH 71

Test

- app defaults 88
- DHCP 147
- DNS 159
- FTP 197
- gateway 163
- HTTP 187
- notifications 54
- Ping/TCP 226

- port notifications 54
- ports 49
- static IP 147
- targets, adding 169
- targets, managing 169
- targets, results 172
- TCP connect 182

Test Accessory 374

Tools, common 71

Transfer, AutoTest settings 99

Trending graphs 64

- reset 67

U

Units, distance 63

Unknown switches 297

Updating

- manual 83

- software 81, 400

Upload

results to Link-Live 225, 265, 360, 384

USB

drive 77

external adapter 40

Type-C to USB cable 78

V

Viewing, Capture 240, 368

Virtual machines 300, 336

VLANs, Discovery 280

VNC

notifications 57

password 62

settings 61

VoIP

devices 336

phones 302

W

Web browser 71

Wi-Fi

 connecting to 40

Wired, general settings 59