netAlly

LinkRunner® AT 3000 & 4000

User Guide

Tap a link to go directly to the app's chapter.
Scroll down to view the full list of Contents.

NetAlly Network Testing Apps

AutoTest

Switch

Cable Test

Ping/TCP

Capture

Discovery

Path Analysis

Reflector

iPerf

Link-Live

App Store

Software v2.5. Published August 14, 2024

Contents

Contact Us

Online: NetAlly.com

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

NetAlly
2075 Research Parkway, Suite 190
Colorado Springs, CO 80920

For additional product resources, visit:
NetAlly.com/Products/LinkRunner-3000
Netally.com/products/LinkRunner-4000

For customer support, visit:
NetAlly.com/Support

Register your LRAT 3000-4000

Registering your product with NetAlly gives you access to valuable information on product updates, troubleshooting procedures, and other services.

Register on the NetAlly Support Page.

Back to Title and Contents

Introduction

The LRAT 3000-4000 is a rugged, hand-held tool for testing and analyzing copper and fiber networks. It features applications developed by NetAlly for network discovery, measurement, and validation, which are available from the Home and Apps screens.

All NetAlly hand-held testers include access to Link-Live Cloud Service at Link-Live.com. Link-Live is an online system for collecting, organizing, analyzing, and reporting your test results. Test data is automatically uploaded once your tester is properly configured. Visit Link-Live.com and "Claim" your LRAT to access these features.

How to Use this Guide

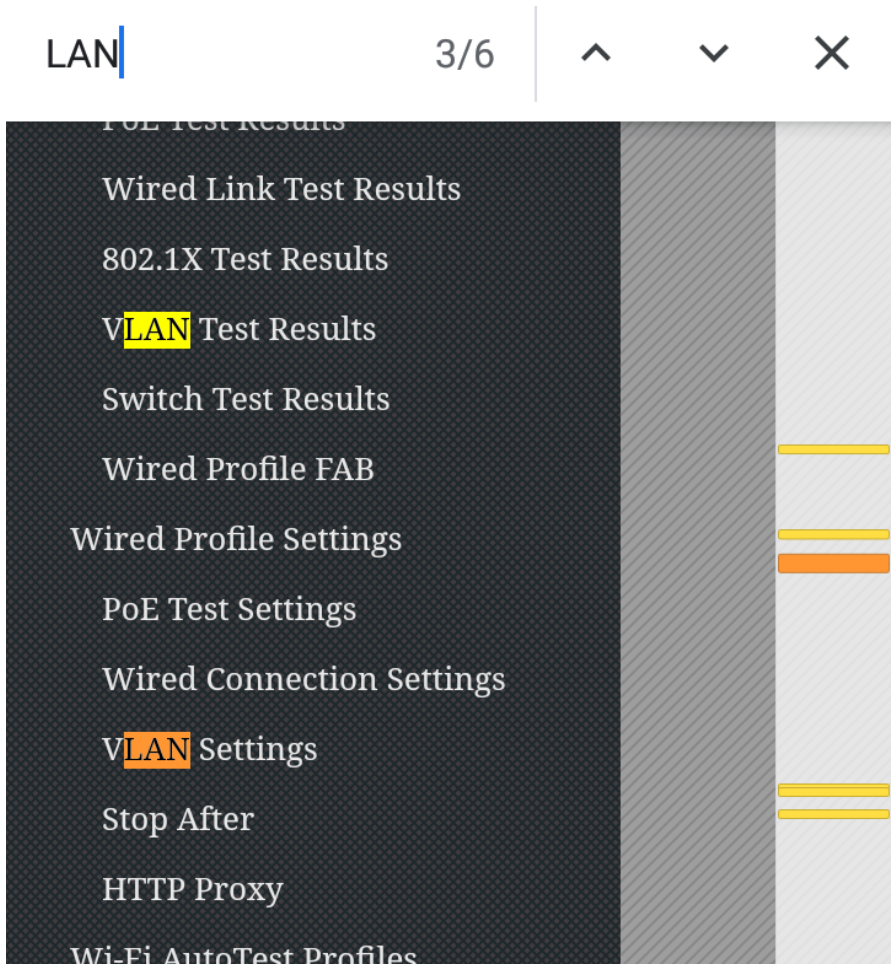
This user guide describes the LRAT 3000-4000's testing functionality and basic elements of the system interface.

The guide is meant for users who are knowledgeable about network operations, tests, and measurements.

The LRAT 3000-4000 is also referred to as just LRAT or the "unit" in this guide.

- Tap **blue links** to go to their destinations. Underlined blue links open external websites.
- Tap bookmarks in the list on the left to go to the corresponding section.
- Tap headings in the **Contents** list that starts on page 2 to go to the corresponding sections.
- To search for a word or phrase:
  1. Tap the browser menu  icon in the upper right.
  2. Select **Find in Page** from the menu.

3. Enter the search text.
4. Tap the find icon . This displays the text at the top of the screen. Tap the up and down arrows to search forwards and backwards for the text. In the image below, the user has searched on "LAN". Tap the highlight bars on the right to go to the corresponding manual text.



Online and Local Versions of This Guide, Videos

- Manuals are also available for download at: https://www.netally.com/support/user-guides/
- To view the User Guide on your LRAT 3000-4000, you must have a network connection with access to the internet. When you tap on **Guides > User Guide** on the "Home Screen" on page 32, this user guide is downloaded and displays on your unit.
- After you have downloaded the User Guide to your unit, the guide is stored in a local cache for the browser. You do not have to repeat the download unless you change the device language or clear the browser cache.
- The Guides icon on the Home Screen (used to access this guide) also gives access to training and information videos specific to this product.

International Versions of This Guide

A Chinese or English LRAT 3000-4000 user guide is available if you change the device language to one of those languages. The English user manual is used if you change the language to German, Japanese, or Korean.

Differences Between Models

The Model number of your LRAT appears on the About Screen and is printed on the back panel of your unit. This manual covers all models and identifies features specific to each model if there are differences. In general:

LINKRUNNER-AT-3000, LINKRUNNER-AT-4000

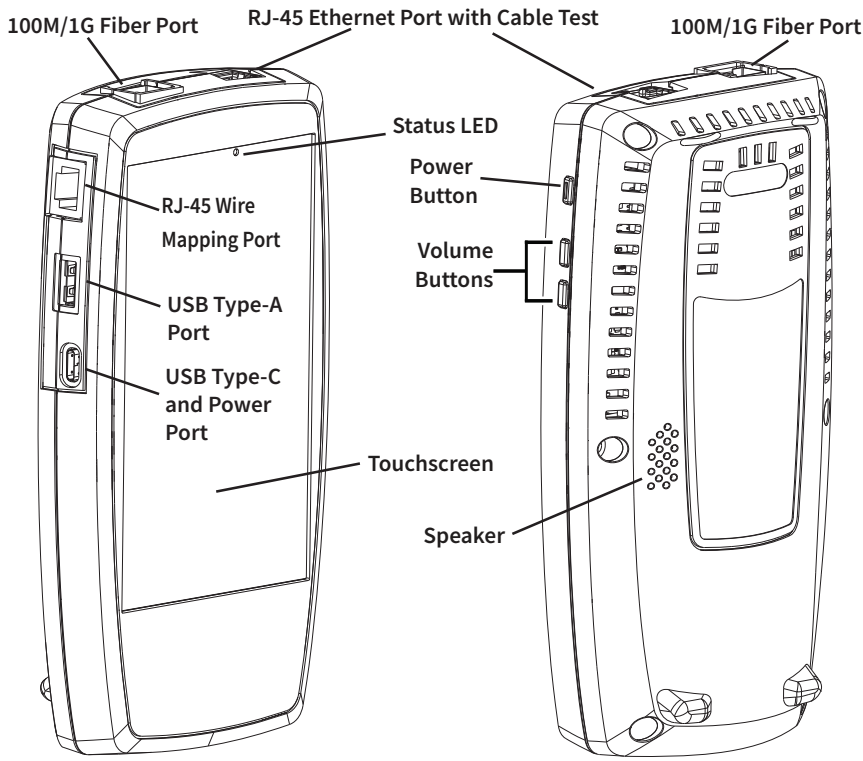
- LinkRunner-AT-3000:
  - Does not include the Capture, Discovery, iPerf, or Path Analysis apps.
  - Does not support Periodic AutoTest.
  - Does not support HTTP/FTP targets in AutoTest.
  - Purchase price does not include an AllyCare subscription.
  - Requires registration before you can use the App Store.
- LinkRunner-AT-4000:

- Includes the Capture, Discovery, iPerf, and Path Analysis apps.
- Supports Periodic AutoTest.
- Support HTTP/FTP targets in AutoTest
- Includes a 1-year AllyCare subscription.
- Does not require registration before you can use the App Store.

For more information, see LRAT 3000-4000 Specifications.

Buttons and Ports

Button and port functions on your LRAT unit are described below.



Feature	Description
Status LED	Red: unit off, USB-C power adapter connected Green: unit on, screen off (with or without power adapter) Rate of blinking LED (red or green) shows % battery charge: • 2 blinks per second: battery low, 0-24% charged

Feature	Description
	• 1 blink per second: 25-49% charged • 1 blink per 2 seconds: 50-74% charged • 1 blink per 4 seconds: ≥75% charged • No blinks: fully charged
RJ-45 Wire Mapping Port	Internal wire mapper port used for loopback cable testing
RJ-45 Ethernet Port with Cable Test	General purpose port for linking to a network, running a cable test, including Tone and Flash Port functions Supports PoE (with compatible unit hardware)
USB Type-A Port	Connects to any USB device. (FAT32-formatted device required only for manual software updates.)
USB Type-C On-the-Go Port	Connects to a USB Type-C connector for file transfer and to charge unit with the included AC adapter

Feature	Description
Volume Buttons	Increase or decrease the audio volume for external Bluetooth or USB speakers or headsets
Power Button	Press and hold to display menu for **Power off** or **Restart**
Speaker	Produces audio

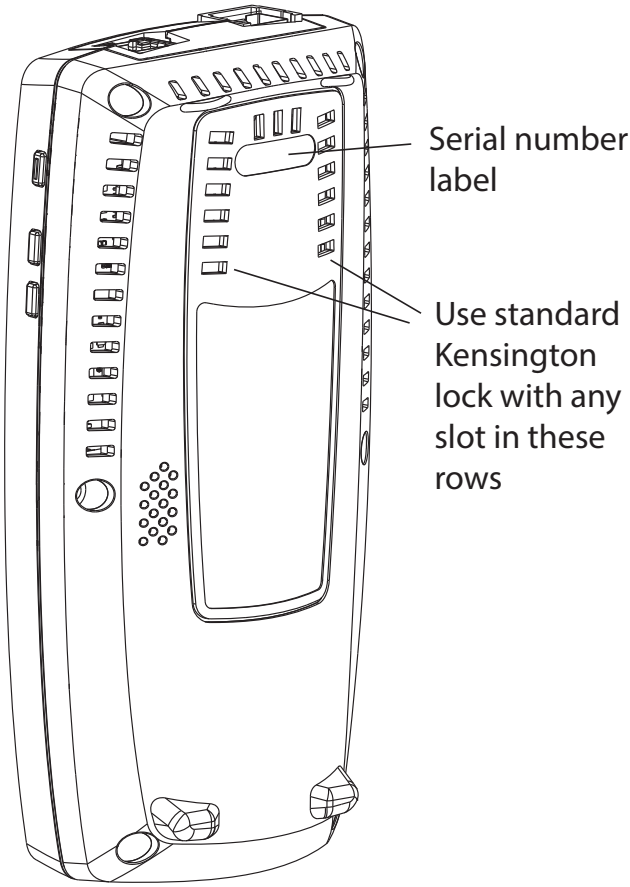
See Test and Management Ports for detailed explanations of the port functions.

See Updating Software for requirements on updating system software.

Refer to the product Specifications if needed.

Using a Kensington Lock

The back panel of the unit has two rows of six vent slots on either side of the serial number label. You can use a standard Kensington lock with any slot in these two rows.


Serial number label
Use standard Kensington lock with any slot in these rows

Charging and Power

Your LRAT 3000-4000 includes a USB-C 15V/3A power adapter.

⚠ **CAUTION**: Only the NetAlly-supplied power adapter is supported.

To begin charging the internal lithium-ion battery, plug the included power adapter into an AC outlet and the USB-C charging port on the left side of the unit. The Power button turns red when the unit is in charging mode and turns off at full charge. Refer to the Specifications for battery run duration and charge times.

PoE Charging

Power over Ethernet (PoE) can provide alternative power to your unit's battery. (Test units that include the **Charge Battery via PoE** setting in General Settings, support PoE.)

- Negotiated PoE class levels 3-8 (≥ 15.5 W) provide enough power to run the test unit indefinitely and to charge the battery.

- Negotiated PoE class levels 0-2 (≤ 6.4 W) provide some power to extend battery run time but not enough to charge the battery.

Use the following steps to enable PoE charging:

1. Connect the top RJ-45 port on the unit to a network switch with PoE or to a PoE injector.
2. Make sure the unit is powered on or in display sleep mode.
3. If your test unit displays the **Charge Battery via PoE** setting in General Settings, tap the setting to enable PoE charging.
4. Detect the PoE availability by running an AutoTest Wired Profile with a PoE test that passes. (The **PoE Test** must be enabled and configured with a **Powered Device Class** that is supported by your switch or PoE Injector.) See Wired Profile Settings and Results.

   NOTE: If the AutoTest app is not currently open, the last Wired Profile in the profile list runs automatically when you power on the

unit or LRAT detects a new copper link in the top Wired Test Port.

See Buttons and Ports for port locations and descriptions.

Powering On

- To start up the unit, hold down the Power Button for approximately one second, until the Power Button LED Status LED turns green.
- When the display goes into Sleep mode, the Power Button LED remains on. Status LED blinks green to indicate the battery level. Tap the Power Button briefly to wake up the display. (Set the timing for display sleep and auto power off in the Device Settings.)
- To shut down or restart, hold down the Power Button for one second until the “Power off” and "Restart" dialog box appears on the touchscreen, and then tap **Power off** or **Restart**.
- If the unit is unresponsive to a normal power off, press and hold the Power Button for five

seconds to perform a hard shutdown.

Back to Title and Contents

Safety and Maintenance

Observe the following safety information:

Use only the Adapter provided or Power over Ethernet (PoE) to charge the battery.

Ensure that the Adapter is easily accessible.

Use the proper terminals and cables for all connections.

⚠ **CAUTION**: To avoid possible electric shock or personal injury, follow these guidelines:

- Do not use the product if it is damaged. Before using the product, inspect the case, and look for cracked or missing plastic.
- Do not operate the product around explosive gas, vapor, or dust.
- Do not try to service the product. There are no serviceable parts.
- Do not replace the battery. There is risk of explosion if the battery is replaced by an incorrect battery type.
- Dispose of battery packs and electronics in compliance with your institution's disposal instructions.

- Use as directed. If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired.

Safety Symbols

	**Warning or Caution: Risk of damage to or destruction of equipment or software.**
	**Warning: Risk of electrical shock.**
	**Not for connection to a public telephone system.**

Cleaning

To clean the display, use a lens cleaner and a soft, lint-free cloth.

To clean the case, use a soft cloth that is moist with water or a weak soap.

Scratches on the dark-colored plastic can be removed by *lightly* scrubbing a 1:2 mixture of toothpaste to water onto the affected surface with a bristled brush.

⚠ **CAUTION:** Do not use solvents or abrasive materials that may damage the product.

Legal Notification

Use of this product requires acceptance of the Terms and Conditions available at http://NetAlly.com/terms-and-conditions or which accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NetAlly and the purchaser of this product.

Open-Source Software Acknowledgment: This product may incorporate open-source components. NetAlly will make available open-source code components of this product, if any, at Link-Live.com/OpenSource.

NetAlly reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.

Back to Title and Contents

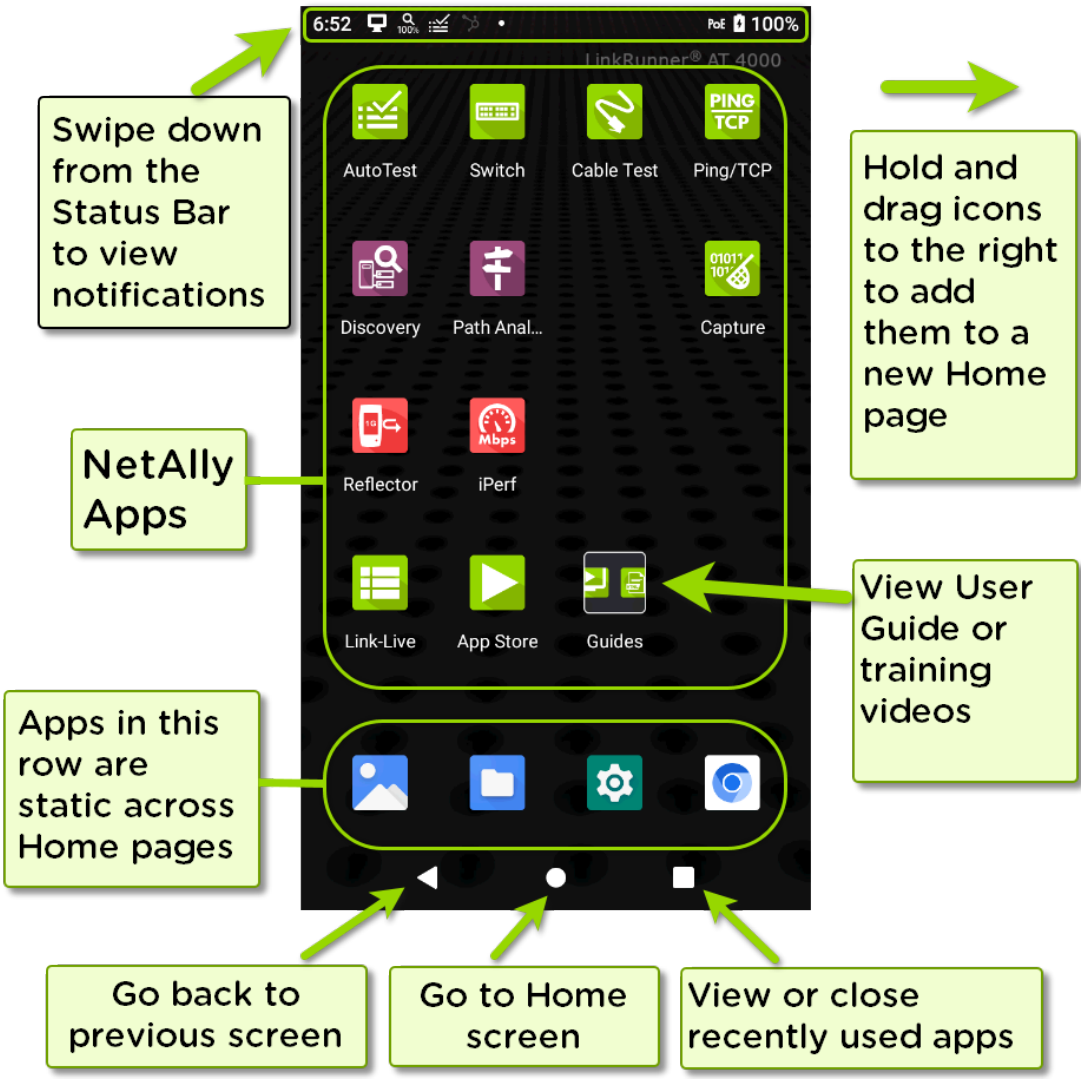
Back to Title and Contents

Home and System Interface

This chapter explains how to use the features of the system Home screen and user interface to navigate and organize your device.

The LRAT 3000-4000 interface supports many of the operations typical of any hand-held device. Use dragging and swiping motions on the touchscreen to navigate through apps, open side menus, drag down the Notification Panel from the Status Bar at the top of the Home screen, or drag up the Apps screen from the bottom.

Home Screen



NOTE: The LRAT-3000 does not include the Discovery, Path Analysis, Capture, or iPerf apps. You must also register your LRAT-3000 before you can use the App Store.

Like other hand-held devices, your LRAT 3000-4000 Home screen is customizable. The image above shows the default configuration, but you can add, remove, and reorganize app icons and widgets to serve your purposes.

You can also create more Home pages by tapping, holding, and dragging an app icon to the right from the main Home screen.

See the Apps screen section for instructions on adding more apps to your Home pages.

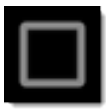
Navigating the System

The navigation actions you can perform to move through screens and panels on the LRAT 3000-4000 are the same as those you would use to navigate many other phone or tablet devices.

The main device navigation buttons appear at the bottom of the touch screen.

The back icon returns to the previous screen.

The circle icon opens the Home screen.



The square icon displays your recently used applications for easily switching between then. This is also the screen where you can close, or stop, the open applications.

TIP: Double tap the square icon to switch back to the previous app you were using and to switch back and forth between two app screens (like a testing app and this User Guide).

Swiping

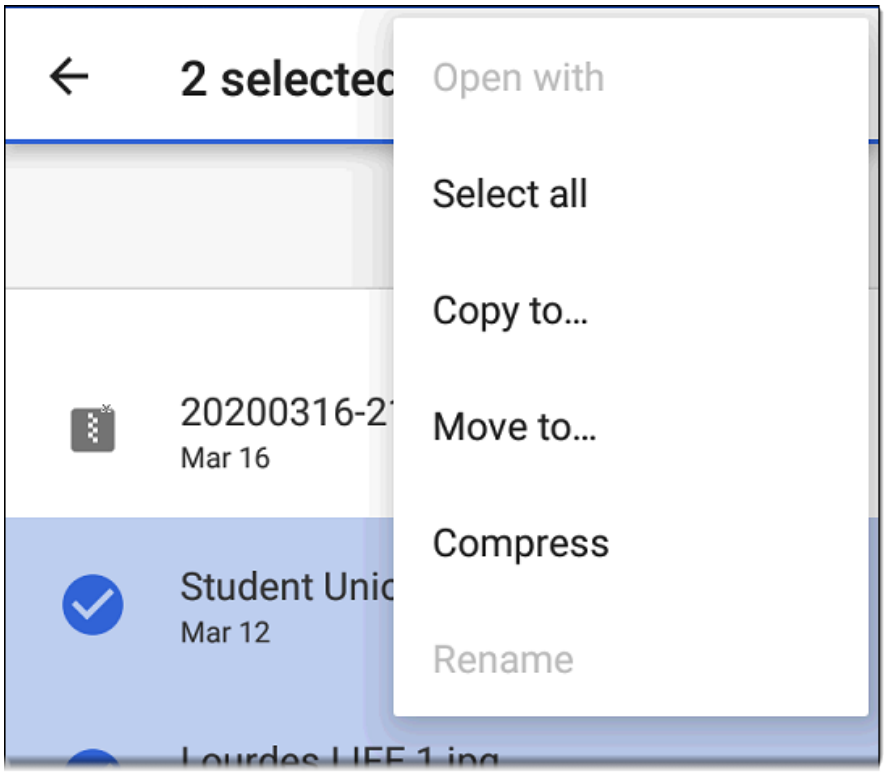
Touch and drag your finger or "swipe" up, down, left, and right to move through pages of the Home screen and applications, scroll up or down, and pull out navigation drawers and panels.

Long Pressing

Touch and hold or "long press" files or application icons to reveal additional operations.

For example, you can long press a file name in the Files Application to reveal the top toolbar with options for sharing, deleting, or moving the file.

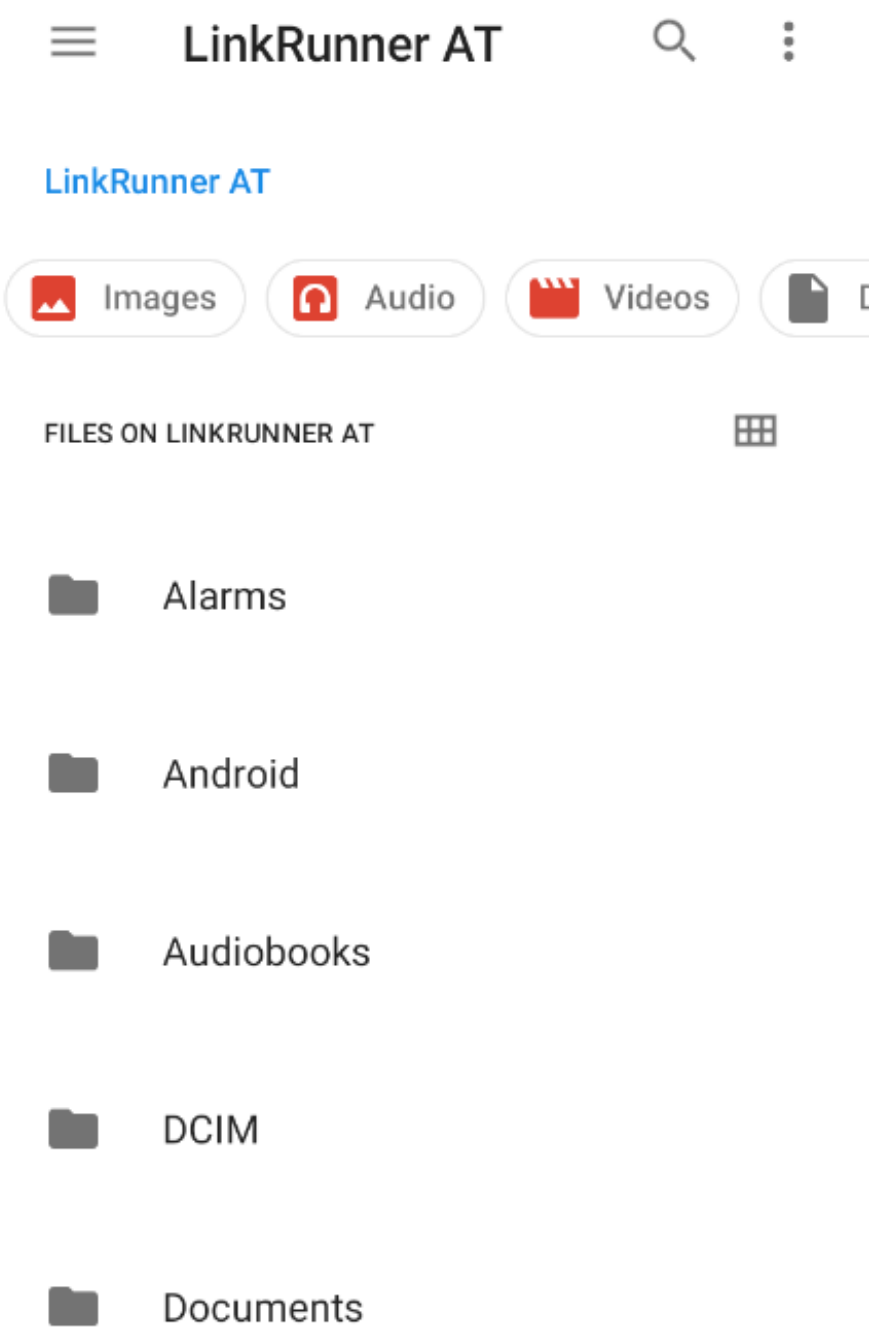
Additional options often appear in an overflow menu, designated by the action overflow icon .



You can also long press on text on most screens to open options for copying and sharing the text.

Left-Side Navigation Drawer

In the Files app, tap the Menu icon or or swipe right to open the navigation drawer. It displays the folders in your file system.



See the Navigation Drawer topic for additional information.

Back to Title and Contents

System Status Bar and Notifications

The Status Bar across the top of the screen displays notification icons from the system as well as LRAT 3000-4000-specific icons related to your network connections and test statuses.

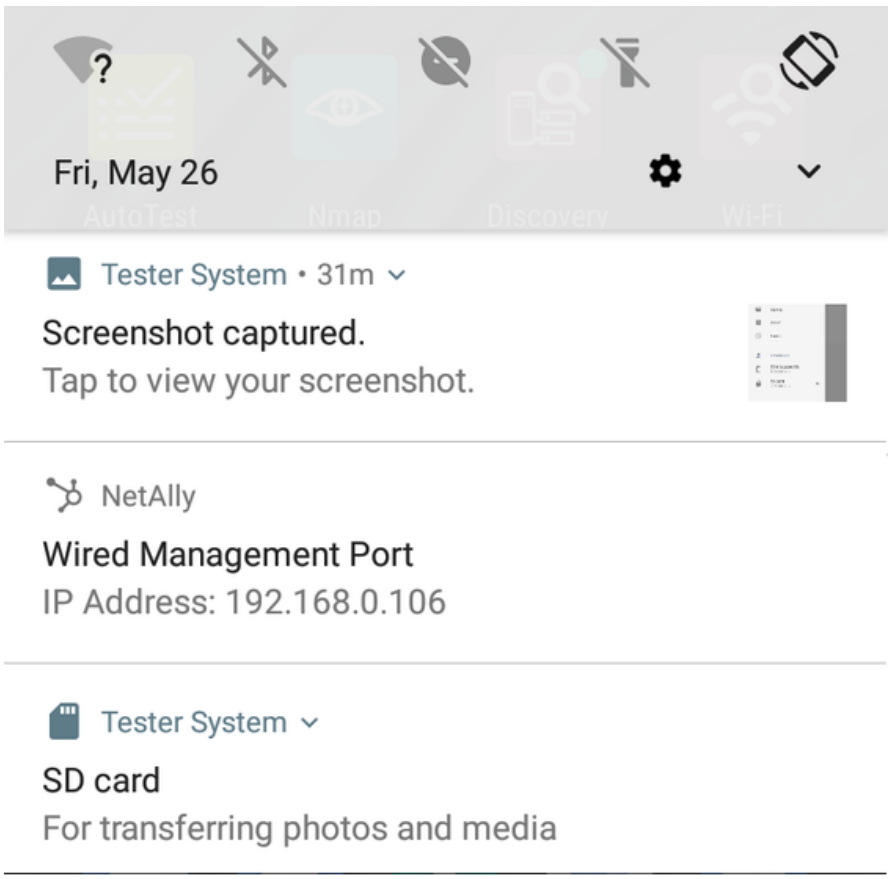
See Test and Port Status Notifications for details about the icons and notifications related to LRAT 3000-4000 network connections, testing, and management.

Tap and swipe down on the Status Bar to open the Notification Panel.

Notification Panel

The Notification Panel contains notifications from your device, such as downloads and installs, inserted hardware, captured screenshots, app and connection statuses, and updates. The panel also displays common system settings icons for quick access.

Swipe (touch and drag) downwards on the Status Bar at very top of the screen to slide down the Notification Panel.



- Tap the title and down arrow ⌄ on a notification (or swipe down on it) to expand the box and view more details or options.
- Tap the middle of a notification to open the related app, image, or device settings or to perform other related actions.
- Swipe left on a notification to dismiss it.

NOTE: Because they are essential to the LRAT testing functions, you cannot dismiss the test and management port-related test and port status notifications.

- Tap **CLEAR ALL** at the lower right of the panel to dismiss all system notifications.

Apps Screen and Store

To access the apps that are not shown on the Home screen, swipe up on the Home screen or tap the up arrow icon ^.

The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.

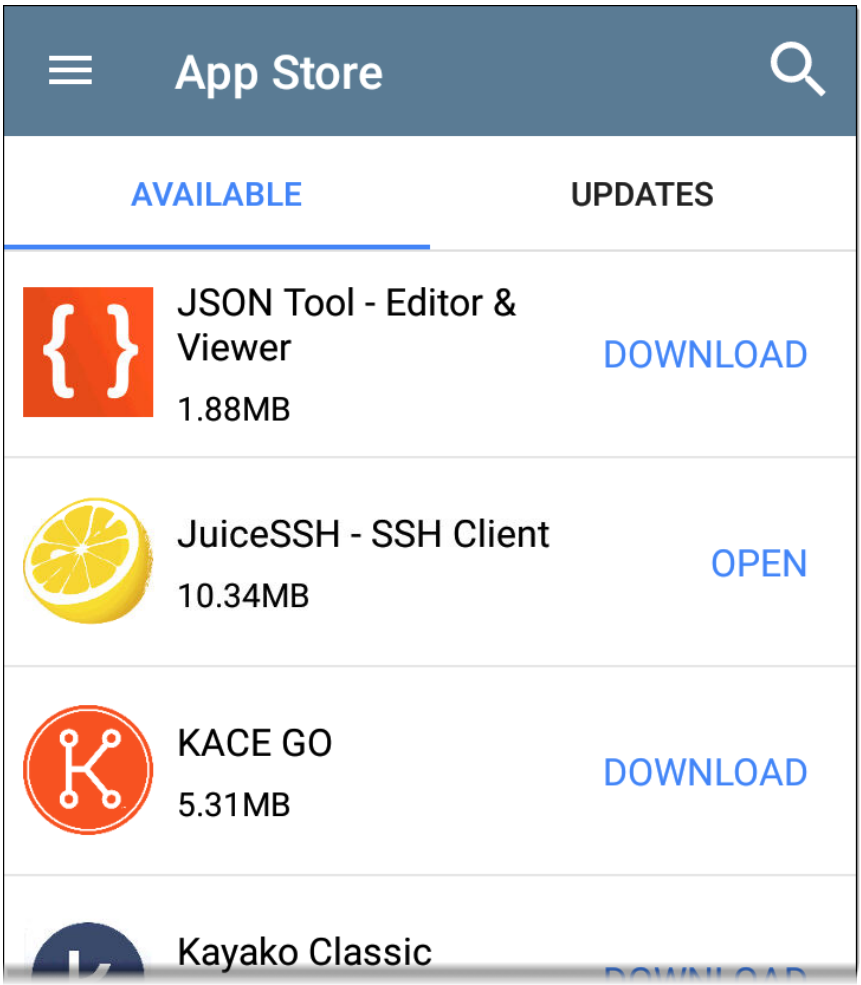
- Tap an app's icon to open the app.
- Hold and drag an icon upwards to add it to your Home screens.
- Touch and hold (long press) an icon to view App Info or access widgets you can add to the Home screen and other actions you can perform.

App Store

NOTE: The LRAT-3000 requires that you register your product before you can access the App Store.

From the Home Screen or Apps Screen, open the NetAlly App Store to download third-party

system applications to use on your LRAT 3000-4000.



NOTE: Your unit must be "claimed" to Link-Live Cloud Service at Link-Live.com to access the App Store.

- Tap the search icon to search for an App.
- Tap **UPDATES** to view available updates of installed apps.

- To request that an App be added to the App Store, visit the Apps ▶ page at Link-Live.com, and select the floating action button (FAB) at the lower right corner to
  - **Request** or **Upload an App**.

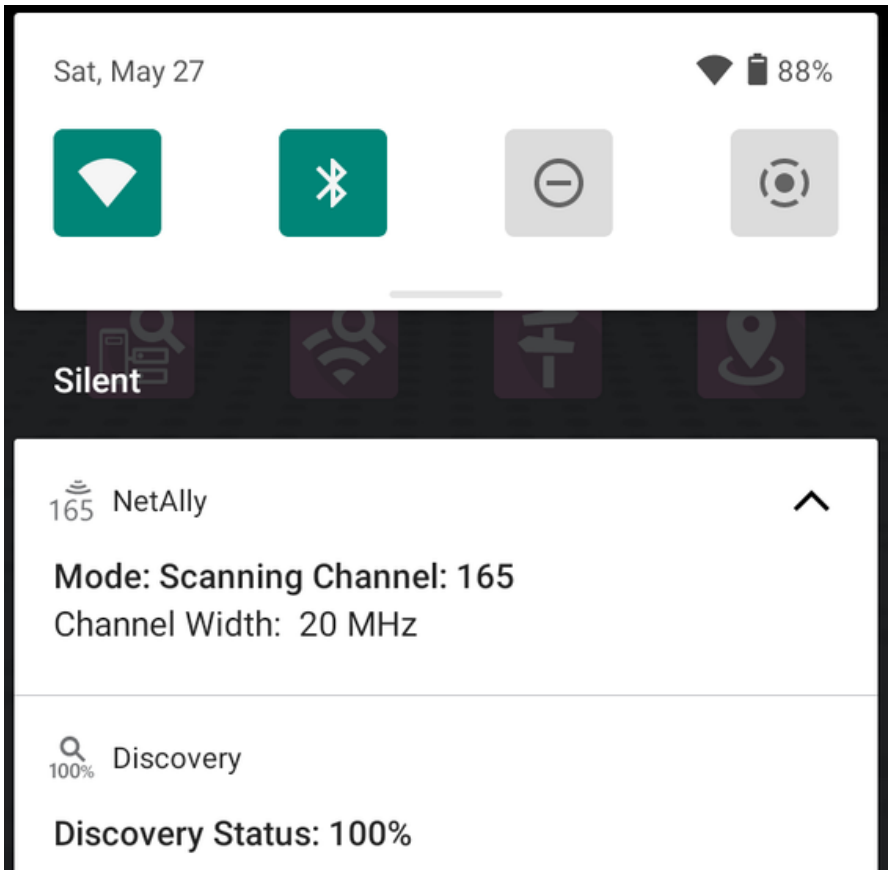
Device Settings

To access the system device settings, tap the Settings  icon at the bottom of the Home screen.

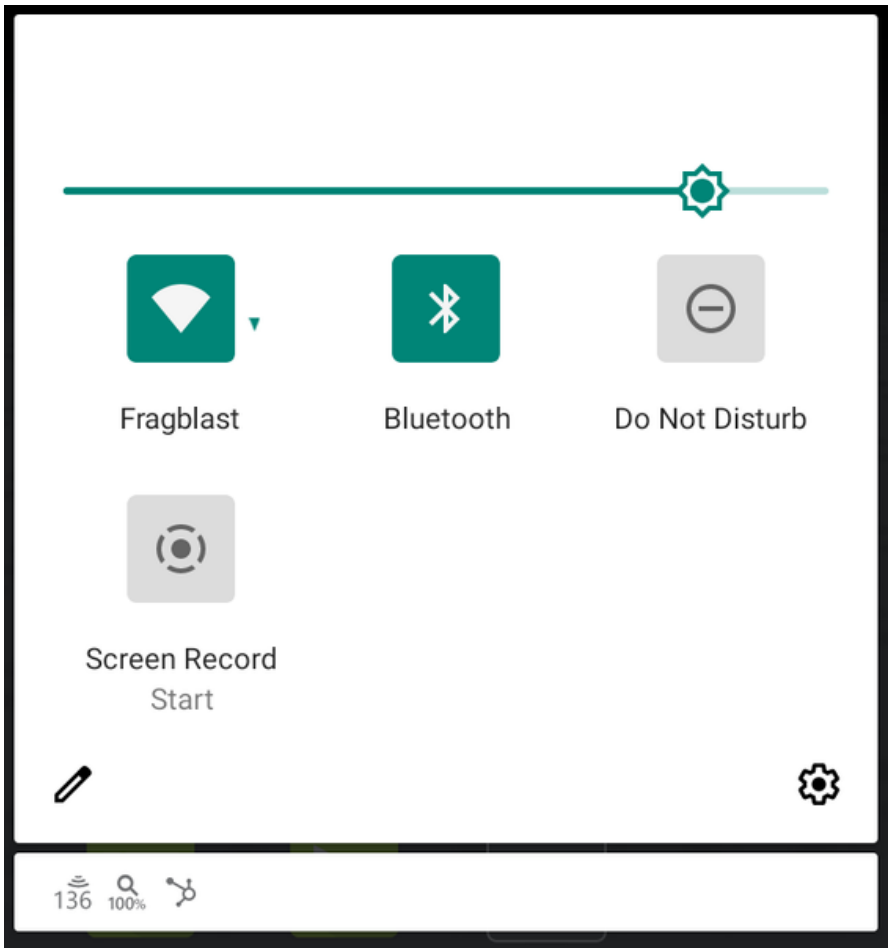
The device settings screen lets you adjust the display; adjust sound ; set date and time; view installed applications and memory devices; or reset to factory defaults.

Quick Settings Panel

You can also access some of the most common device settings from the Quick Settings Panel by swiping down from the Status Bar at the top of the touchscreen.



Swipe down twice to open the full Quick Settings Panel.



- Touch and drag the slider control at the top of the panel to adjust the screen's brightness.
- Tap an icon in the panel to enable or disable the corresponding feature.
- Touch and hold an icon to open the relevant device setting screen, if there is one.

Auto Power Off

Activating the Auto Power Off function helps to extend the battery run time.

1. From the Device Settings  , select **Display**.
2. On the Display settings screen, tap **Device auto power off**.
3. In the pop-up dialog box, select how long you want the unit to remain On with no activity occurring. The unit automatically powers off after the selected period of inactivity has passed.

Similarly, you can adjust the setting that controls when the display goes into **Sleep** mode from the **Display** settings screen.

Language

Your device supports Chinese, English, German, Japanese, and Korean language displays. See Changing the Device Language for information on changing the device interface language. The user guide is available in Chinese and English. See How to Use this Guide.

Using Wi-Fi Adapters

The LRAT does not support Wi-Fi or Bluetooth. Either service shuts down immediately if you try to enable it using the system interface. However, you can connect to Wi-Fi using a supported external USB adapter, which you must purchase separately.

When in use, the USB-to-Wi-Fi adapter behaves like another network connection.

For additional information, see Supported Wi-Fi/Bluetooth Adapters.

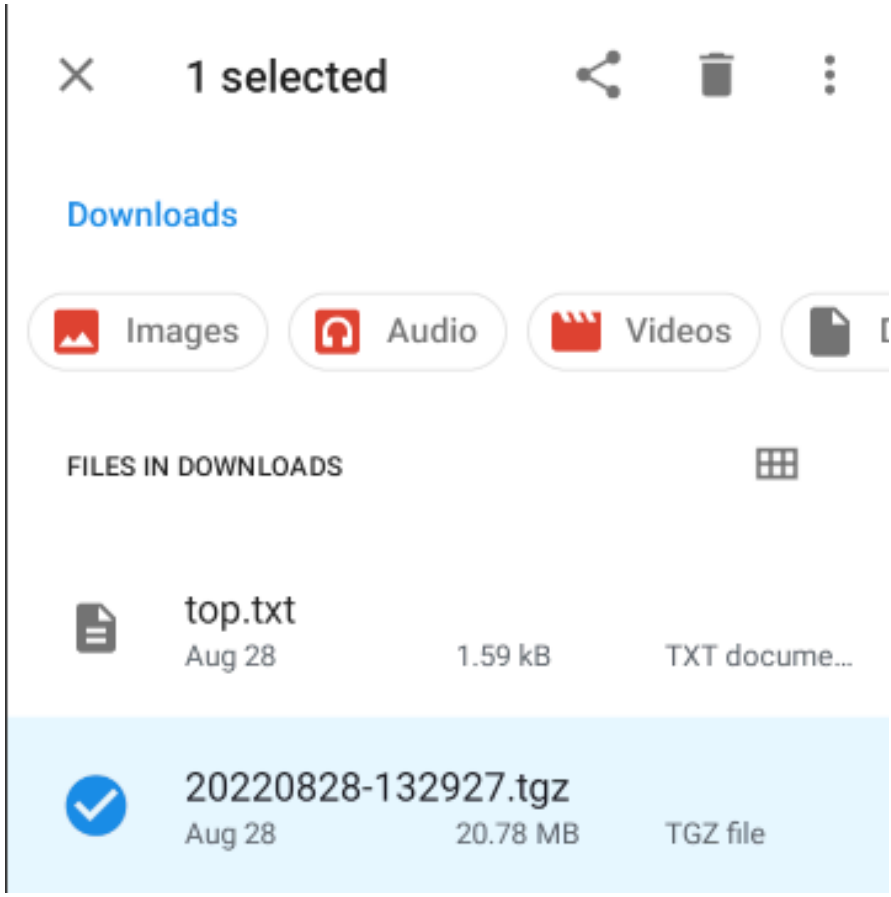
Back to Title and Contents

Sharing

The system Files app lets you share files from internal or external storage to a printer, or the Link-Live cloud service. You can upload one selected file or multiple files at once.

NOTE: Many apps on your unit allow you to save settings and configuration information directly to Link-Live. See Saving App Settings and Configurations.

1. On the Home Screen, open the Files app by tapping the icon .
2. Navigate to the folder containing the files you want to share using the Navigation menu or the left-side navigation drawer.
3. Long-press on one or multiple files to select.



4. Tap the share icon in the top toolbar to open the Share pop-up dialog.
5. Tap to choose a sharing method and follow the system prompts to share the file or files.
6. (Optional) If uploading to Link-Live:
   a. Tap the **Link-Live** option.
   b. Enter any **Comments** you would like attached to your file.

c. Select **SAVE TO LAST TEST RESULT** or **SAVE TO UPLOADED FILES**. Your files are then uploaded and viewable on Link-Live.com.)

d. See the Link-Live chapter for more information on using Link-Live with your LRAT 3000-4000.

Sharing a Screenshot

To take and share a screenshot:

1. Press and hold the **Power** button and the **Volume Down** button at the same time for one second. (See Buttons and Ports for button locations). The unit beeps and adds a notice to the Notification Panel.
2. Access the file either by opening the Notification Panel and tapping the screenshot notice or by using the Files app.
3. Follow the Sharing procedure to share the image using Link-Live, Bluetooth, or another configured application.

Changing the Device Language

The LRAT 3000-4000 supports Chinese, English, German, Japanese, and Korean language displays.

To change the device's interface language:

1. Go to the Device Settings screen by tapping the Settings  icon at the bottom of the Home screen.
2. Scroll to and select **System**.
3. Select **Languages & input** and then **Languages**. This displays the Language preferences screen.
4. On the Language preferences screen, select **+ Add a language**.
5. Tap the language option you want. This returns you to the Language preferences screen.
6. Touch and hold the icon  to the right of the language, and then drag the language to

the top (number 1) place on the list.

The LRAT displays the chosen languages, as available, in the priority order shown on the Language preferences screen.

NOTE: This user guide supports Chinese and English. If you choose German, Japanese, or Korean as the device language, the system uses the English user guide. See How to Use this Guide for more information about the user guide.

NOTE: Manuals are also available for web download at: https://www.net-ally.com/support/user-guides/

Back to Title and Contents

LRAT 3000-4000 Settings and Tools

The LRAT 3000-4000 features a common set of tools and General Settings that apply to multiple NetAlly apps and testing behaviors. This chapter covers settings, icons, and notifications *specific to LRAT 3000-4000*.

(See the Device Settings topic for information on the system settings.)

Access common settings and informational screens for the NetAlly testing apps (like AutoTest or Capture) by opening the left-side Navigation Drawers  or Settings  .

Navigation Drawer

Many system apps, including the NetAlly test apps, contain additional settings, tools, and information in a "navigation drawer" that slides out from the left side of the screen.

To open the navigation drawer:

- Tap the menu icon  at the top left of one of the testing application screens.
- Touch and drag (swipe) to the right from the very left side of the app screens.

As an example, the AutoTest navigation drawer (above) provides access to the enabled AutoTest profiles, AutoTest Settings, General Settings, and the About screen.

Settings for each specific app are described in the chapter for the app.

About Screen

The About screen displays the model number, serial number, MAC addresses, software versions, SFP details, and current AllyCare contract status for your LRAT 3000-4000.

If a **User-Defined MAC** is enabled in an NetAlly apps' General Settings or in the Wired Profile Settings, (User-defined) appears next to the MAC address on the About screen.

Exporting Logs

The About screen contains the Export Logs function, which allows you to save your unit's logs for analysis by NetAlly's technical support team.

Tap the **EXPORT LOGS** link to download a .tgz file to the Downloads folder on your unit. Open the Files app to transfer the file using email or another method. (See Managing Files.)

Import/Export for All Apps

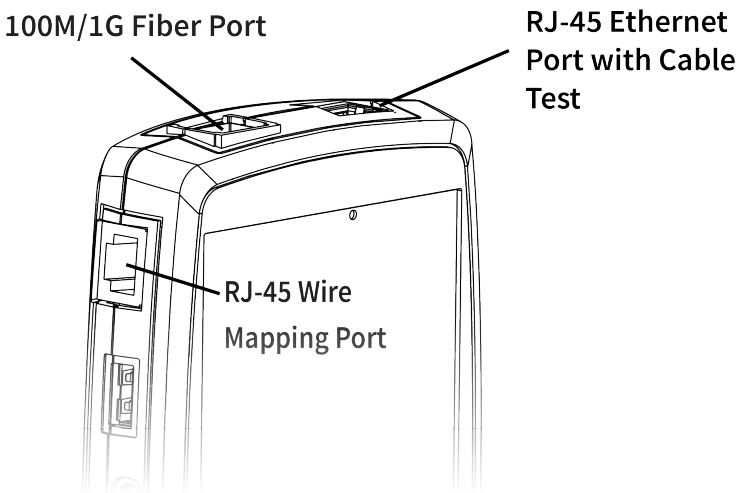
Tap the action overflow icon ⋮ on the About Screen to display a menu for importing or exporting of settings for *all* applications that allow import/export. See Import/Export Settings for details.

Restarting the Test Unit

To restart your test unit, tap the action overflow icon on the About Screen and select the **Restart Tester** option.) (This functions the same as holding down the power button and then tapping the **Restart Tester** option.)

Test and Management Ports

The LRAT 3000-4000 has two wired RJ-45 copper ports and a fiber port, each with specific test or management functions described in this section.



See the sections below for more information on the ports. Also see Buttons and Ports and the technical Specifications as needed.

Test Ports

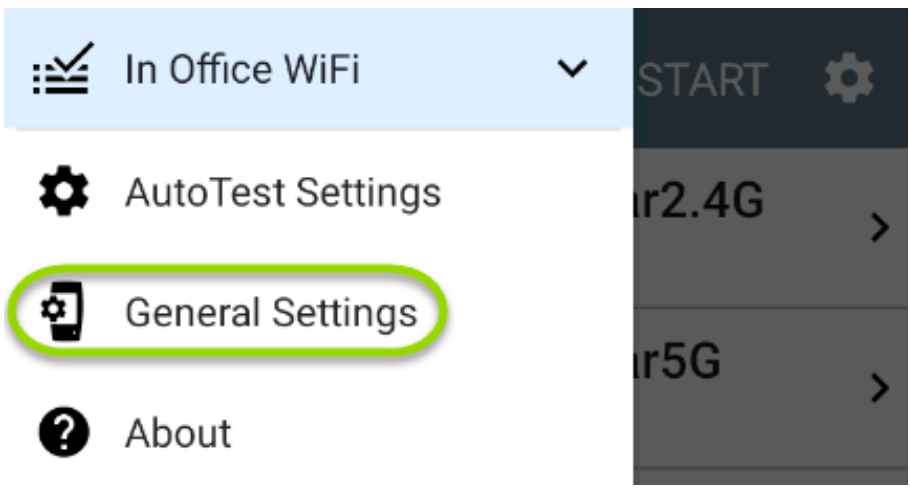
Wired Copper Test Port: The copper test port is the RJ-45 port on the top of the unit. To disable, unplug the connection.

Wired Fiber Test Port: The SFP and fiber test port is also on the top of the unit. To disable, unplug the connection.

LinkRunner AT 3000/4000 runs Wired AutoTests, Captures, Discovery, and other comprehensive network analysis apps over the test port.

You must also run an AutoTest Wired Profile to establish a link on the Wired test ports. If the AutoTest app is not currently open, the last Wired Profile in the profile list runs automatically when you power on the unit or LRAT detects a new copper link in the top Wired Test Port. Wired fiber connections must be started manually in the AutoTest app.

Note that the General Settings affect how you can use the test port. (The General Settings are accessible from the left-side navigation drawer from most NetAlly testing apps.)



 Management Port

LRAT can run Discovery, Ping/TCP Connect tests, Path Analysis, and iPerf tests on the management port, but not AutoTests

 **USB Wired Management Port**: You can use a USB-to-Ethernet adapter to run an alternative wired management port for your LRAT. This option allows you to set up a stable wired connection for system updates, updating software, communicating with Link-Live, AP uplinks, and for running basic wired tests that can help diagnose problems that may affect Wi-Fi devices.

> NOTE: NetAlly has tested many but not all USB-to-Ethernet adapters for compliance with the LRAT 3000-4000. The following adapters are supported:
>
> - j5create model JUE130 (USB 3.0)
> - StarTech.com model USB21000S
>
> For additional information, see Ethernet Adapters and Cameras.

Contact NetAlly support for more details if needed.

To set up the adapter interface:

1. Plug the adapter into one of the USB Type A ports on your device.
2. Connect the adapter to a network RJ-45 cable.
3. Verify that the LEDs on the adapter are on. This indicates that the connection is active.
4. Verify that the USB Wired Management Port is now listed as a management port in the Test and Port Status Notifications.

You can now use the USB Wired Interface in the following applications:

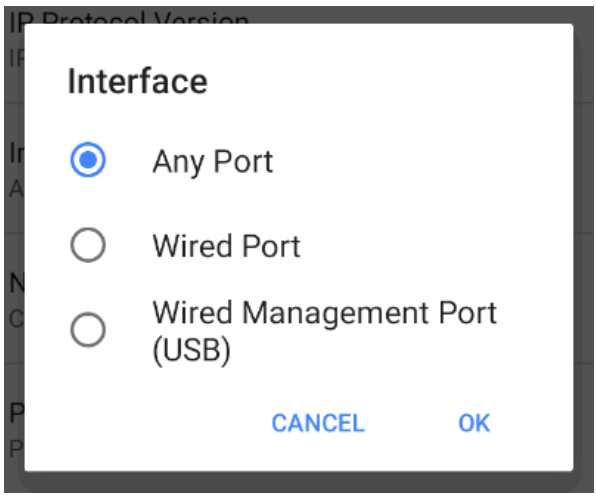
- Discovery (Active Discovery Ports and TCP Port Scan)
- Ping
- Path Analysis

See Selecting Ports below for more information.

Selecting Ports

Some of the individual NetAlly testing apps let you select which port interface to use for tests or analysis.

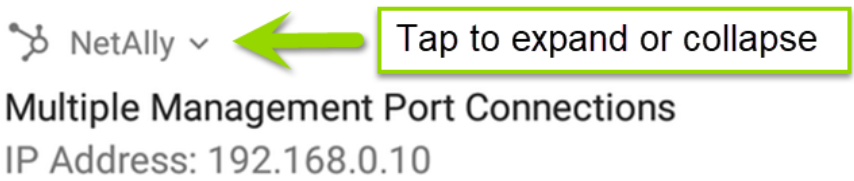
To change the port, tap an app's settings icon to display the settings screen. Then tap **Interface** to select the port from a dialog.



Test and Port Status Notifications

LRAT 3000-4000 shows notifications from the NetAlly testing apps and unit ports in the top Status Bar and Notification Panel. Swipe down on the Status Bar to view the notifications.

On each notification, you can tap the title and down arrow to expand the box and view more details or options.



Various LRAT icons appear in your Status Bar, as listed in the following sections.

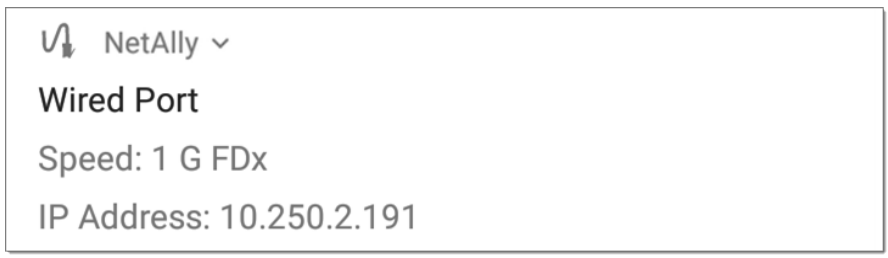
> NOTE: Read Test and Management Ports for descriptions of the port functions.
>
> See General Settings for settings that control port functions.

Test Port Notifications

Active network connections on the test ports are established using the AutoTest app.

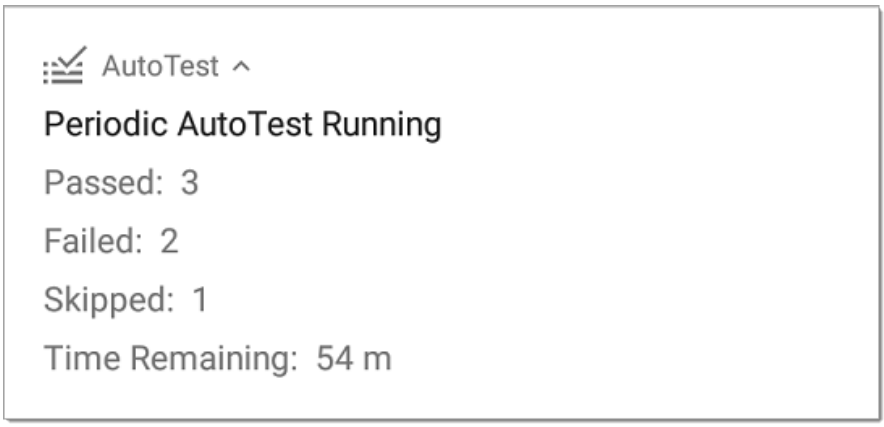
 You can set up a **Wired Test Port** connection (called the "Wired Port" in app settings) by running an Auto Test Wired profile.

> NOTE: If both the fiber and top copper ports are connected to an active network, the LRAT uses the fiber link as the "Wired Port" for testing.



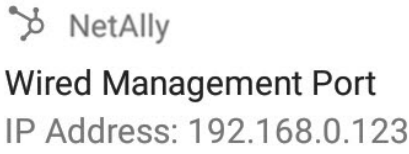
 **Periodic AutoTest** is running or has completed. When Periodic AutoTest is running, the Wired Test Port may not be available to other testing apps.

> NOTE: Periodic AutoTest is available for the LRAT-4000 only.



Management Port Notifications

You can establish a **Management Port** connection through an optional USB-to-Wi-Fi adapter.



The alternative **Wired Management Port** connection can be established through the optional USB-to-Ethernet interface. Its details are displayed under the system Management Port notifications. See USB Wired Management Port for more information.

If your Management connection is lost, the following notification displays.

Discovery Notifications

NOTE: This application applies to the LinkRunner AT 4000 only.

The Discovery notifications show the progress of the discovery process. See the Discovery app chapter for more information.

The active discovery process is running and has progressed to the specified percentage.

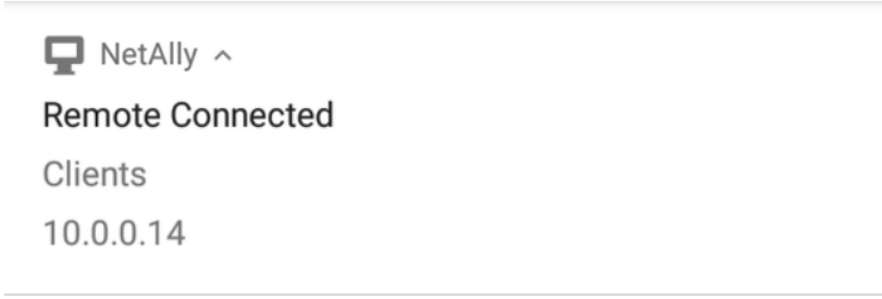
No links are currently available for active discovery, either because none of the ports enabled for discovery are connected or AutoTest is running. Discovery is temporarily disabled when AutoTest is running.

PoE

Indicates that your unit is connected to a Power over Ethernet source. See PoE Charging for more information.

VNC/Link-Live Remote

 A remote VNC connection is active through a standalone VNC client and/or the Remote function in Link-Live Cloud Service.

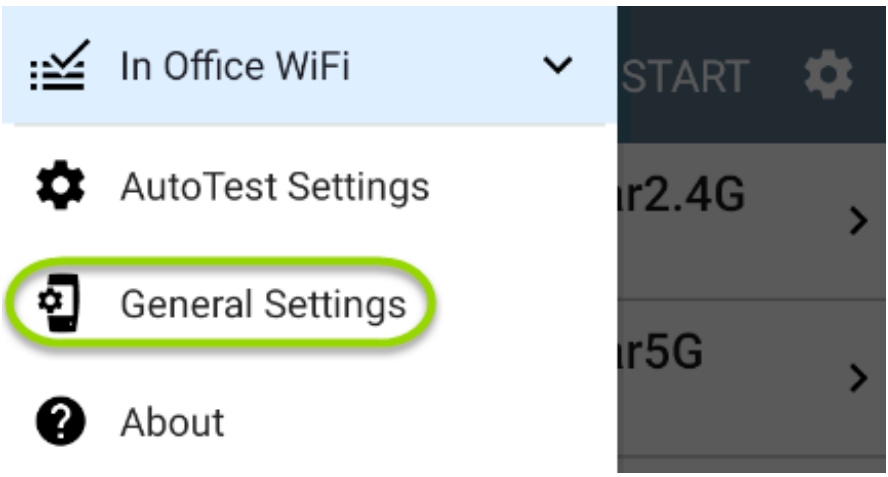


Back to Title and Contents

LRAT 3000-4000 General Settings

LRAT's General Settings control test and management-related connections that affect multiple test apps.

Access the General Settings from the left-side navigation drawer in the NetAlly testing apps, such as AutoTest, Discovery, Capture, iPerf, etc.



See also Test and Management Ports and Test and Port Status Notifications for related information on port functionality and status icons.

Wired General Settings

Wired General Settings control functions of the Wired Test Port.

Test PoE before Link: By default, an AutoTest Wired Profile performs the Link test before the PoE test can complete. Enable this setting to make your LRAT complete the PoE test before the Link test. Enabling this setting forces PoE negotiation to be completed before establishing link, improving compatibility with some switches.

Charge Battery via PoE: (Available if supported by tester hardware.) This setting is enabled by default. If you do not want your LRAT unit to charge when connected to a switch with PoE, tap the toggle button to disable. An AutoTest Wired Profile must run and detect PoE availability before the unit can use it for charging.

See also PoE Charging.

Receive Only: Enable this setting to prevent the LRAT from transmitting packets on the Wired Test Port. You can also use the **Stop After** function in Wired AutoTest Profile Settings to

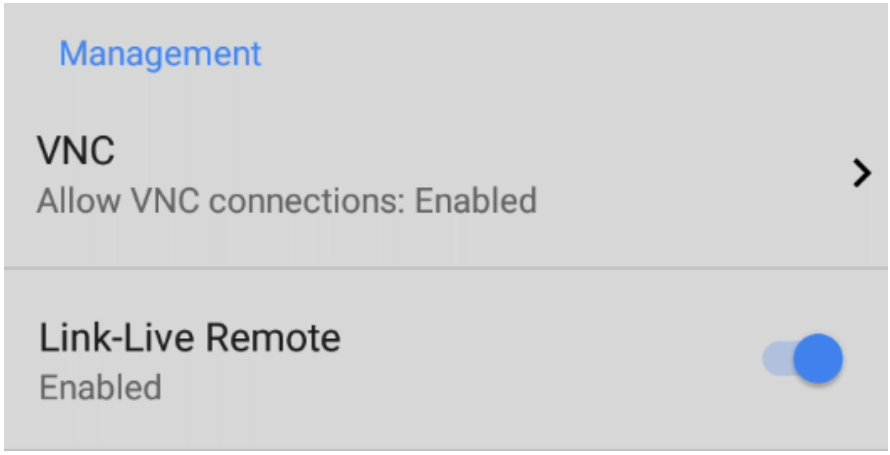
hide the AutoTest cards that require transmit capability. Set the AutoTest **Stop After** setting to **Switch**. Otherwise, when **Receive Only** is enabled, the Wired DHCP/Static IP test shows a Result Code of "Interface is configured to only receive packets," and the subsequent tests do not run.

User-Defined MAC: This setting affects the Wired Test Port only. Tap the toggle switch to enable a user-defined MAC address. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. Tap the lower field to enter your desired MAC address for the LRAT. When a User-Defined MAC is enabled, **(User-defined)** appears next to the MAC address on the About screen and on relevant test result screens.

> NOTE: This definition can be overridden by a profile-based user-defined MAC. See Wired Connection Settings for more information.

Management

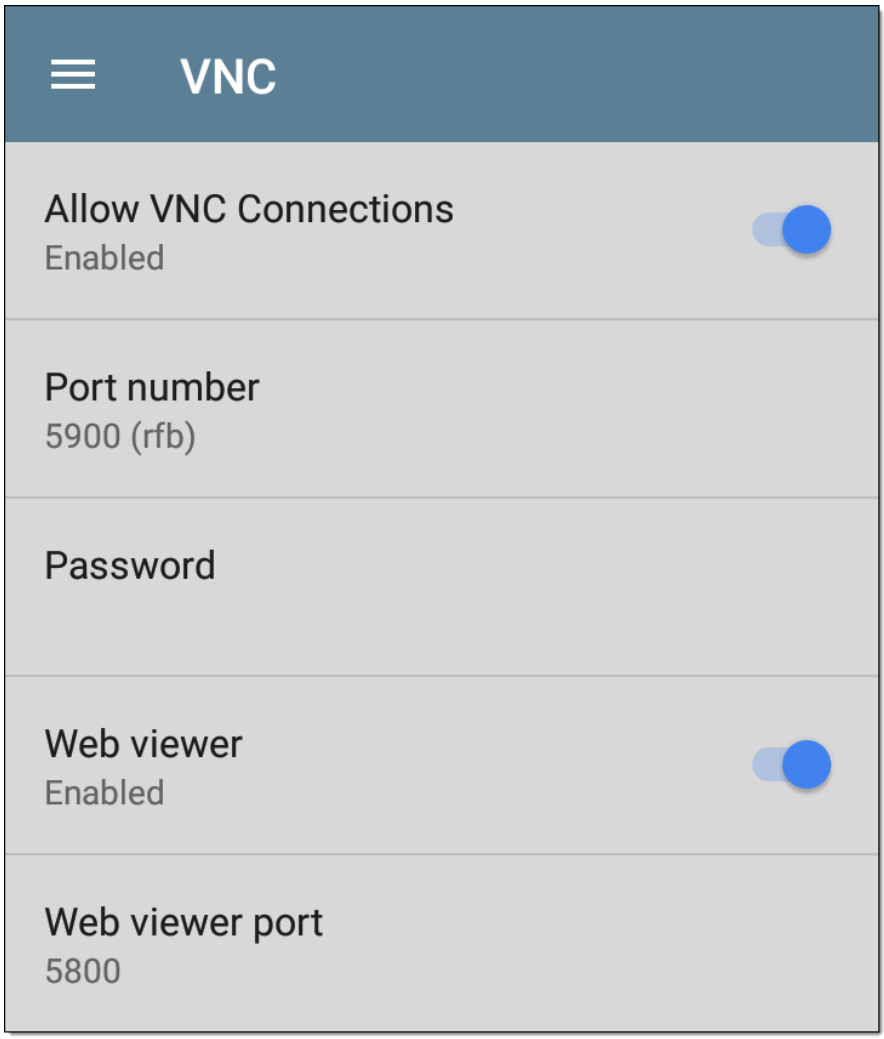
These settings affect management-related functions on the LRAT, including remote access.



VNC

Tap **VNC** to open the VNC settings screen and configure your unit's VNC connections for remote operation.

See Using VNC for more information about connecting to a VNC client or Link-Live Remote.



Allow VNC Connections: (Disabled by default.) Tap the toggle button to enable remote connections from VNC clients and display VNC options.

Port number: Tap to enter a port number other than the default.

Password: Tap to enter a password, which a VNC user must enter to access the LRAT interface remotely.

NOTE: If you set a **Password** here in the **VNC** settings, the password is required to connect to both a standalone VNC client and the Remote feature at Link-Live.com.

Web viewer: Tap the toggle to enable or disable web viewer access.

Web viewer port: Tap to enter a port number other than the default.

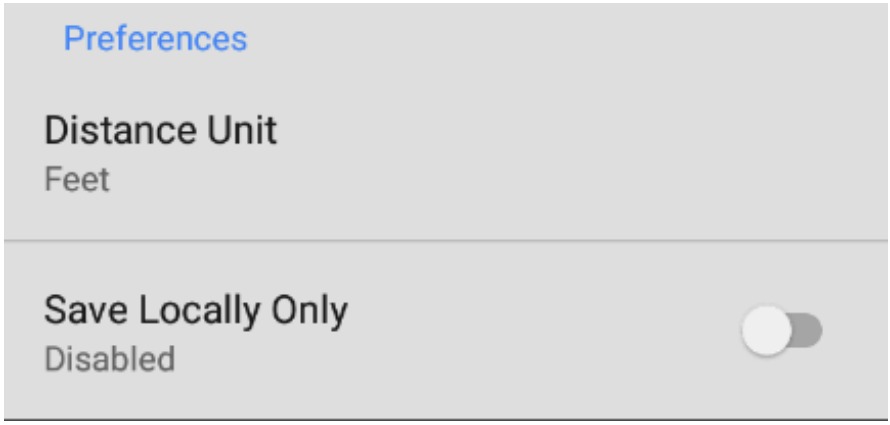
Link-Live Remote

This setting enables or disables the LRAT's remote control function in Link-Live Cloud Service at Link-Live.com.

NOTE: The Link-Live Remote feature is only available to customers with an active **AllyCare** subscription. Your LRAT must be claimed. See NetAlly.com/Support for more information.

Access the Remote function on the **Units** page at Link-Live.com by selecting the claimed LRAT 3000-4000.

Preferences



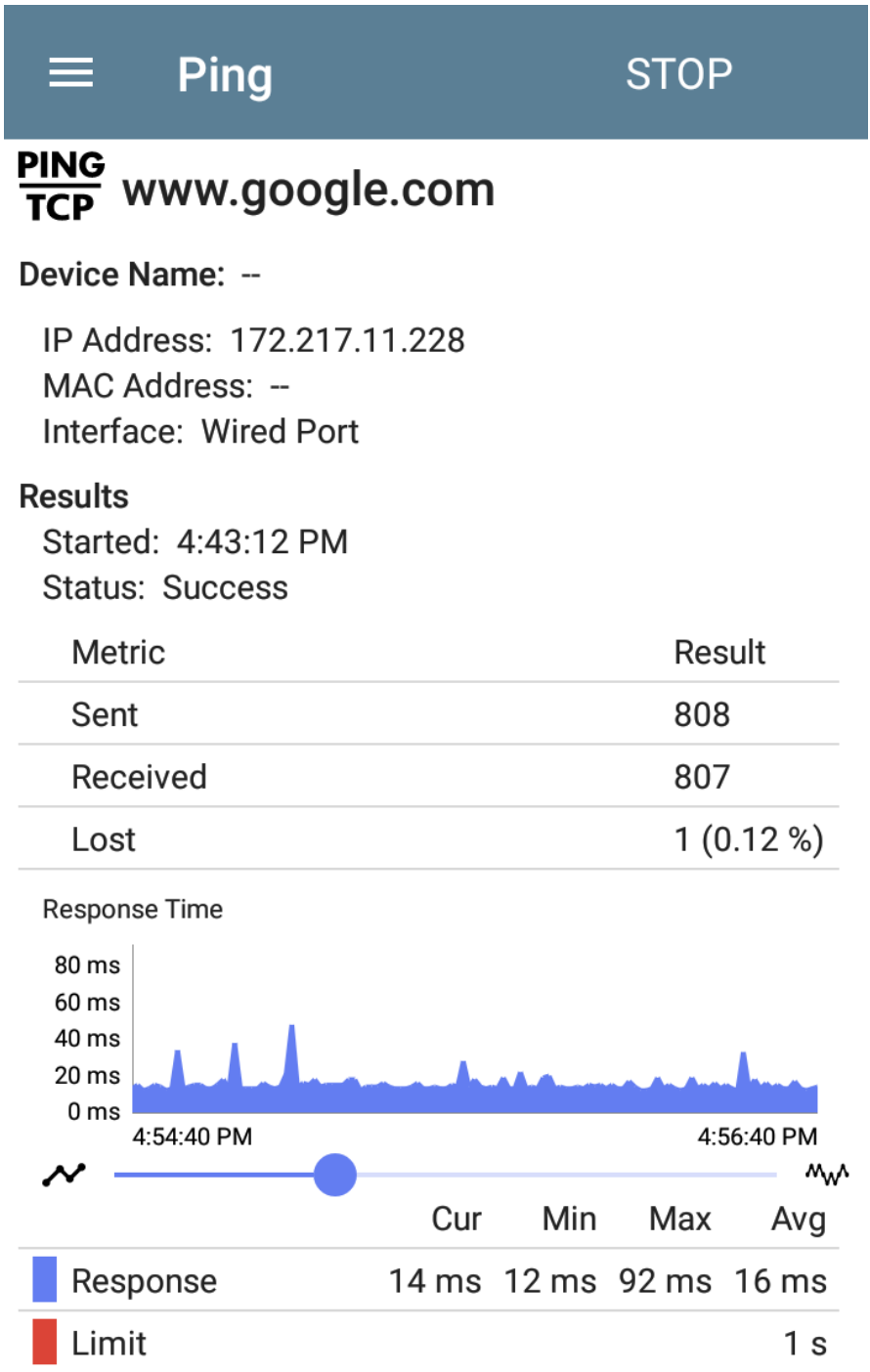
Distance Unit: This is the unit LRAT uses for distance measurements in the testing apps, specifically Cable Test. Tap the field to switch between Feet and Meters.

Save Locally Only: Tap this toggle field to change the unit default behavior for saving files. (The default is to give you the option to save to Link-Live *or* locally.)

Back to Title and Contents

Trending Graphs

Many of the LRAT 3000-4000 testing apps feature time-based line graphs of recorded measurements, which you can pan and zoom to view different time intervals. For example, the image below shows the Response Time graph from the Ping Test Results Screen.

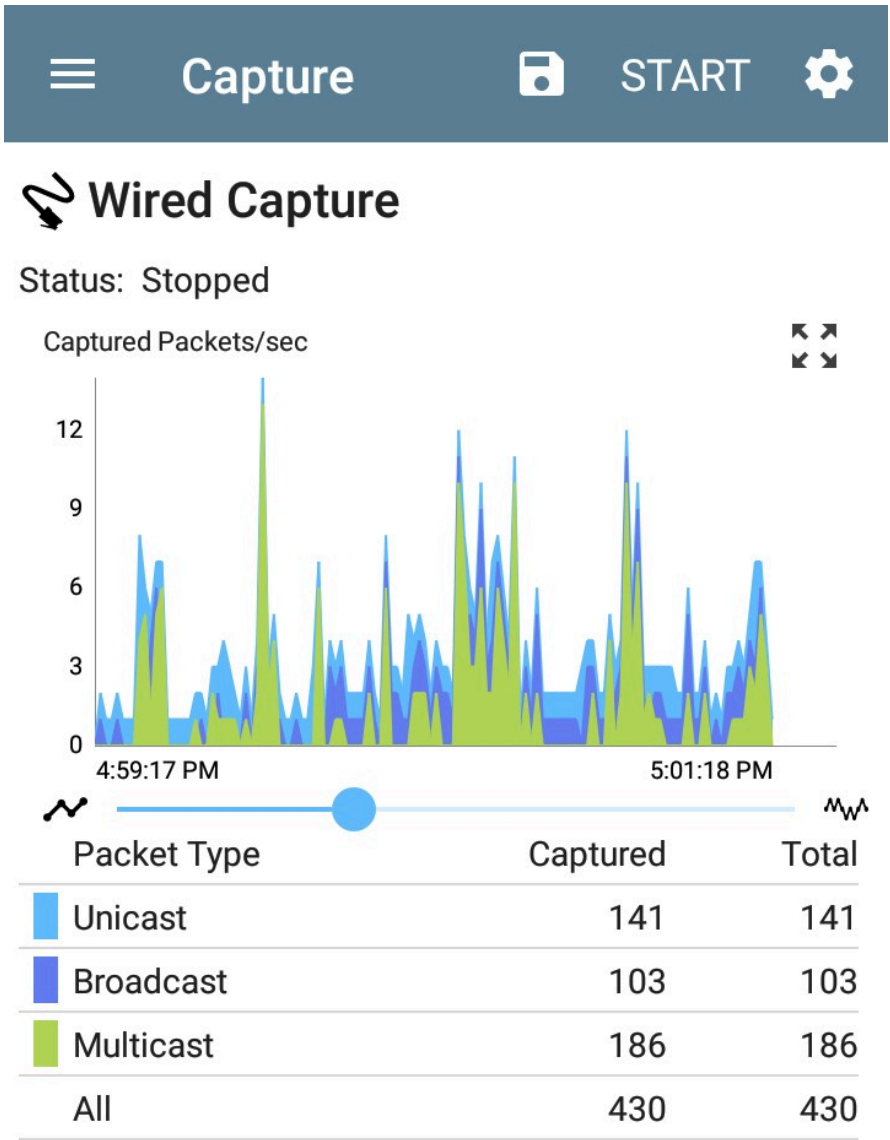


d

The graphs update in real time and then save and display data for up to 24 hours (depending on test type and/or link status).

A legend indicates the measurements that correspond to each plotted color.

For another example, the image below shows the Capture app graph.



- To pan, or move backward and forward in time, touch and drag (swipe) left and right on each graph.

- To zoom in on a specific point, double tap the point on the graph. The view zooms in 2x (or displays half the amount of time) for each double tap.
- To zoom in or out, decreasing or increasing the time interval displayed, drag the slider or tap the slider bar below the graphs.
  - The largest time interval (maximum zoom out) is the total time data has accumulated.
- To reset the graph to the default time interval, tap the zoom reset icon  .
  - The zoom reset icon appears *after* you zoom or pan on the graph.
  - The default time interval varies across different apps.

The following apps and screens contain trending graphs:

- Ping/TCP – Ping Test
- Capture (LinkRunner AT 4000 only)
- Discovery – Interface Statistics (LinkRunner AT 4000 only)
- iPerf (LinkRunner AT 4000 only)

Common Icons

The icons below appear in multiple NetAlly test and system apps.

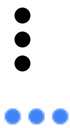
Menu Icon - opens the left navigation drawer or other menus

Refresh Icon - restarts testing and measuring on the current screen

Settings Icon - opens configuration options for the current app

Save Icon - saves settings or files or loads saved configurations

Floating Action Button (FAB) - opens the Floating Action Menu, which contains additional actions



Action Overflow Icon - contains additional actions

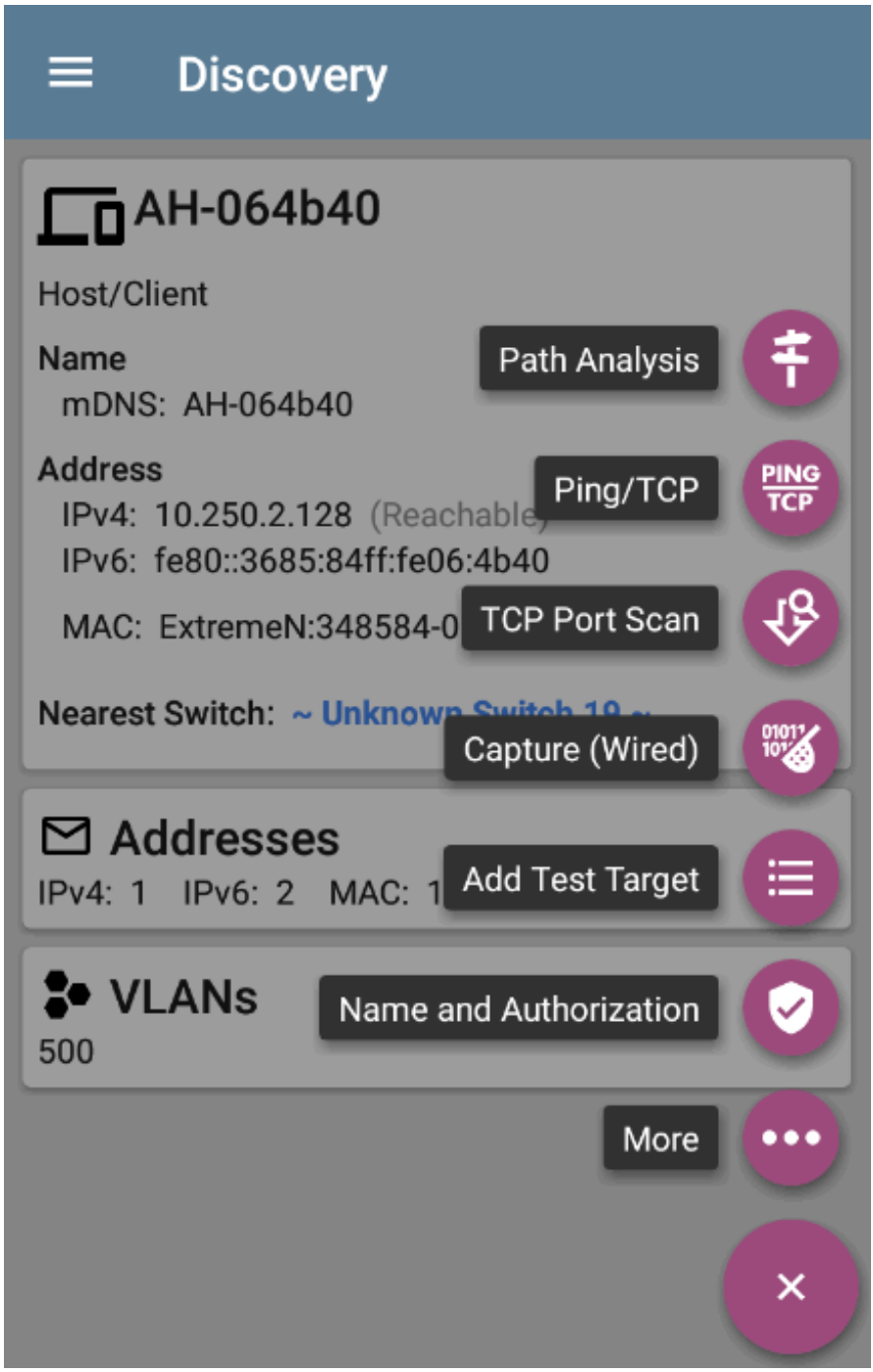
Directional Arrows (or Carets) - indicate the ability to "drill in," open a screen, or expand a panel for more detailed information, or to change the order of a list

For explanations of the LRAT icons that appear in the Status Bar at the top of the screen, see Test and Port Status Notifications.

Floating Action Button (FAB) and Menu

Many system applications, including NetAlly's AutoTest and Discovery apps, feature a Floating Action Button or "FAB"  that opens a floating action menu with more options for analysis.

The FAB on the Discovery app's Details screen opens other apps for further testing of the selected device.



See the chapter for each app for descriptions of the FABs specific to that app. For example, see Discovery App Floating Action Menu describes the Discovery FAB in more detail.

Common Tools

Web Browser/Chromium

Some of the testing apps, like AutoTest, Ping/TCP, and Discovery, give you the option to **Browse** to internet addresses using a web browser application. LRAT has the Chromium browser pre-installed.

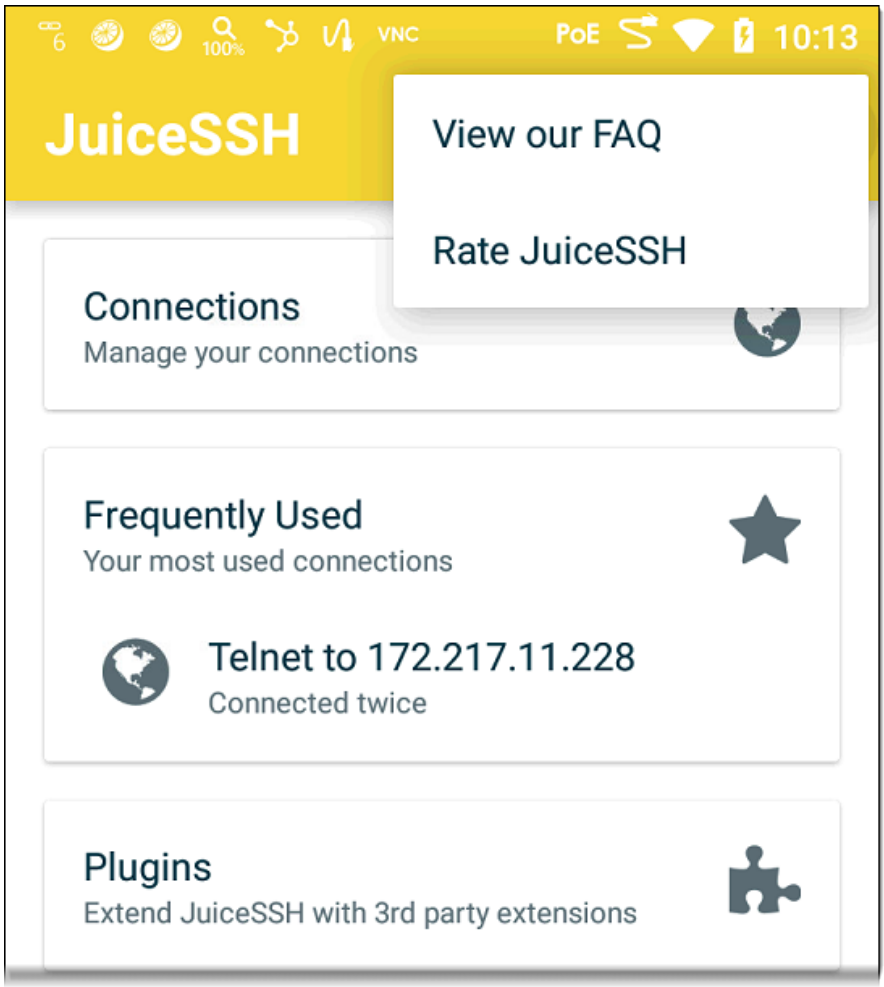
Telnet/SSH

The JuiceSSH  application pre-installed. Both the AutoTest and Discovery apps provide links to start a Telnet or SSH session using the current device address. Selecting these options opens JuiceSSH and starts a session. You can also open JuiceSSH from the Apps screen.

The JuiceSSH app maintains a list of previous connections. When opened from a NetAlly app, JuiceSSH uses the first connection in the list that matches the IPv4 address or device name and type. If no match is found, a new connection entry is created and used.

As a third-party app, JuiceSSH contains its own tutorials. For additional help, tap the action

overflow button ⋮ at the top right of the JuiceSSH app screen, and select **View our FAQ**.



Back to Title and Contents

Back to Title and Contents

Software Management

This chapter explains how to save and transfer files, reset app and device defaults, update your software, and remotely access your LRAT 3000-4000.

Tap a link below to skip to a topic:

Managing Files

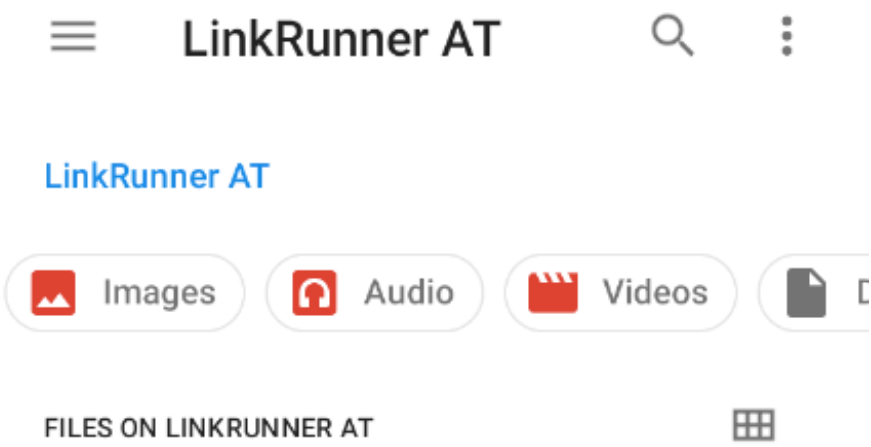
The LRAT 3000-4000 operating system, images, documents, and other files reside in a folder system, where you can copy, move, and paste them between folders or to external storage locations.

See also Sharing.

Files Application

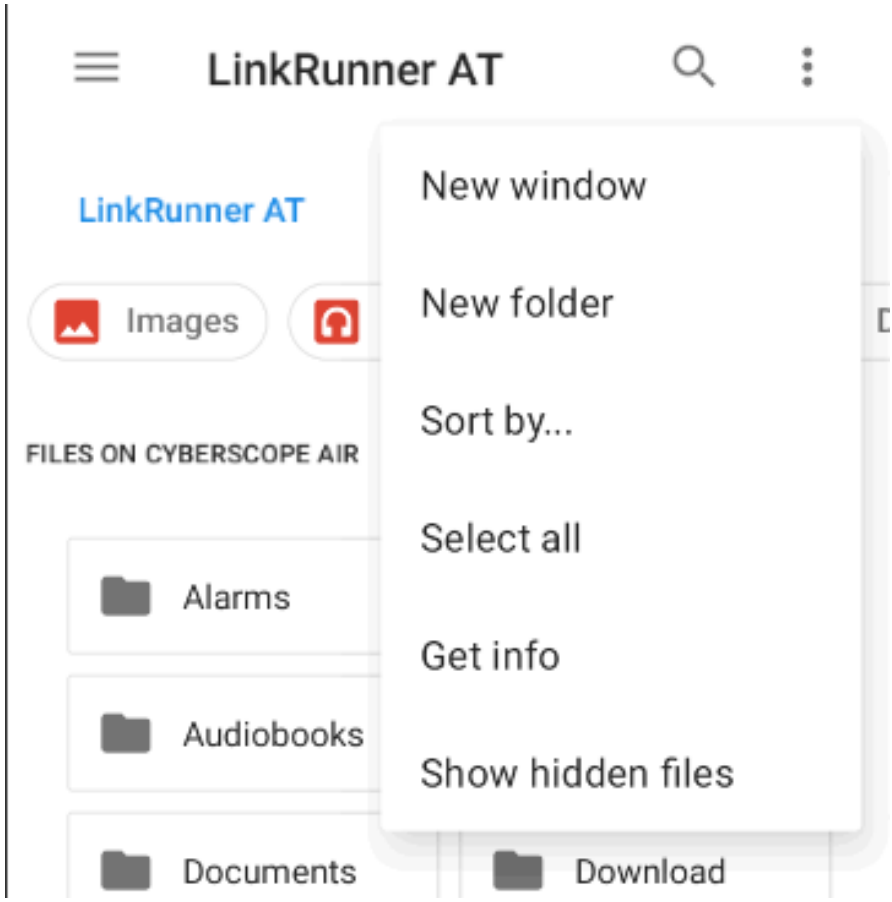
The Files app allows you to access the files saved on your LRAT. Tap the icon at the bottom of the Home Screen (or from the Apps screen) to manage your files.

> NOTE: To select the device sub-folders in the Files app as shown below, you may need to open the navigation drawer by swiping from the left side of the screen or by tapping the navigation icon at the top left and then tapping the **LinkRunner AT** folder.

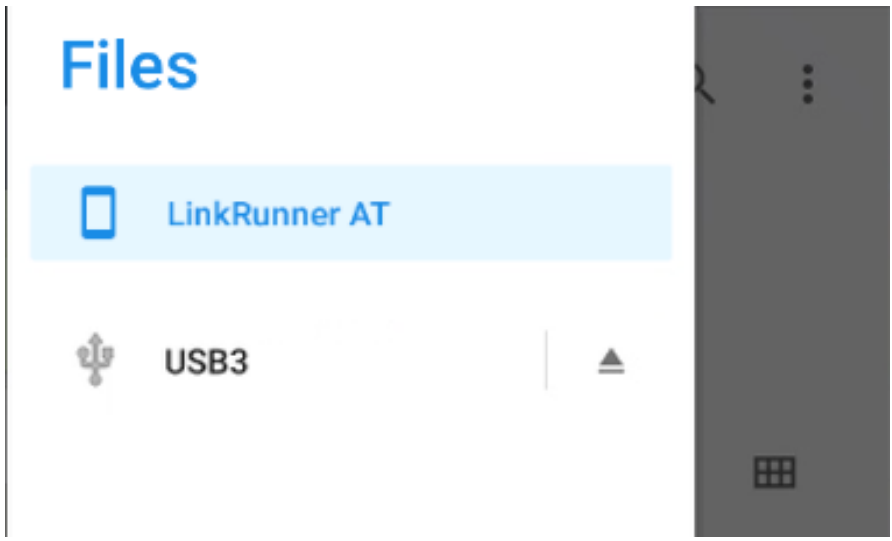


- Tap a folder or file to open it.
- Long press on folders or files to select multiple and to view additional file management operations in the top toolbar, including the Share and Delete buttons.

- Tap the action overflow icon to see even more actions, such as to create a new folder, move a file, delete an item, and to show or hide the main internal storage folder.

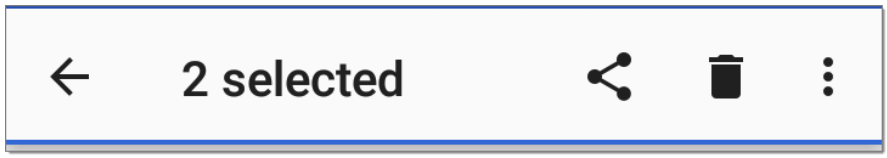


- Open the left-side navigation drawer to easily navigate through the top-level folders and attached storage devices.

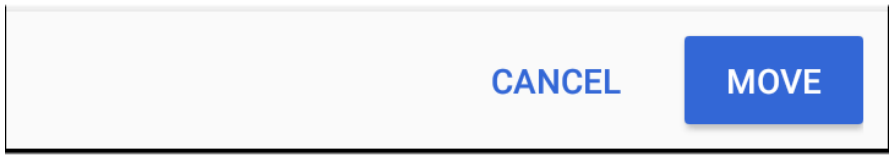


How to Move or Copy a File

1. Long press on a file to select it. You can then select more files as needed by tapping them.



2. Tap the overflow icon ⋮ at the top right.
3. Select **Copy to...** or **Move to...**. Your selected action button appears at the bottom of the screen.

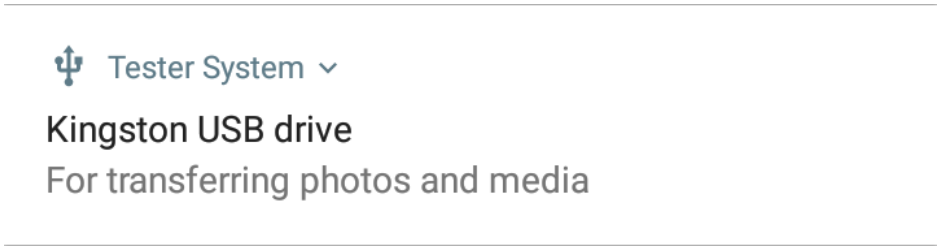


4. Navigate to the folder where you want to move or copy the file.
5. Tap the **Move** or **Copy** button at the bottom of the screen.

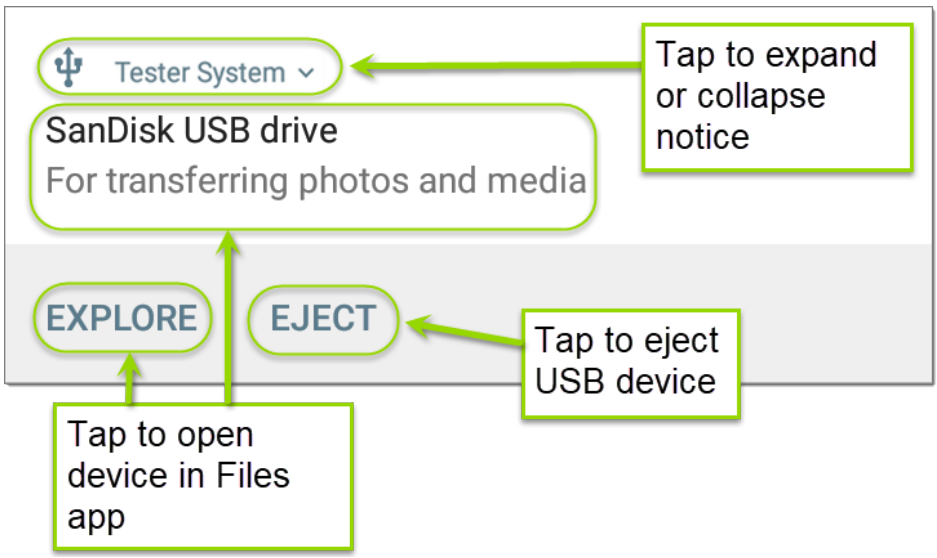
Using a USB Drive

Insert a USB flash drive into the USB port on the top of the LRAT.

A USB icon appears in the Status Bar at the top of the screen. Pull down the top Notification Panel to reveal the USB drive notification.



Tap the notification title or down arrow to expand the notification and display additional options:



The **USB storage** location is now available from the Files application.

⚠ **CAUTION:** Use the system **EJECT** function before physically removing your USB drive from

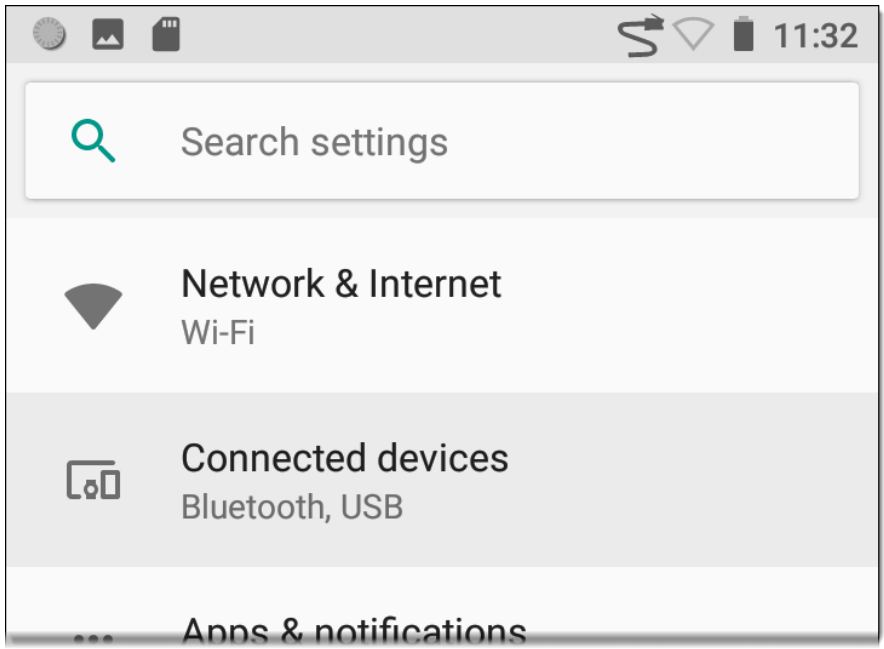
the USB port to avoid potential corruption of your storage device's file system.

Ejecting Storage Media

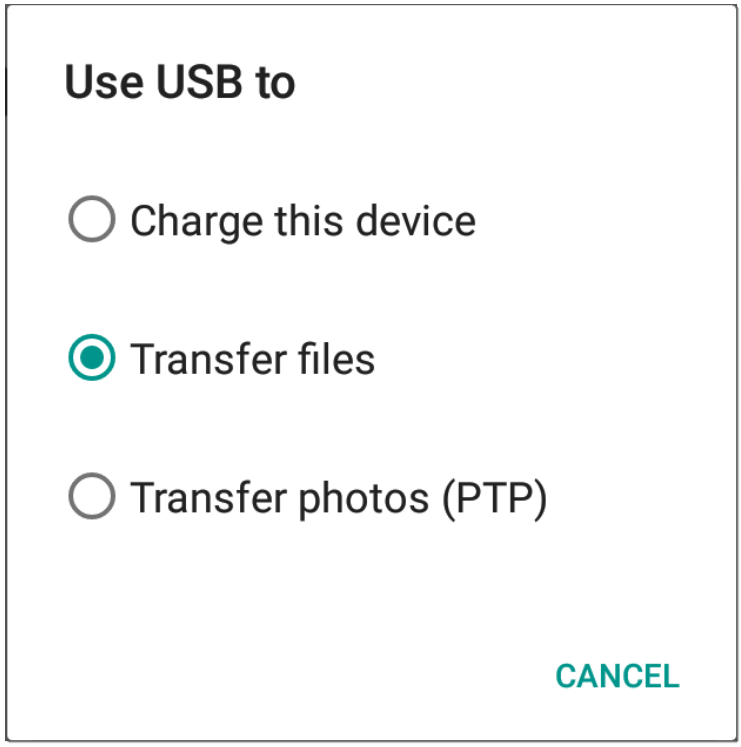
You can eject storage media from the expanded system notification (as shown above) in the Notification Panel or from the left-side navigation drawer in the Files app (below).

Using a USB Type-C to USB Cable

1. Plug a USB-C cable into the USB-C port on the left side of the LRAT, and connect to a PC or tablet.
2. On the LRAT Unit, open the system device settings by tapping the Settings icon at the bottom of the Home screen.
3. Select **Connected devices**.



4. On the Connected devices screen, select **USB**.
5. In the pop-up dialog, tap **Transfer files** to enable file transfer.



NOTE: LRAT does not charge through a USB cable connected to a PC.

6. On a PC or tablet, navigate to the LRAT 3000-4000 folder, and then move, copy, and paste files to and from the LRAT 3000-4000's file system.

⚠ **CAUTION:** Use the system **EJECT** function before physically disconnecting the USB cable from your PC or LRAT to avoid potential corruption of your storage device's file system. See Ejecting Storage Media above.

Back to Title and Contents

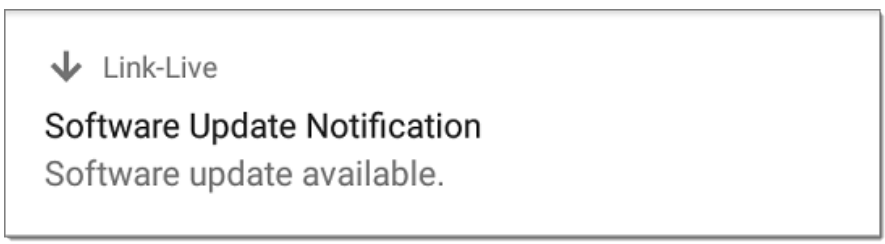
Updating Software

Your LRAT 3000-4000 accesses software updates from the Link-Live Cloud Service "Over-the-Air" (OTA). However, you can also manually download and install updates if you do not want to claim your unit to Link-Live. See Manual Updates below.

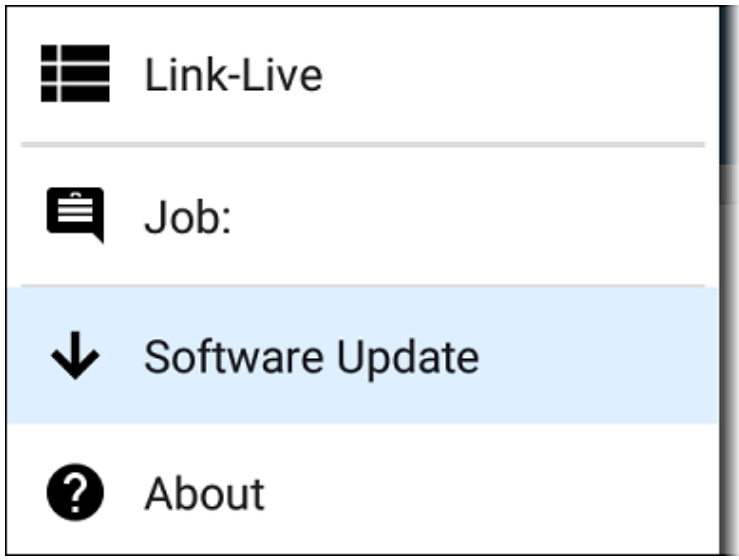
Over-the-Air Updates

For an OTA update, you must create an account and "claim" your LRAT 3000-4000 unit at Link-Live.com. Then your LRAT can find and download software updates. See Getting Started in Link-Live.

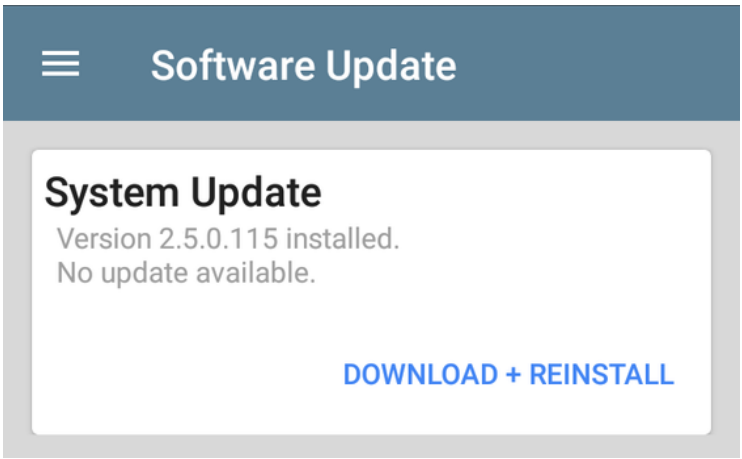
The first time you claim your LRAT 3000-4000 to Link-Live, a software update may be available. If so, an update icon appears in the Status Bar. Slide down the Top Notification Panel, and then select the notification to update your unit.



1. To check for available software updates at any time, open the Link-Live App from the Home screen.
2. In the Link-Live App, tap the menu icon or swipe right to open the left-side navigation drawer.



3. Tap **Software Update**. The Software Update screen opens and displays the version number of any available updates.



4. Tap **Download + Install** (or **Download + Reinstall**) to update the operating system and NetAlly applications. The update downloads and installs automatically. When finished, the unit restarts.
5. After updating, check the Software Update screen again in case another update is still required.

Manual Updates

You can get update files by contacting NetAlly's Technical Support at NetAlly.com/Support or by downloading them from Link-Live.com as follows:

1. Log in to the Link-Live web site.
2. Open the left-side navigation drawer by clicking the menu icon  , and then select **Support > Software Downloads**.
3. Locate and select the update file for your unit. The file name is in the format: **<product name abbreviation>-ota-user.zip**.
4. Save the update file to a PC.

Updating the System Software

Reference Buttons and Ports if needed.

1. From your PC, copy the .zip file to a FAT32-formatted Type A **USB drive**, and then insert the drive into your LRAT.
2. Power off your LRAT unit.
3. Press and hold the **Volume Up** button, and then press the **Power** button. Continue to hold the **Volume Up** button until the Recovery screen appears. (You can release the **Volume Up** button a few seconds after this screen appears.)

4. In Recovery Mode, use the volume buttons to highlight **apply update from USB drive**.
5. Press the **Power** button to confirm the selection.
6. Use the volume buttons to highlight the correct update file on the USB drive.
7. Press the **Power** button to confirm. The LRAT opens the Updater, installs the update, and then restarts with the update installed. This process can take 5 to 10 minutes. When complete, the message 'Install from USB drive completed with status 0.'should show on the install line.
8. Use the volume keys and **Power** button to select **reboot system now**. Your unit should boot normally.

Back to Title and Contents

Remote Access

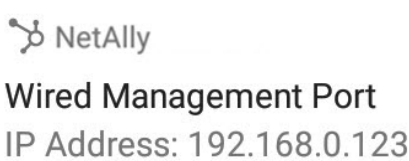
LRAT supports remote access and control using either a standalone VNC client or the Link-Live Remote feature, which uses a VNC client through the Link-Live website.

> NOTE: The Link-Live Remote feature is only available to customers with an active **AllyCare** subscription. Your LRAT must be claimed. See NetAlly.com/Support for more information.

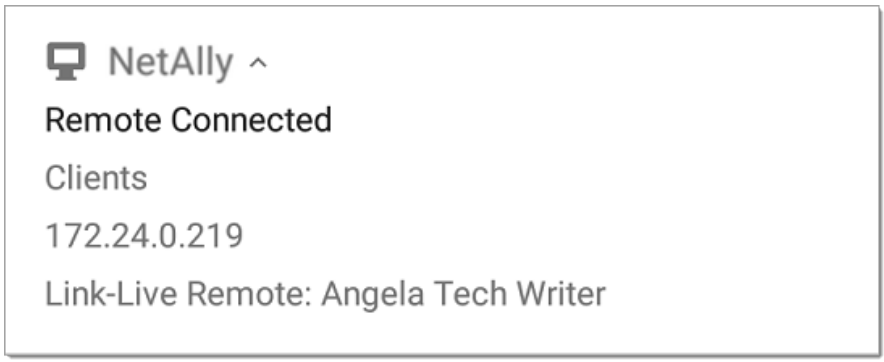
You can establish remote connections using the Wired Test Port. However, the Management Port provides a more stable link for remote control because the test ports may disconnect and reconnect frequently.

See Test and Management Ports.

The top notifications are the quickest way to find assigned IP addresses for your LRAT ports. Swipe down from the Status Bar to view them.



When a remote session is active, the remote icon appears in the top Status bar, along with a notification.



Using VNC

Remotely access the LRAT 3000-4000 using a peer-to-peer VNC client installed on a PC or other machine.

See **General Settings > VNC** to enable and configure VNC connections.

To connect to LRAT using a VNC client:

1. Get the IP address of a connected port (preferably a management port) by swiping down from the Status Bar at the top of the screen to view the notification panel.

2. Provide the Wired Test or Management Port's IP address to your chosen VNC client application.
3. Connect using your VNC client.
4. If needed, enter the password that is set in the VNC settings.

Using Link-Live Remote

The Link-Live Remote feature uses end-to-end encryption, allowing secure remote control of your LRAT.

On your LRAT, go to General Settings > Link-Live Remote to ensure the feature is enabled.

> NOTE: If a Password is enabled in the VNC General Settings, you must also enter the same password to access the Remote feature in Link-Live.

1. If you have AllyCare, sign in to Link-Live.com to access the Link-Live Remote feature. Your LRAT must be claimed.
2. Navigate to the **Units** page at Link-Live.com.

3. Select the LRAT you want to remote control from the list of claimed units.
4. Click or tap the **REMOTE** icon  at the top right of the page to open an embedded window containing the LRAT interface.
5. If necessary, at the top of the window, enter the Password set in General Settings **> Management > VNC** on the LRAT unit.

To use the Link-Live website while your remote session is active, you must open a new Link-Live tab or window.

Managing NetAlly App Settings

This topic explains how to reset, load, save, import, and export the test settings for NetAlly testing apps.

For instructions on restoring factory defaults to the entire test unit, see Restoring LRAT 3000-4000 Factory Defaults.

Resetting Testing App Defaults

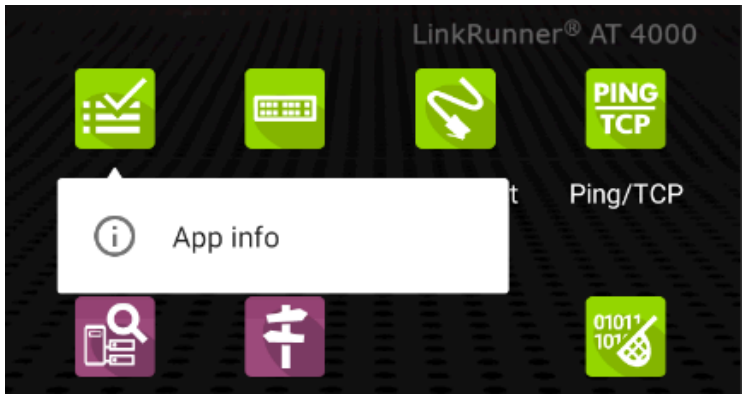
After you adjust settings in the NetAlly apps, you may need to reset an app's settings to the defaults. The following process resets all app-specific settings to the factory defaults.

> ⚠ **CAUTION:** This operation deletes all saved settings, including testing profiles and other application data.

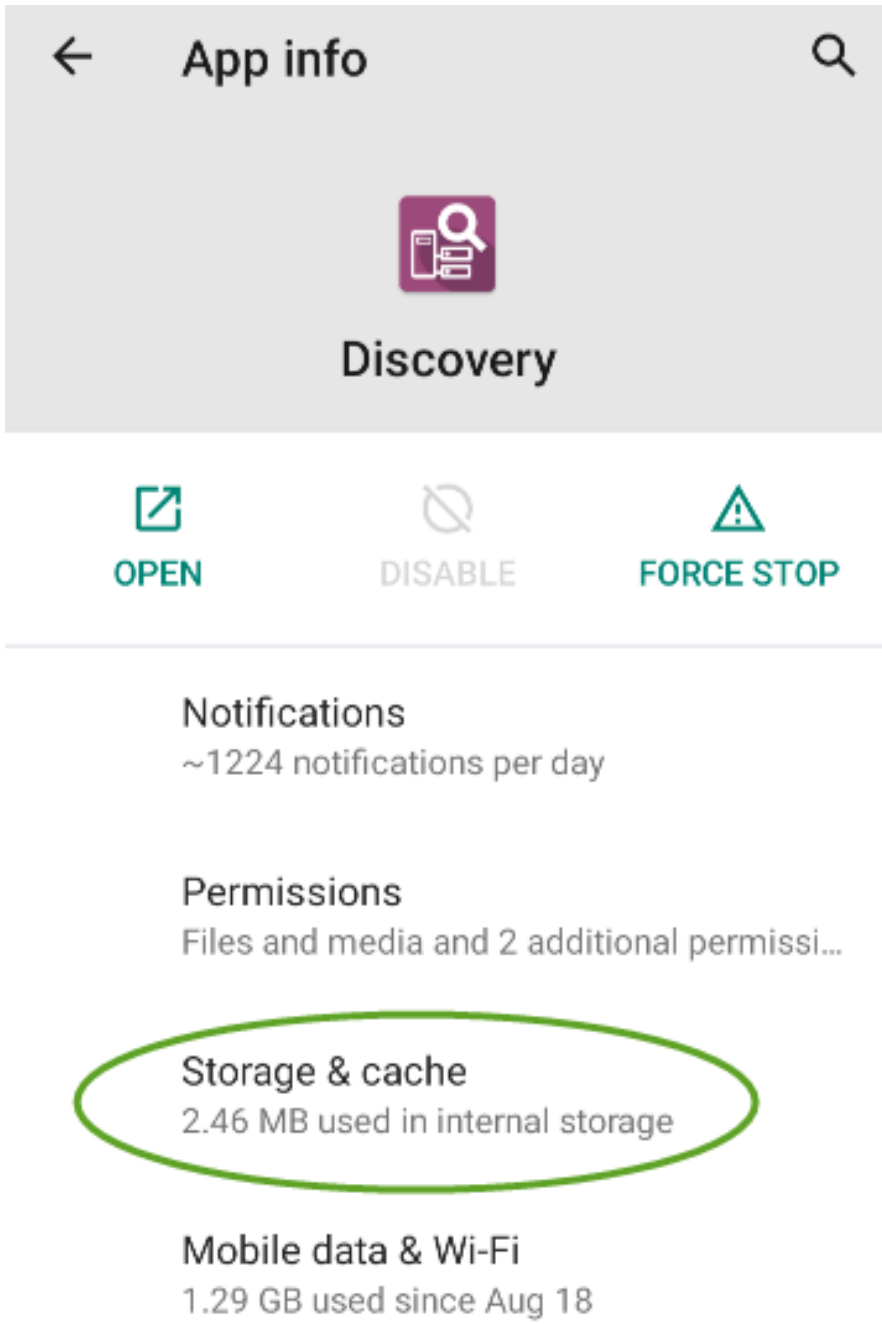
The Discovery app is used as an example in the following steps:

1. Access the **App Info** screen by long pressing (touch and hold) on an app's icon on the

Home or Apps screen.



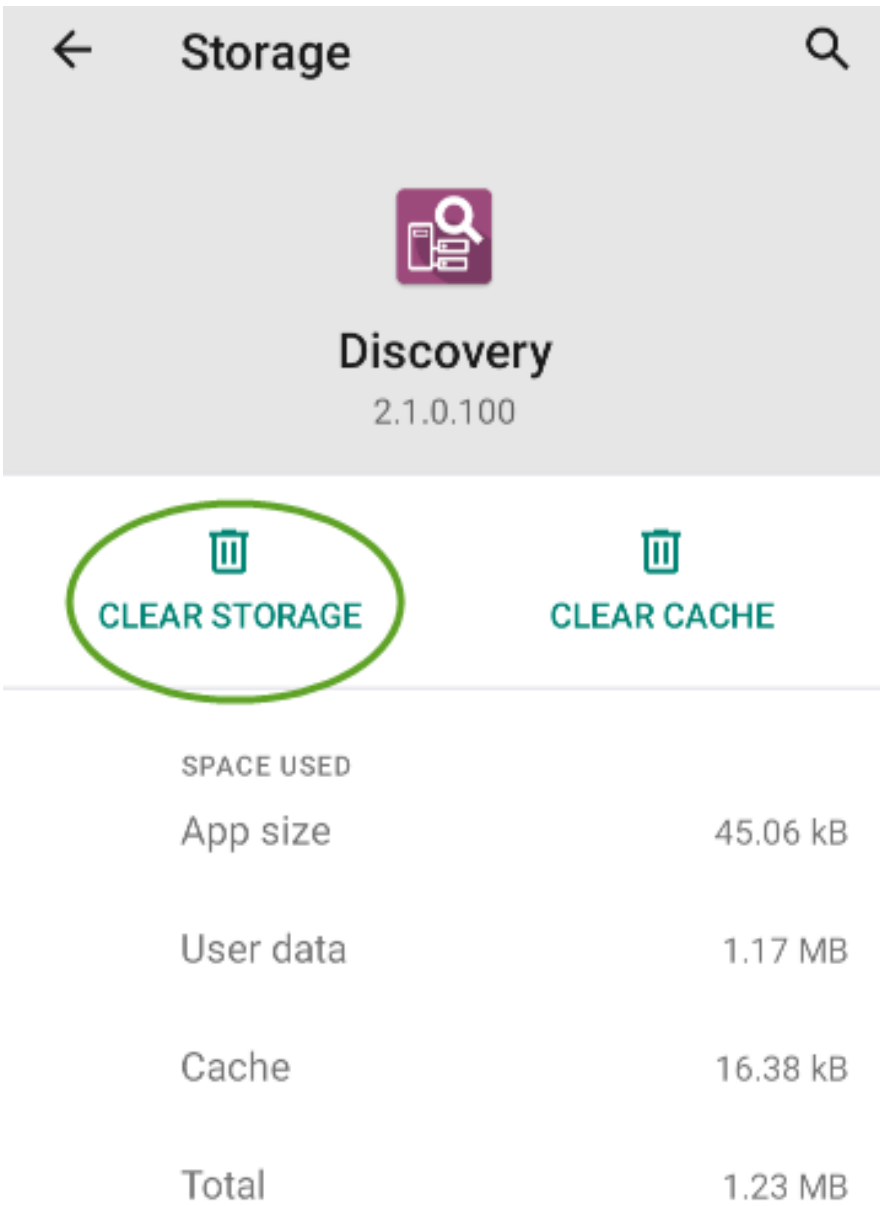
2. Tap **App info**.



3. On the App info screen, select **Storage & cache**.
   (You can also access the App Storage screen from Device Settings

> Storage > Internal shared storage > Other apps.)

4. On the Storage screen for the app you selected, tap **CLEAR STORAGE**.



5. When a dialog prompts you to delete the data, tap **OK**.

All of the app's settings are reset to factory defaults.

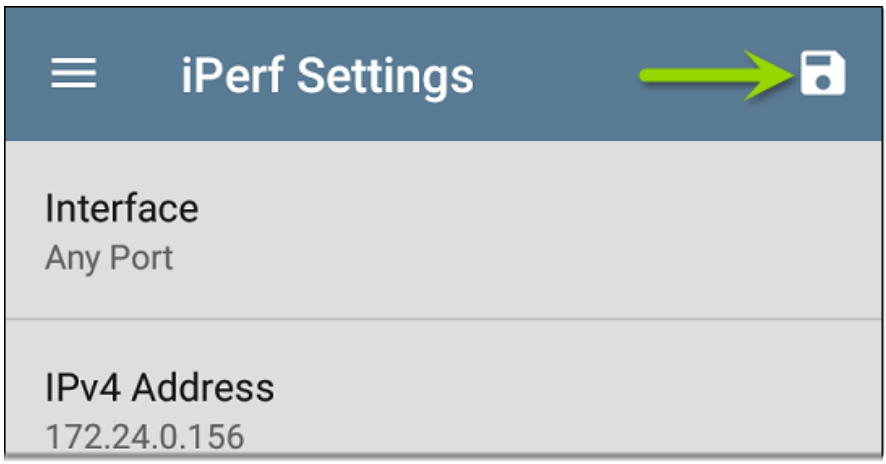
Saving App Settings and Configurations

Many of the NetAlly testing applications allow you to save and reload configured settings by selecting the save button that appears at the top right within the app's main screen.

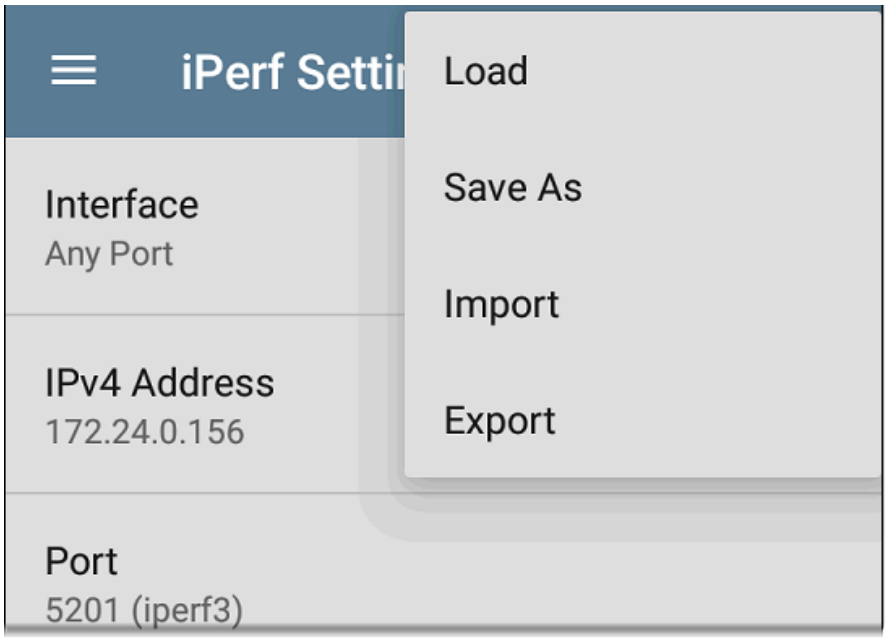
The following apps allow you to save and load settings configurations:

- AutoTest, including Profile Groups
- Discovery
- Discovery Problem Settings
- iPerf

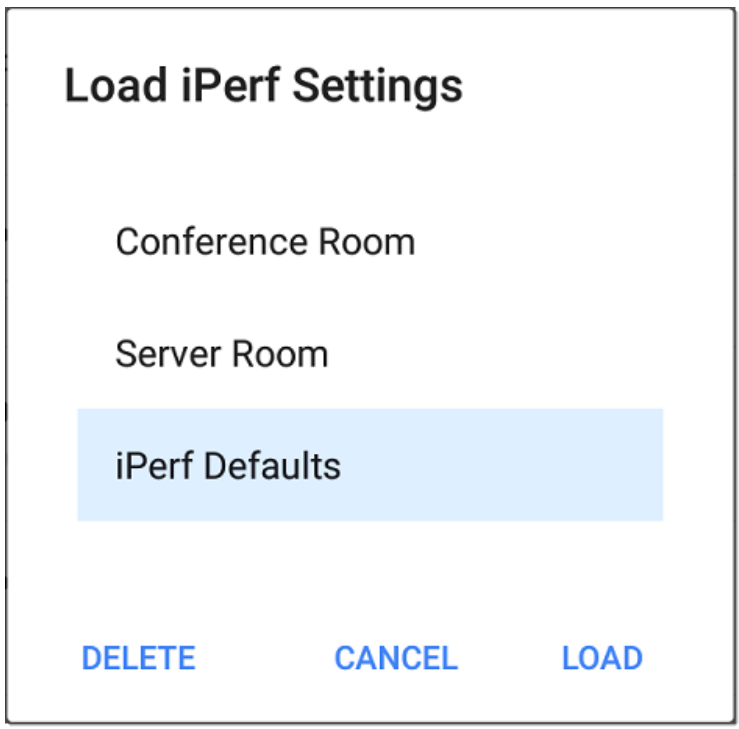
The iPerf app is shown below as an example.



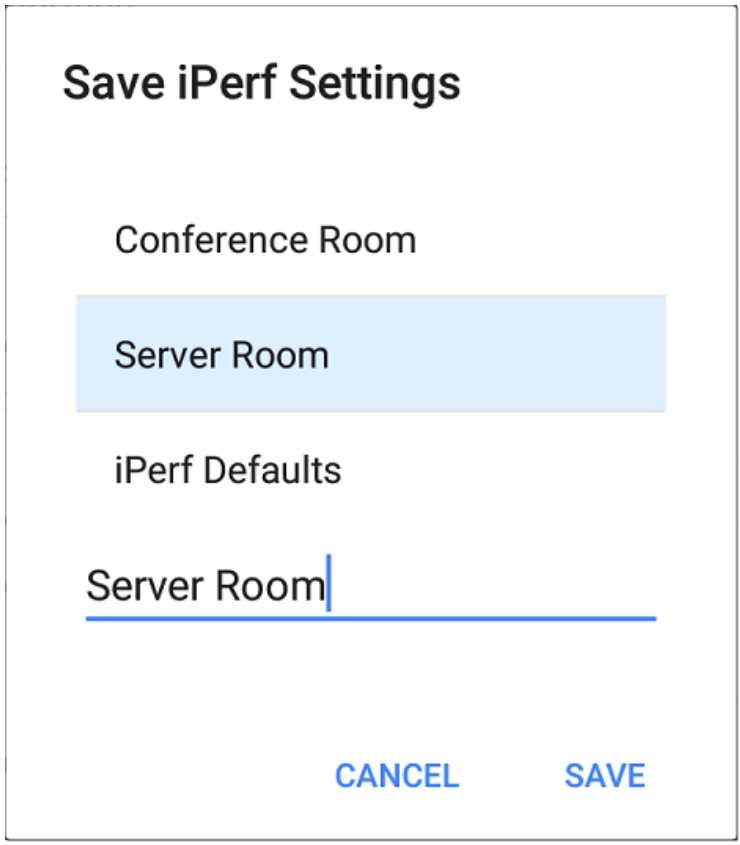
The following options display in a drop-down menu:



- **Load**: Open a previously saved and named settings configuration.



- **Save As**: Save the current settings with an existing name, or enter a new custom name.



- **Import**: Import a previously exported settings file.
- **Export**: Create an export file of the current settings, and save it to internal or connected external storage.
- **Export To Link-Live**: Export the current settings directly to the Link-Live cloud service.

See Exporting/Importing App Settings (below) for more details.

Saving a Default Test App Configuration

If you find you are frequently resetting app defaults, you can save  the default configuration of settings for later use within the NetAlly testing apps. Loading a saved default configuration within an app allows you to access the default settings without deleting other configurations. This strategy can be most useful for Discovery Settings and Problem Settings.

1. Go to an app's settings  screen.
2. With all settings set to the defaults, tap the save button  and **Save As**.
3. Save a default configuration with an obvious name like "Default Profiles" or "Discovery Defaults."
4. Do not change the settings in your default configuration to non-defaults without also saving a new, custom-named configuration.

Import/Export Settings

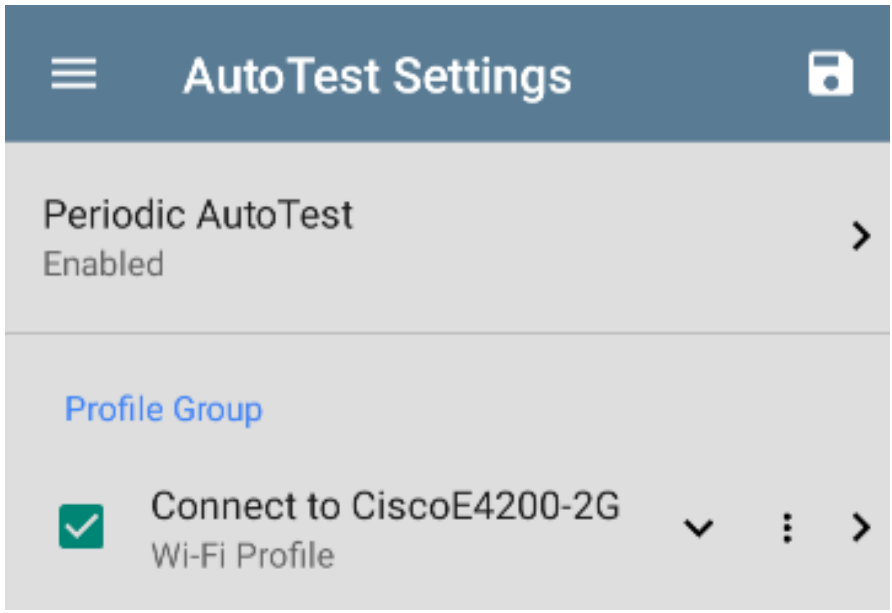
LRAT 3000-4000 provides functionality for importing and exporting saved test app settings for transfer to additional units, Link-Live, USB storage, or to other devices.

> NOTE: You can import and export settings only between the same kind of NetAlly products. For example, *both* units must be LinkRunner AT 4000s for a transfer to work. You cannot import or export settings between a LinkRunner AT 3000 and a LinkRunner AT 4000.

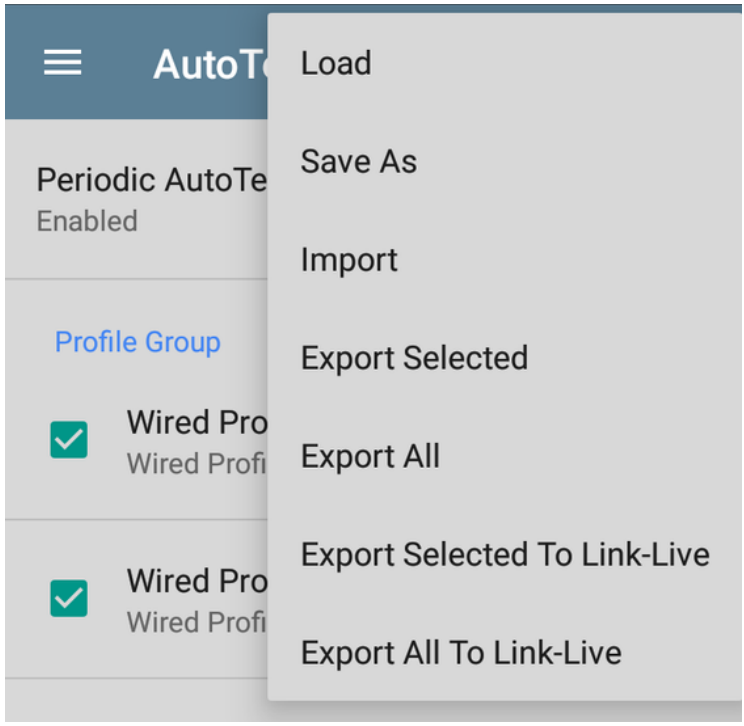
The following apps enable you to import and export settings and configurations:

- AutoTest Settings, including Profile Groups
- Discovery Settings
- Discovery > Problem Settings
- iPerf Settings

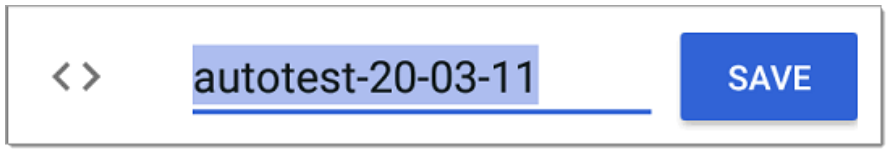
The AutoTest Settings are shown as an example in the images below.



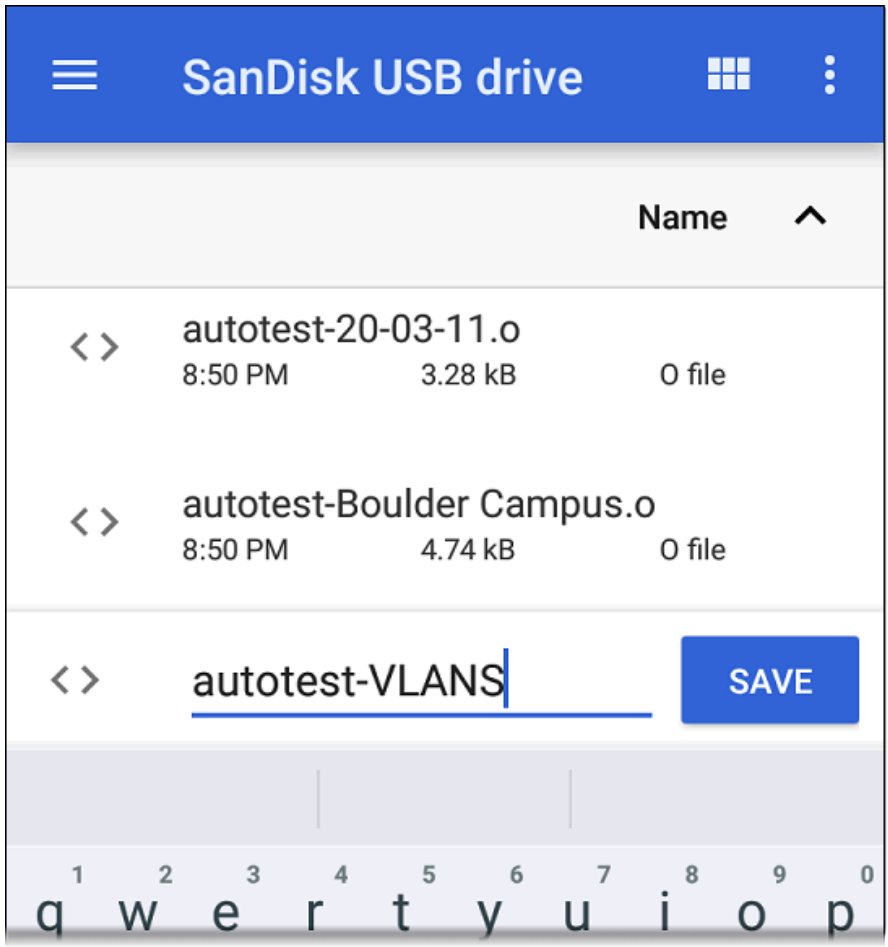
- Tap the save button to import new app settings or export the *currently active and selected* app settings.



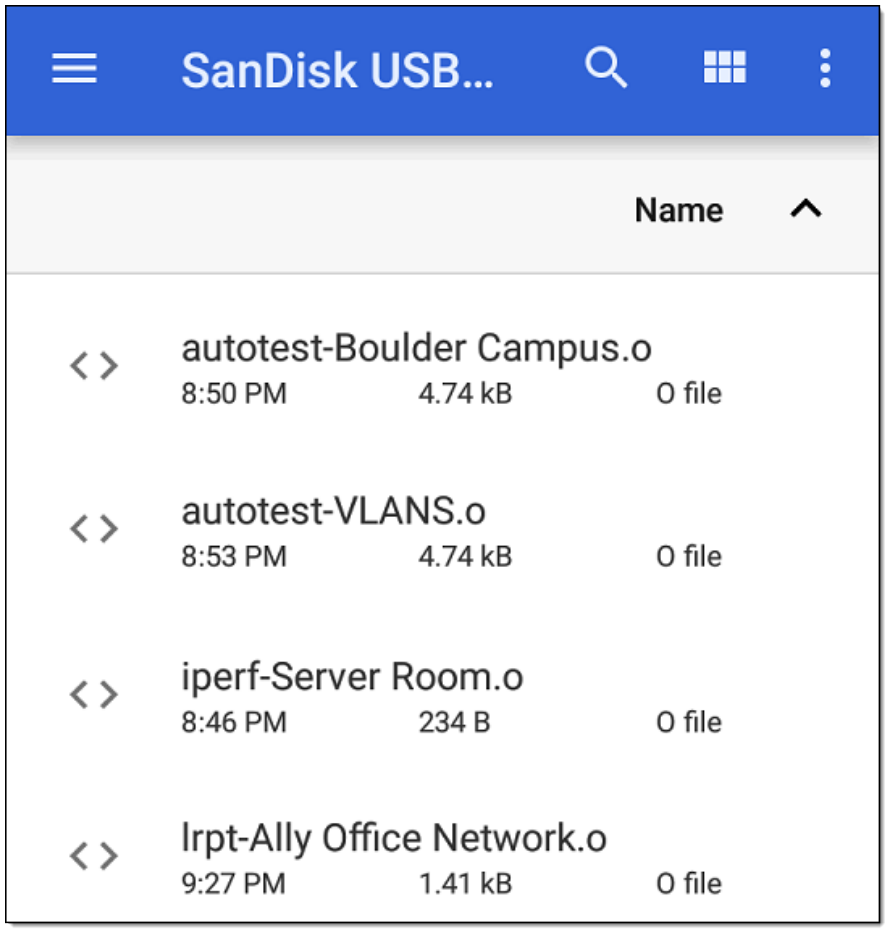
- Selected (checked) items in shared lists of configurations are the only ones exported when you choose **Export Selected**. This can include any checked items in submenus (such as AutoTest Test Targets or Community Strings in Discovery Settings). You can also select **Export All** to export all selected and unselected items.
- Unsaved configurations without a custom name are auto-named with the app name and date:



- Saved configurations are auto-named with the app name and custom settings name:



- You can rename the export file as needed.
- Settings can be saved to any connected external or internal storage. See Managing Files for instructions on accessing folders and moving files.
- Settings are saved with the **.o** file extension.



- Selecting **Import** from an app opens the Files app, where you can navigate to and select the .o file you want to import.
- Imported settings configurations overwrite existing saved configurations with the same name that are already in the app.

Transferring AutoTest Settings to Other Devices Using Link-Live

You can use the Link-Live cloud service to transfer AutoTest settings with other LRAT 3000-

4000 devices.

- Do some setup before you begin.
- Export the settings file(s) that you want to share to Link-Live.
- Use Link-Live to select other devices to which you want to transfer the settings.
- Use each selected unit to import the settings.

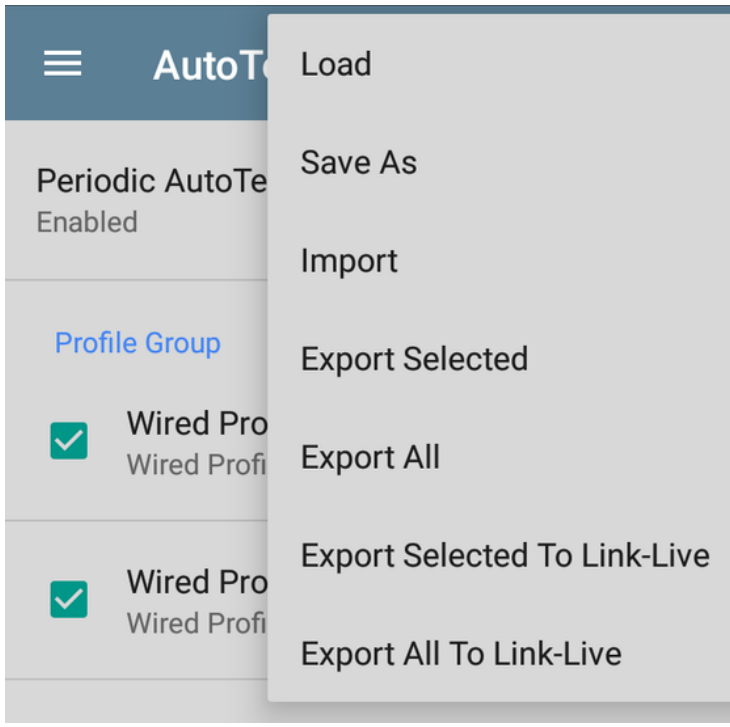
Before You Begin

- Make sure that you have access to the following:
  a. The device from which you will get the settings
  b. A PC-based browser
  c. The devices to which you will transfer the settings file
- Make sure that you have claimed and updated the software for all LRAT 3000-4000 devices to which you want to transfer the settings. (You can use the Link-Live app or web site to do the claiming. See Claiming the Unit for instructions.)

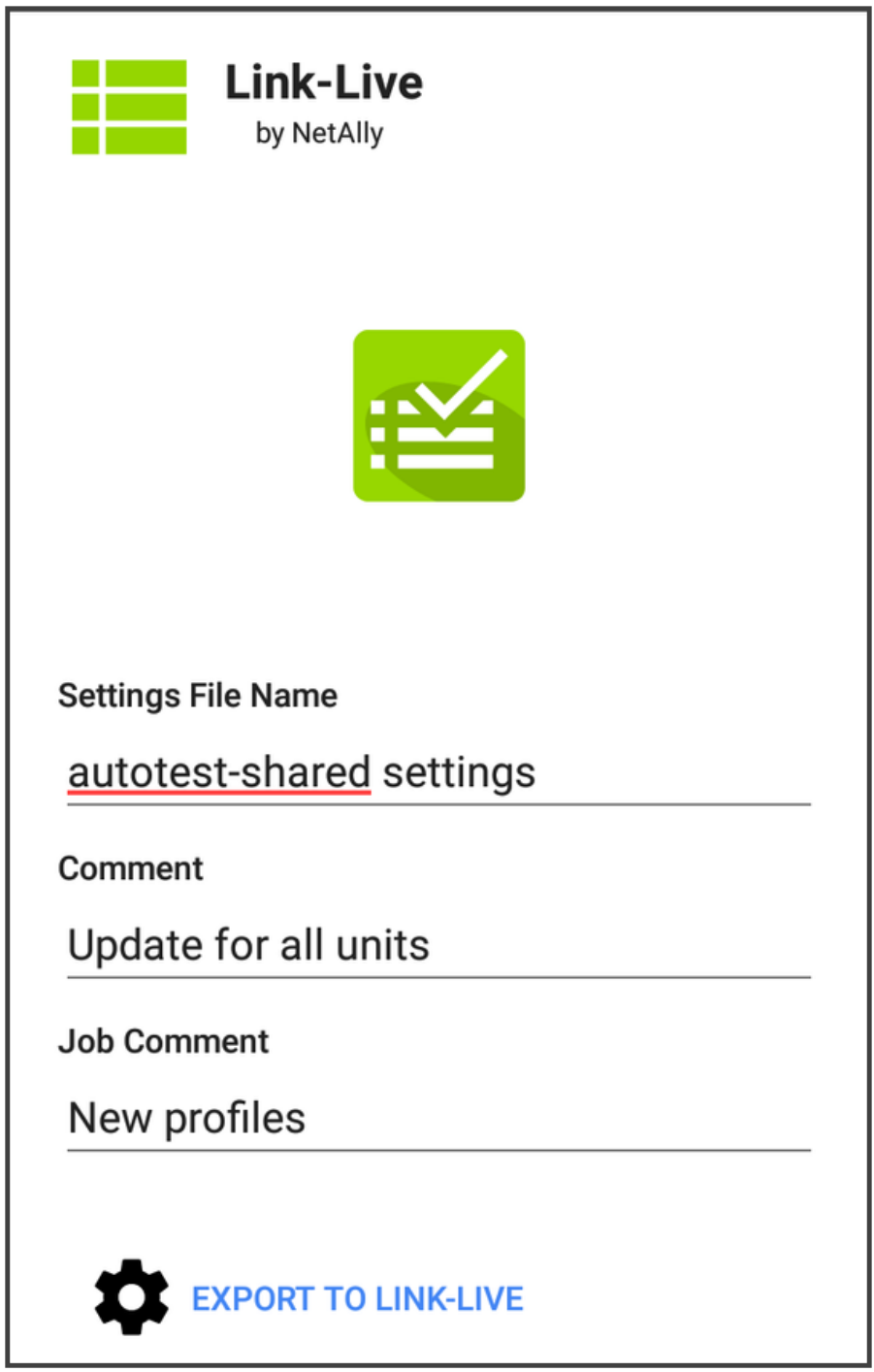
Export the Settings File(s)

This procedure is done on the device from which you are transferring the settings.

1. In the AutoTest app main page, tap the settings icon in the top right. This opens the list of profiles.
2. If you plan to export only selected profiles, use the checkboxes to choose those profiles from the list.
3. Tap on the save icon in the top right to display the save menu options.



4. Tap **Export Selected To Link-Live** (if you selected profiles) or **Export All To Link-Live** on the menu. This opens the save screen for Link-Live.



5. (Optional) Edit the file name, add a comment, or add a job comment on the screen.
6. Tap **Export To Link-Live**. This uploads the file to Link-Live.

Use Link-Live to Select Other Devices

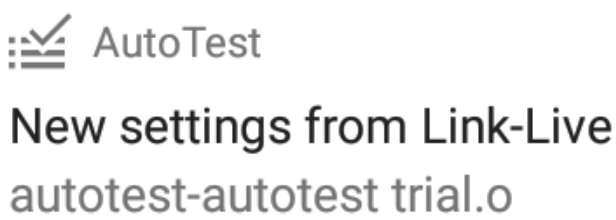
This procedure is best performed on a PC-based browser.

1. Use a PC-based browser to log in to the Link-Live web site.
2. Tap the main menu icon  .
3. Click on **Settings** to open the settings menu.
4. Select **LRAT 3000-4000** to list the .o settings files available for your devices.
5. Select the settings file you want to transfer.
6. Follow the screen instructions to transfer the file to specific units or to all units that you have claimed.

Use Each Selected Unit to Import the Settings

This procedure is performed on the device to which you want to apply the settings.

1. Wait for up to 30 seconds after the file was pushed from Link-Live.
2. Swipe (touch and drag) downwards from the Status Bar at the very top of the home screen to display the Notification Panel.
3. Locate the notification that says there are new AutoTest settings from Link-Live and lists the profile name.



4. Tap on that notification to open the AutoTest application.
5. Tap on the save icon in the top right.
6. Tap on **Import** and navigate to Downloads.

7. Select the downloaded .o file to apply the new profile settings.

Import/Export Settings for All Apps

Your LRAT 3000-4000 supports the importing or exporting of settings for *all* applications that allow import/export of settings.

> NOTE: You can import and export settings only between the same kind of NetAlly products. For example, *both* units must be LinkRunner AT 4000s for a transfer to work. You cannot import or export settings between a LinkRunner AT 3000 and a LinkRunner AT 4000.

To perform a group export or import:

1. Open the About Screen by tapping the navigation menu icon  in any NetAlly application and then tapping **About**.

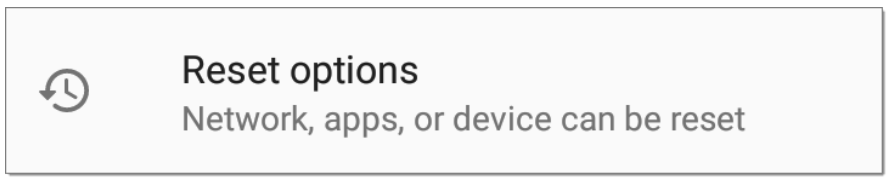
2. Tap the action overflow icon  to display the export or import menu.

3. To import settings:
    a. Tap **Import LinkRunner AT Settings**. This opens the Files app to the default Settings folder.
    b. (Optional) Use the Files app to navigate to a different folder.
    c. Select the .nas settings file you want to import.
    d. Tap **Yes** at the prompt to import the settings for all apps at the next system restart.
4. To export settings:
    a. Tap **Export LinkRunner AT Settings**. This opens a dialog with a system-generated file name and the default Save To folder.
    b. (Optional) Tap the Save To folder or tap Save As to open the Files app to select a different folder.
    c. Tap **Save** to save the settings file.

Resetting LRAT 3000-4000 Factory Defaults

⚠ **CAUTION:** Resetting your device to factory defaults can delete *all* test results, user-installed applications, testing app settings, and saved files.

1. Make sure to back up any files you wish to keep before resetting.
2. Open the system Device Settings by tapping the Settings icon at the bottom of the Home Screen.
3. On the Settings screen, scroll down to and tap on the **System** section.
4. On the System screen, tap **Reset options**.



5. On the Reset options screen, select an option based on the defaults you want to reset. Your LRAT displays a list of the items that will be reset based on the option and a

confirmation button.

Reset Wi-Fi, mobile & Bluetooth: resets all network settings for Wi-Fi (test and management), mobile data, and Bluetooth.

Reset app preferences: resets any preferences or settings for applications, although app data is not lost.

Erase all data (factory reset):
⚠ **CAUTION:** Erases ***all*** user data from your tester's internal storage, including: system and app data and settings; downloaded apps; test profiles; credentials; packet information; and screen captures.

6. Tap the confirmation button to begin the reset.
7. Your unit may ask you to confirm a final time before resetting. If so, tap the final confirmation button to reset your LRAT's defaults. The unit then restarts with the factory default settings you selected.
8. Data on removable drives is not included in the reset. To be thorough, you may also

want to use the Files application to delete any application settings, preferences, or other data that you have saved on a USB thumb drive. (Do not delete your backup files.)

Back to Title and Contents

Back to Title and Contents

LRAT 3000-4000 Feature Access

This chapter explains how to semi-permanently control the availability of features on your LRAT 3000-4000.

Tap a link below to skip to your desired topic:

Introduction to Feature Access

The LRAT 3000-4000 provides the ability to semi-permanently disable certain features to meet a variety of security needs. These features are referred to as controlled features.

Controlled features have categories to help you identify which features can be disabled.

Removable Storage

- USB Access

Connectivity Apps

- Browser App
- Telnet/SSH App

Remote Control

- VNC

Documenting

- Packet Capture (LRAT-4000 only)
- Network Discovery (LRAT-4000 only)

Link-Live Cloud Service

- Link-Live Access
- Download from App Store

Removable Storage

USB Access

Both the USB Type-A port on the top of the unit and the Type-C port on the left side of the unit are deactivated when the USB Access feature is disabled. This means that there can be no data transfer in either direction via these ports and that external devices cannot receive power from these ports.

> NOTE: The USB Type-C port continues to function to support powering the unit using the AC adapter.

Connectivity Apps

Browser App

The Chromium browser is removed if you disable the Browser App feature. All NetAlly apps that normally provide access to the Chromium

browser remove that option. Other apps cannot access the browser.

> NOTE: If you re-enable the Browser App feature, the Chromium browser, User Guide, and Video apps are restored but do not appear on the Home screen. See **Apps** for more information about the Apps screen.

Telnet/SSH App

The JuiceSSH app, which provides Telnet and SSH client services, is removed when the Telnet/SSH App feature is disabled. All NetAlly apps that normally provide access to this app remove this option.

Remote Control

VNC

The ability to remotely access and control the product UI using a standalone VNC client is deactivated when the VNC feature is disabled. See **Remote Access** for more information about this capability.

> NOTE: The Link-Live Remote feature remains active when VNC is disabled. To deactivate

Link-Live Remote, Link-Live Access must be disabled.

Documenting

Packet Capture (LRAT-4000 only)

The Capture app is disabled when the Packet Capture feature is disabled. All NetAlly apps that normally provide access to the Capture app will remove this option.

NOTE: See Capture for more information.

Network Discovery (LRAT-4000 only)

The Upload to Link-Live or Save Locally function in the Discovery app are disabled.

NOTE: See Discovery for more information.

Link-Live Cloud Service

Link-Live Access

The Link-Live app is disabled when the Link-Live Access feature is disabled. All NetAlly apps and services that provide an interface to Link-Live will remove access.

NOTE: The Link-Live Remote feature and the App Store app are also disabled when Link-Live Access is disabled.

Download from App Store

The App Store app is disabled when the Download from App Store feature is disabled. Adding additional apps to the product is not possible.

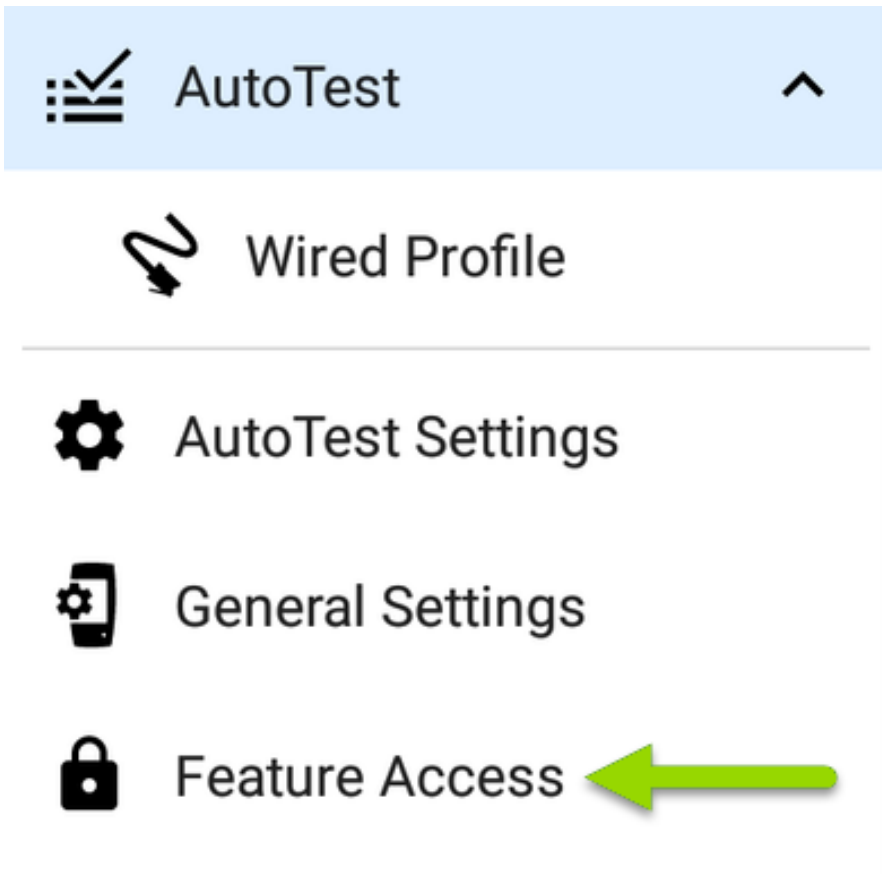
NOTE: Disabling Link-Live Access also disables the App Store app.

Back to Title and Contents

Controlling Feature Access

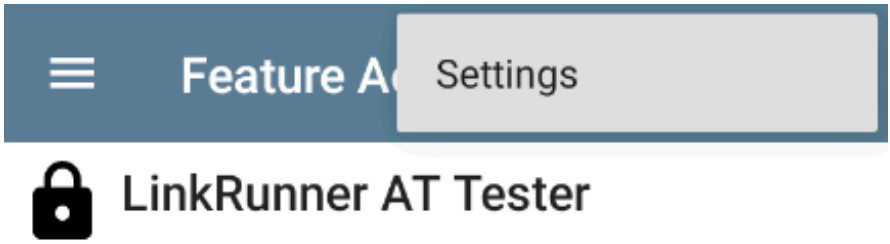
The LRAT 3000-4000 supports disabling (and re-enabling) certain features to meet a variety of security needs. These features are referred to as controlled features.

Use the **Feature Access** selection to manage feature access. It is accessible from the left-side navigation drawer in NetAlly apps, such as AutoTest and Ping/TCP.

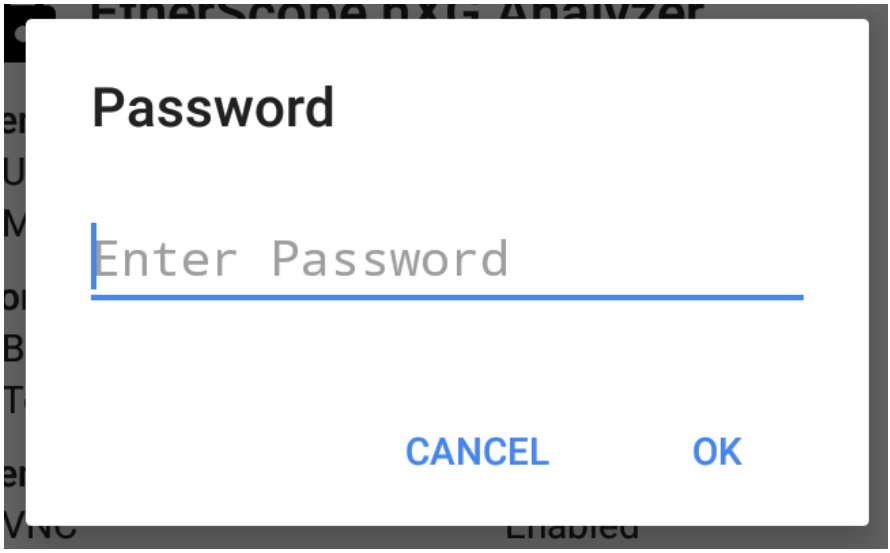


Select **Feature Access** to view the **Feature Access** status screen. This screen shows the current state of the controlled features.

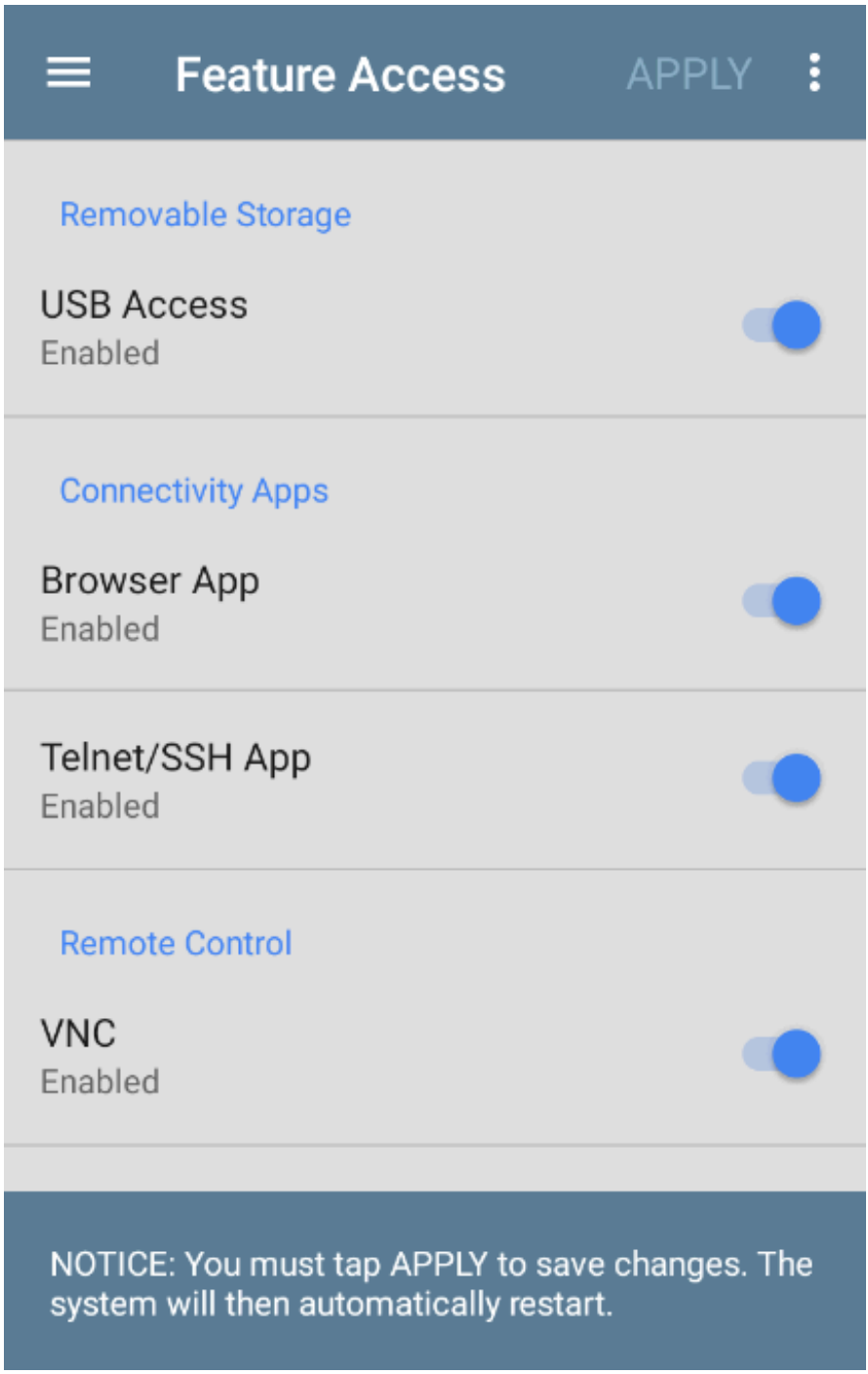
To change access to a controlled feature, tap the action overflow icon  , and then tap the **Settings** option.



When prompted, enter the **Feature Access** admin password, and then tap the **OK** button.



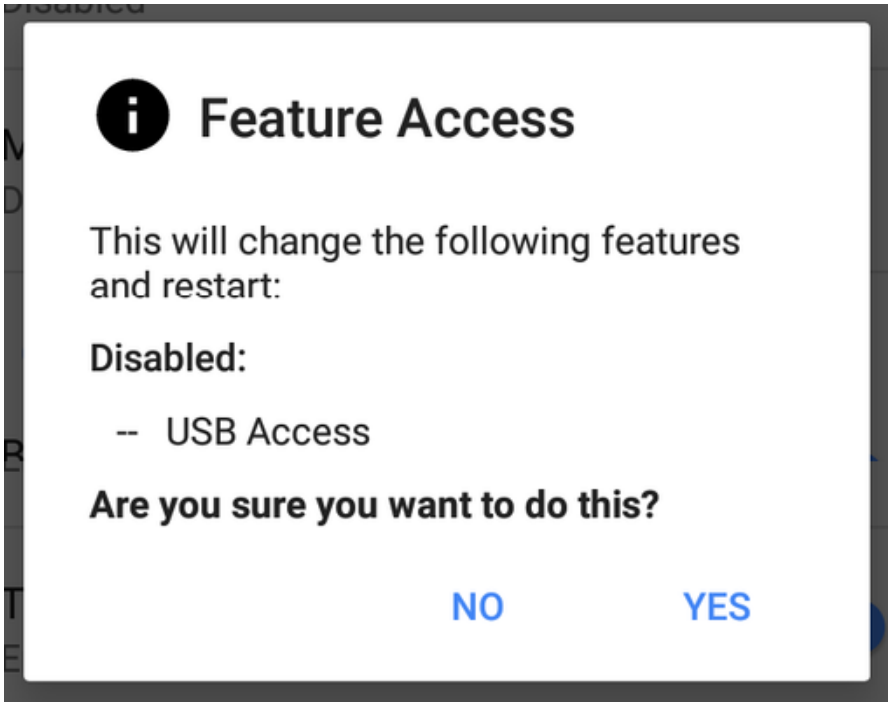
The **Feature Access** screen shows the current state of the controlled features and lets you turn features off or on using the toggle



If you make changes, the **Apply** button at the top of the screen becomes active.

Tap **Apply** as the first step in completing the changes.

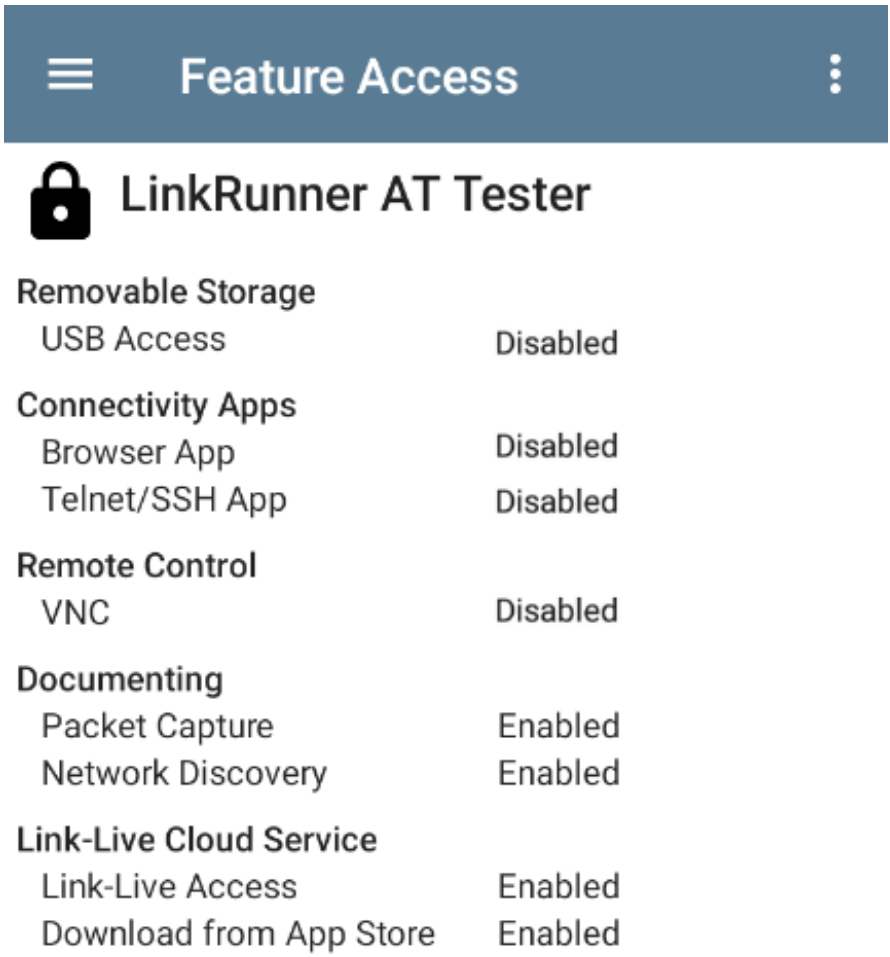
A message lists the pending feature changes.



- Select **Yes** to make the pending changes
- Select **No** to cancel the pending changes and return to the Settings screen

After the changes are applied, the unit automatically restarts.

To view the state of the controlled features, visit the **Feature Access** status screen.



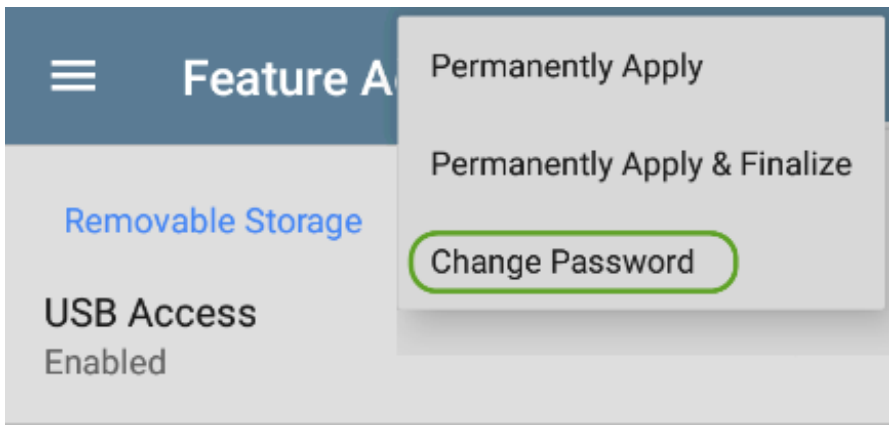
Back to Title and Contents

Changing the Administrative Password

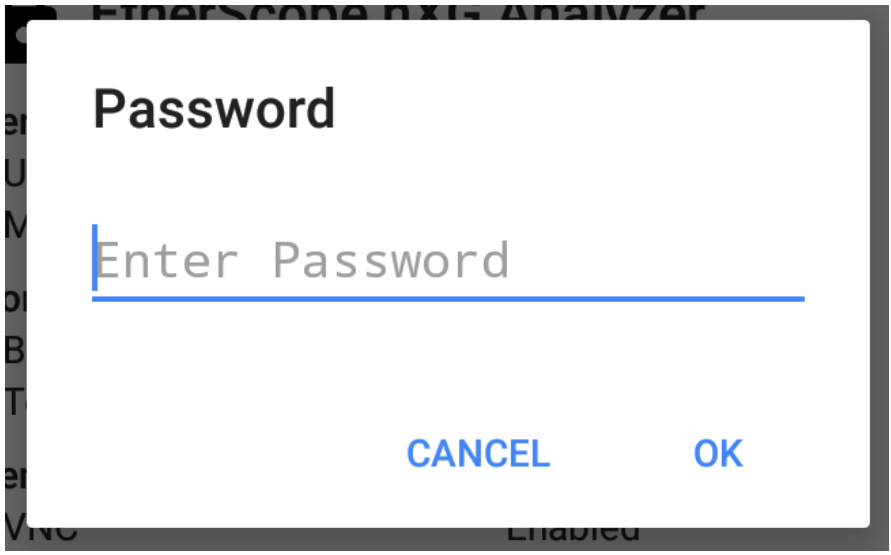
NetAlly recommends that you change the factory-set admin password when you configure **Feature Access** to prevent non-administrative users from gaining access to the **Feature Access** screen.

To change the admin password:

1. Follow the procedure in Controlling Feature Availability to access the **Feature Access** selection screen.
2. From the selection screen, tap the action overflow icon  at the top of the screen to display the overflow menu.



3. Select **Change Password** to display the Current Password entry screen.



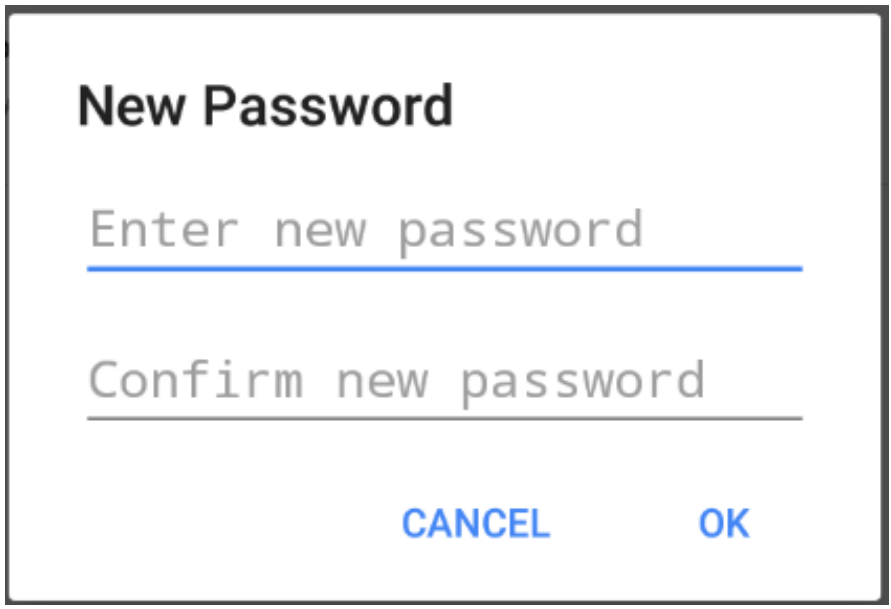
4. Enter the current admin password and tap **OK** to continue. (Select **CANCEL** to return to the **Feature Access** selection screen without making any changes.)

   Note: The factory-set administrative password is: **admin**

5. Wait for the New Password entry screen to display, enter the new password in both fields, and then tap **OK** to complete the admin password change. (Select **CANCEL** to return to the **Feature Access** selection screen without changing the current admin

password.)

Note that you cannot complete the admin password change until the new password fields contain matching entries.



Back to Title and Contents

LRAT 3000-4000 Testing Applications

This section of the User Guide describes the NetAlly-developed network testing apps. Each app is specially designed for fast analysis and intuitive operation to enhance and simplify your network tasks.

Open the testing apps by selecting their icons from the Home screen or the Apps screen.

AutoTest App and Profiles

AutoTest is the most comprehensive NetAlly testing application on LRAT 3000-4000. You can quickly run a variety of test types and save their configurations and network credentials for access whenever you need them. The app is fully customizable with test "Profiles" for Wired network connections, as well as individual Test Targets

AutoTest establishes the Wired Test Port connection used by other testing apps.

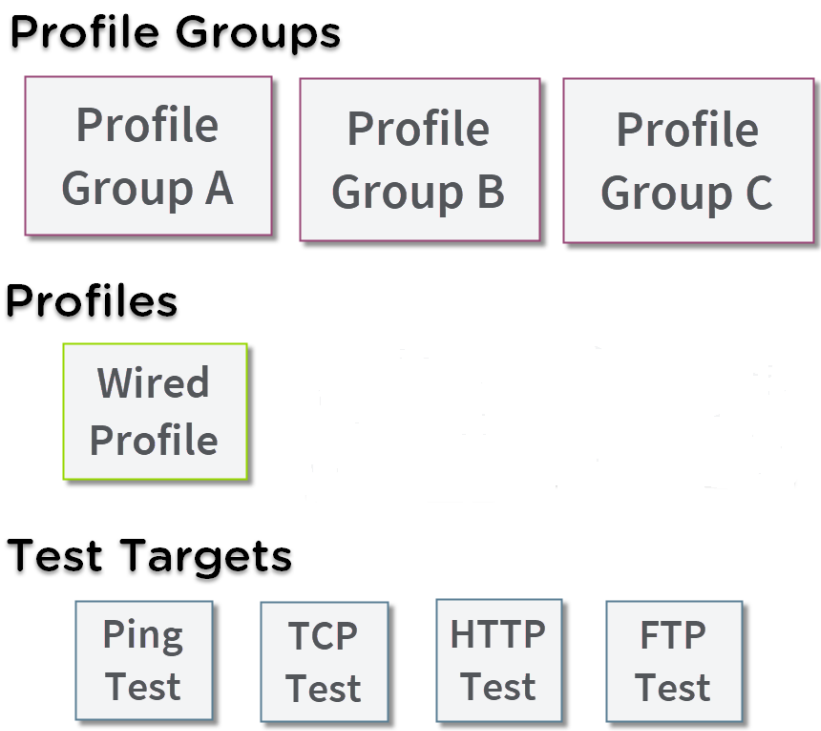
AutoTest results are automatically uploaded to Link-Live Cloud Service after you claim your LRAT.

AutoTest Chapter Contents

This chapter describes AutoTest Profiles, screens, settings, and test results.

AutoTest Overview

AutoTest consists of three distinct testing levels: **Test Targets**, **Profiles**, and **Profile Groups**. You can create as many Profile Groups, Profiles, and Test Targets as you need.



At the bottom level is a set of individual **Test Targets** that connect to network services, such as a web app or FTP site. A Test Target defines parameters including type, target URL/IP address, port number, and Pass/Fail thresholds. More complex tests, like HTTP, allow further Pass/Fail criteria, such as strings that must or must not be contained in the HTTP body.

A Test Target can be added to and used in any number of **Profiles**.

A **Profile** contains a series of individual network tests. There is one Profile type: Wired which includes connection tests and credentials for a Wired VLAN. Profiles provide an automated and consistent way to verify a network from layer 1 through layer 7.

A Profile can be added to and used in any number of **Profile Groups**.

A **Profile Group** is a custom-named collection of Profiles. Profile Groups are designed to allow further automation for testing multiple networks or network elements with a single tap of the START button.

A Test Target can be in any number of Profiles, and a Profile can be in any number of Profile Groups.

For example, you can:

- Test multiple Wired VLANs on a trunk port.
- Test wired access from a conference room.

Back to Title and Contents

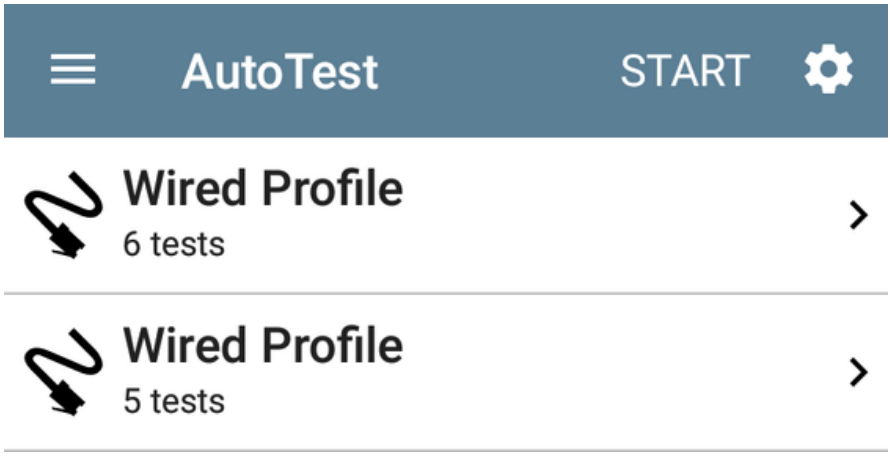
Managing Profiles and Profile Groups

Profiles are a series, or suite, of tests designed to analyze the different characteristics of your networks. The LRAT 3000-4000 AutoTest app has a single test profile type:

Wired Profiles to test copper and fiber connections.

Factory Default Profiles

The LRAT begins with a default version of the AutoTest profile types, which you can customize, delete, or replace for your purposes.



To customize each Profile with the required network settings and a custom name, tap the Profile name *first*, and then select the settings icon.

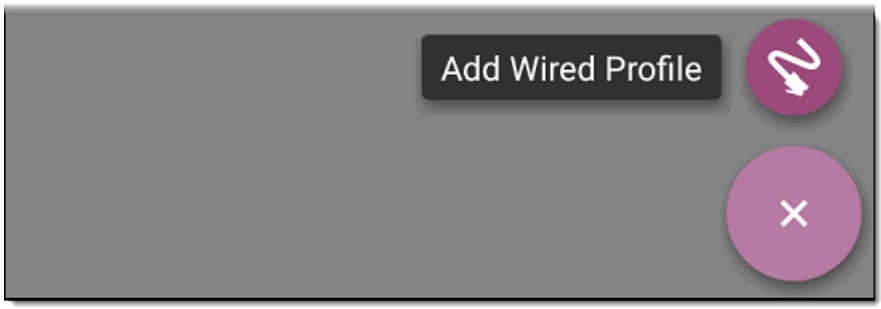
NOTE: Tapping the settings icon on the main AutoTest screen (shown above) opens the AutoTest Settings and Profile Group screen, not the individual Profile settings.

- The default **Wired Profile** runs automatically and establishes a wired link as soon as your unit is powered on and an active Ethernet connection is available on the top RJ-45 port.
- The default **Wired Profile** for the LinkRunner AT 4000 includes an HTTP test target. The default profile for the LinkRunner AT 3000 includes a Ping test.

  NOTE: The default Wired Profile does not run automatically over a fiber link. You must tap START in AutoTest to run a Wired Profile on a fiber connection.

Adding New Profiles

To add new test profiles to the current AutoTest, tap the floating action button (FAB) on the AutoTest screen.



The profile's configuration screen appears. See the topic for each profile type for a description of its settings.

After you configure the profile settings, tap the back button at the bottom of the screen to open and run the new test profile.

Profile Groups

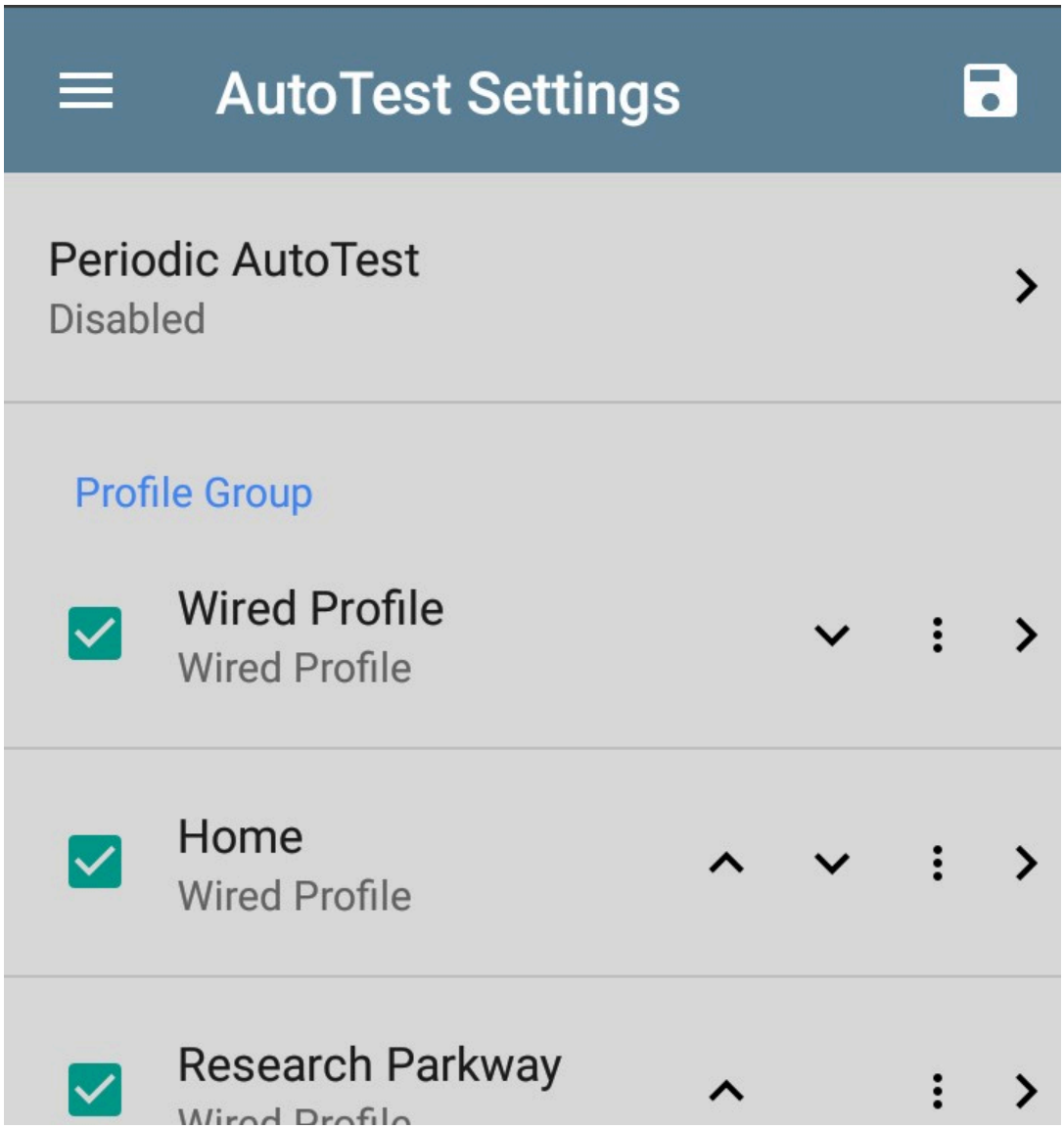
LRAT 3000-4000 also allows you to save Profile Groups. Profile Groups are simply **the included list of test Profiles and the order in which they run** when you start an AutoTest. (See AutoTest Overview for more explanation of Profile Groups.) You can configure and select Profiles and Profile Groups for different locations, jobs, networks, or other purposes.

To manage your Profiles and Profile Groups, tap the Settings  button on the main AutoTest screen (with the list of Profiles).

AutoTest Settings Screen

The AutoTest Settings screen contains the Periodic AutoTest and Profile Group settings.

> NOTE: Periodic AutoTest is available for the LRAT-4000 only.



You can perform these actions on the AutoTest Settings screen:

- Check or uncheck the boxes to include or exclude a test Profile from the currently active Profile Group.

- Tap the up and down arrows  to reorder the test Profiles on this and the main AutoTest screen for the Profile Group.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a Profile.
  CAUTION: When you delete a Profile, it is deleted from all Profile Groups. To remove a Profile from the current group, simply uncheck it.
- Tap any Profile's name to open the test and connection settings for the Profile.
- Tap the save icon  to perform the following actions:
  - **Load**: Open a previously saved settings configuration, which includes the Profile Group.
  - **Save As**: Save the current settings and Profile Group with an existing name or a new custom name.

    See also Saving App Settings Configurations.

- **Import**: Import a previously exported settings file.
- **Export**: Create an export file of the current settings, and save it to internal or connected external storage.

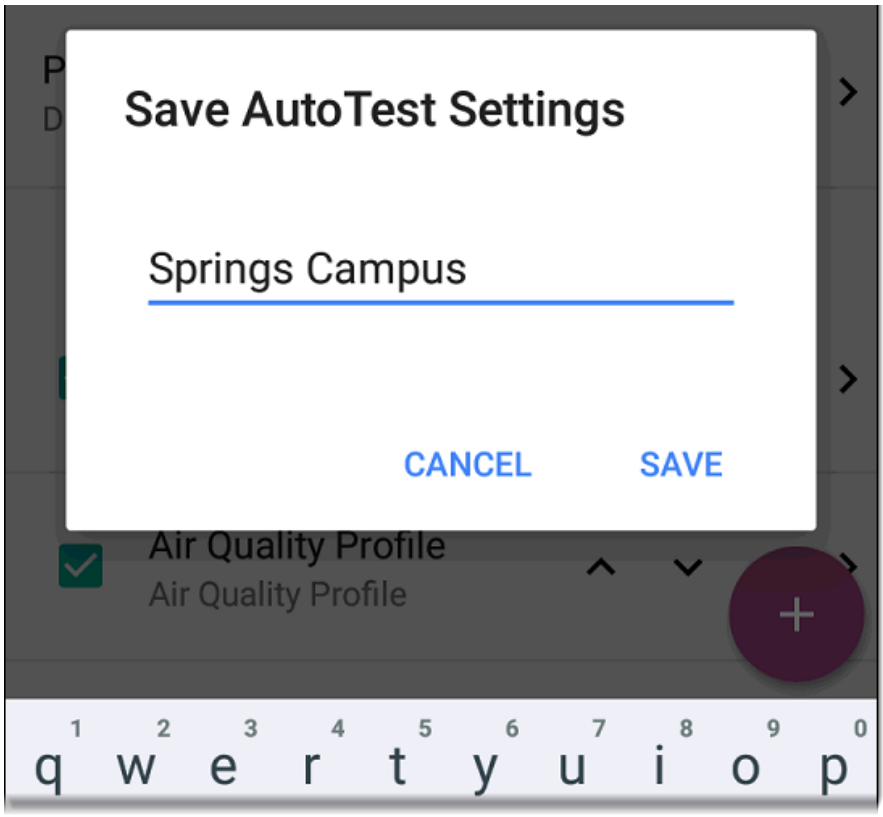
  See Exporting and Importing App Settings for more details.

Each Profile Group can run one or many instances of the profile type. Saved Profiles are available across all of your Profile Groups.

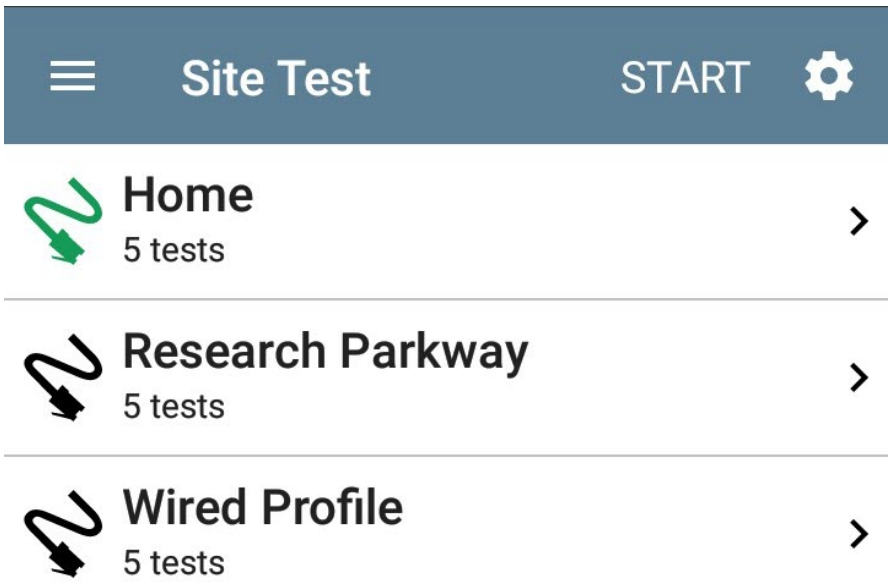
Custom AutoTest Settings/Profile Group Names

By default, the AutoTest app screen shows "AutoTest" in the header, and the AutoTest Settings screen header is "AutoTest Settings." Once you save a custom name, the name displays in the AutoTest app header and in the AutoTest Settings screen header.

In the example below, the user saves a custom AutoTest configuration named "Springs Campus."



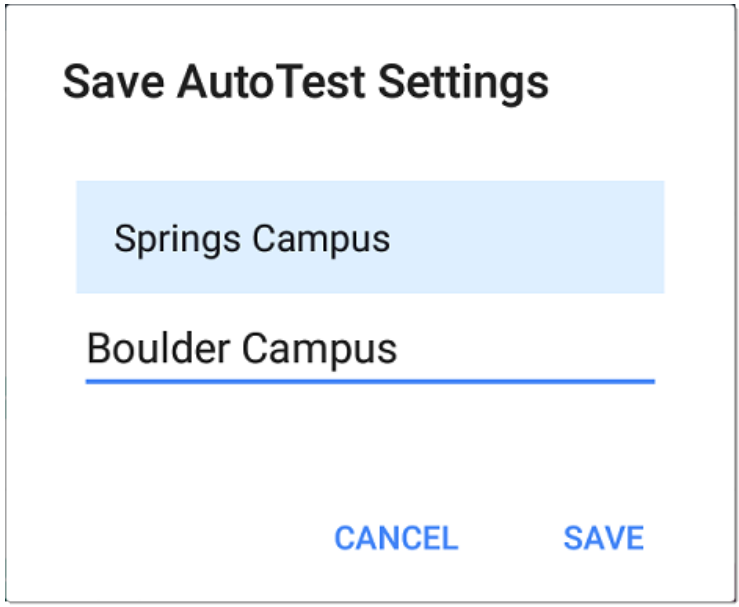
The main AutoTest app screen now displays the custom name in the header.



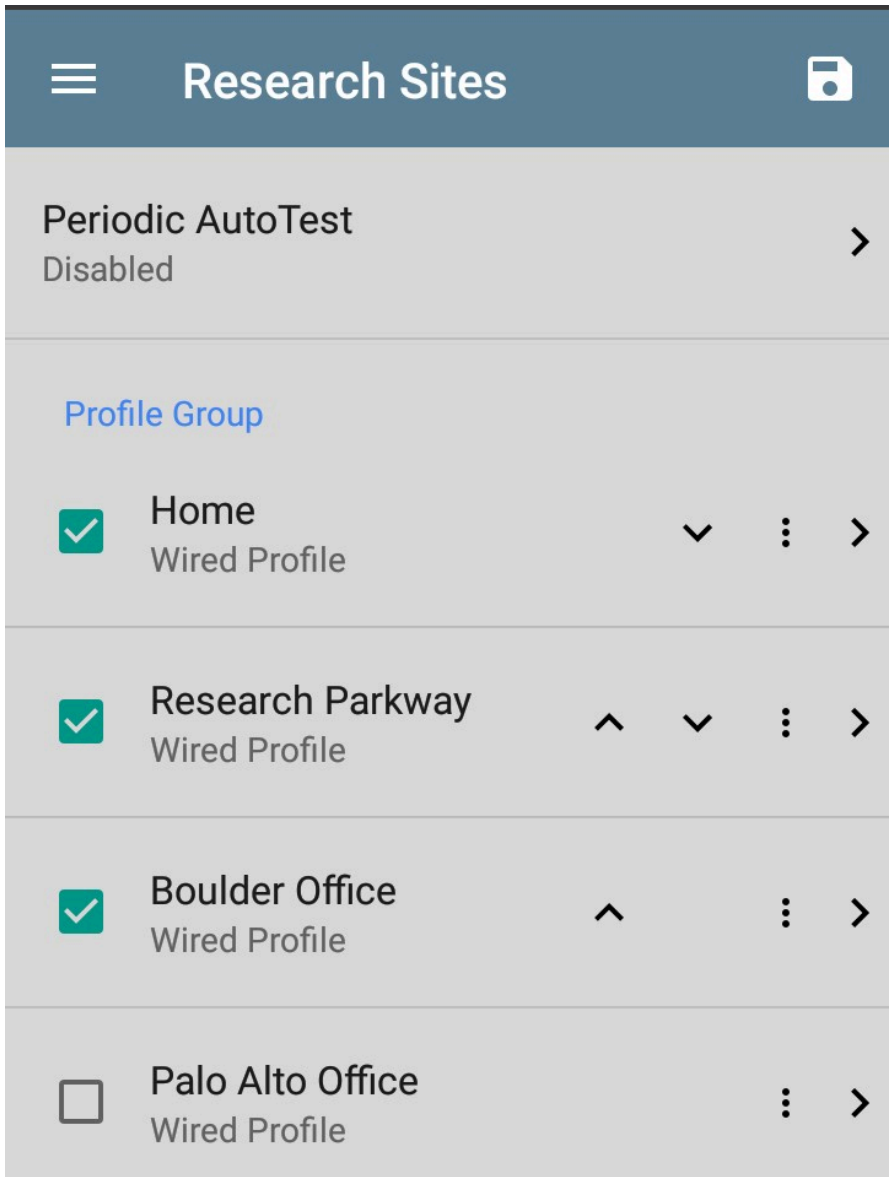
Creating New Profile Groups

To create a new Profile Group, follow these steps:

1. Go to the AutoTest Settings and Profile Group screen by tapping  on the main AutoTest screen.
2. Uncheck the boxes for any Profiles you do not want included in the new Profile Group.
3. Tap the FAB  to add new test Profiles to be included in your new Profile Group.
4. Tap the up and down arrows  to change the order in which the test Profiles run. Unchecked profiles automatically move to the bottom of the list once you leave and revisit this screen.
5. Tap  , and select **Save As**. A dialog box opens, where you can enter the new name.



6. Enter a new Profile Group name, and tap **SAVE**. The LRAT returns to the Profile Group screen with the new group name shown as the title.


Research Sites
Periodic AutoTest
Disabled
Profile Group
Home
Wired Profile
Research Parkway
Wired Profile
Boulder Office
Wired Profile
Palo Alto Office
Wired Profile

Import/Export AutoTest Profiles

In addition to creating new profiles or using defaults, you can also:

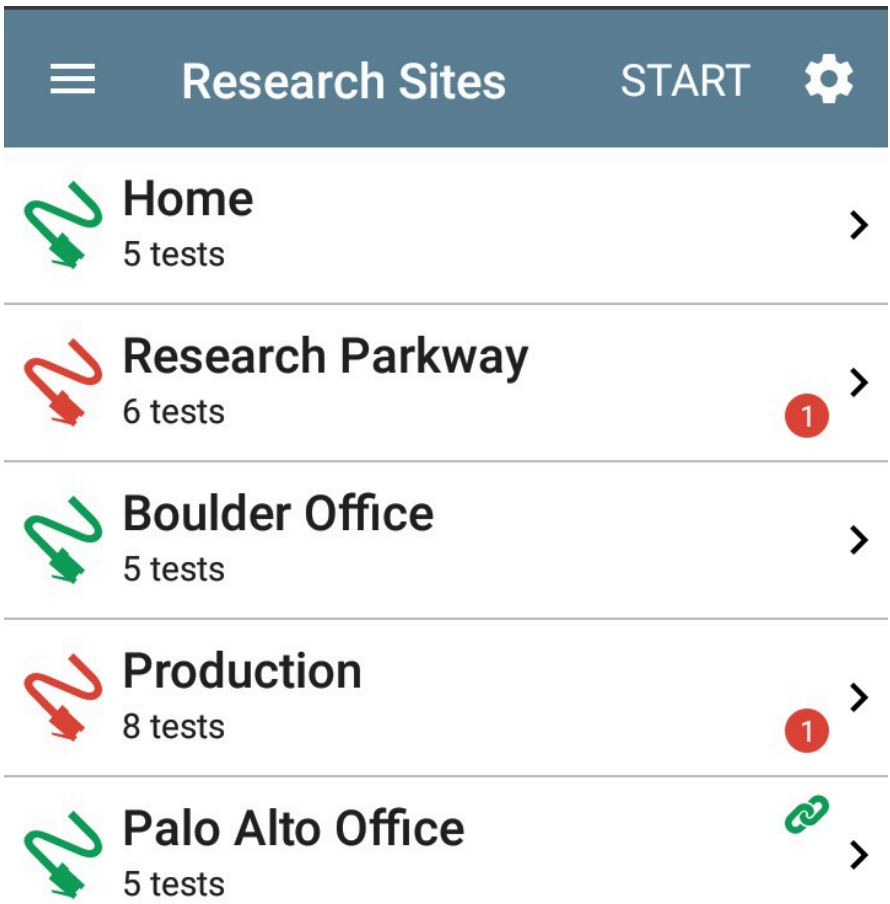
- Import and export profile settings to any connected external or internal storage. See Import/Export Settings.
- Use the Link-Live cloud service to transfer profile settings to other devices in near-real time. See Transferring AutoTest Settings to Other Devices Using Link-Live.

Back to Title and Contents

Main AutoTest Screen

To open the AutoTest app, tap the AutoTest icon on the Home screen.

Tap the **START** button on the main AutoTest screen to run all the Profiles in the currently active Profile Group.



The AutoTest screens display icons that correspond to the type of profile, test, or measurement. After running, these icons change color to indicate the status of the test:

- **Green** indicates a successful test or measurement within the set threshold.
- **Yellow** indicates a Warning condition.
- **Red** indicates test Failure.

The number of warnings or failures within each test profile is also displayed in a colored circle to the right of each profile card: 2 1 (2 Warnings, 1 Failure). The thresholds that control the colored test gradings are adjustable in the settings screens for each profile and test type.

The green link icon indicates an active network connection.

Each profile and test is summarized on a card. Tap a profile's or individual test's card to open and view test result details, including the causes of any Warnings or Failures.

Back to Title and Contents

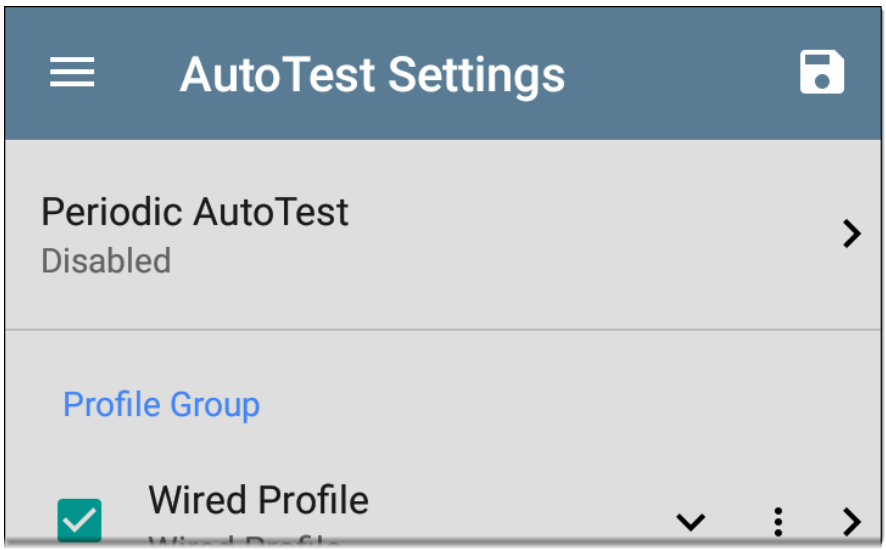
Periodic AutoTest

The Periodic AutoTest feature allows you to run AutoTests at set time intervals.

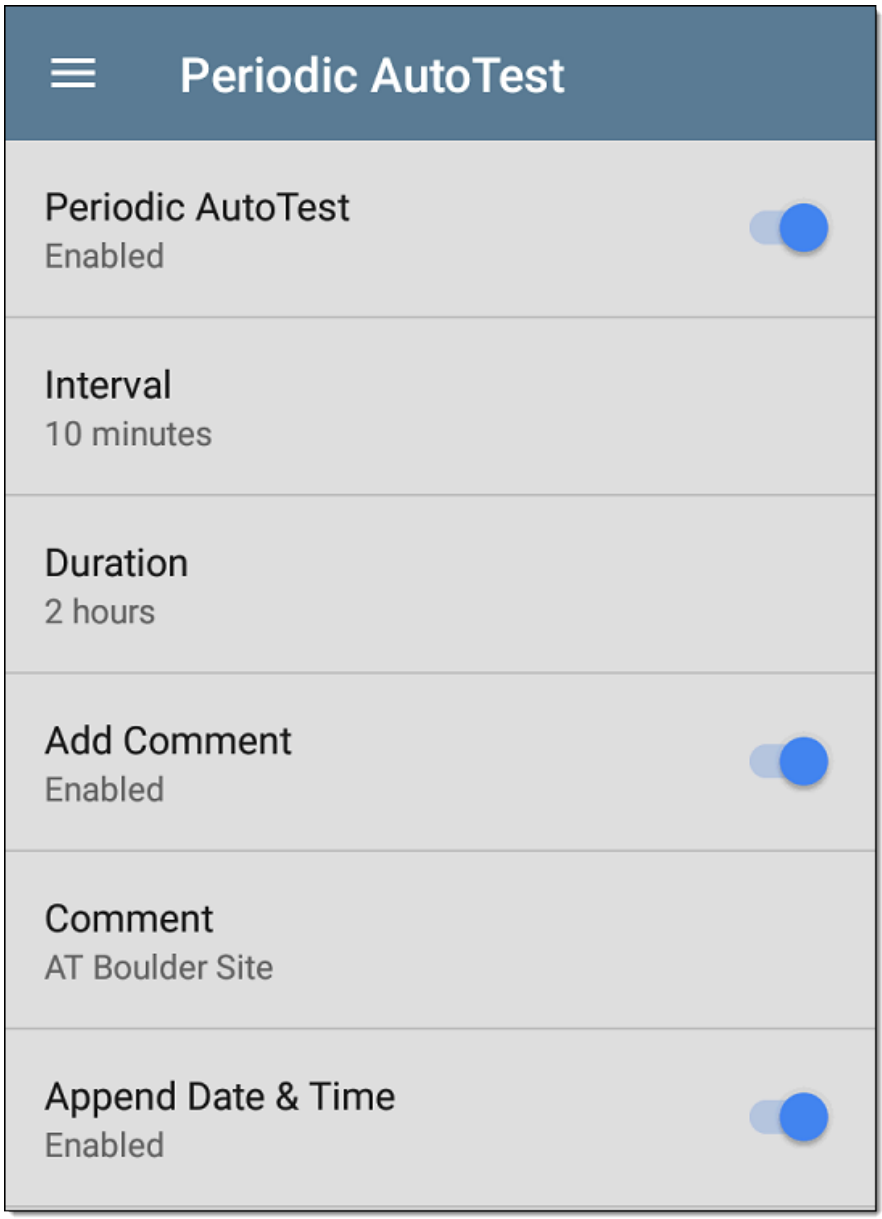
> NOTE: Periodic AutoTest is available for the LRAT-4000 only.

Periodic AutoTest Settings

To enable and configure Periodic AutoTest, open the AutoTest Settings and Profile Group screen, and tap **Periodic AutoTest**.



The Periodic AutoTest settings screen displays the following options:



Tap the **Periodic AutoTest** field to enable, and adjust the settings below as needed.

Interval: Amount of time between each AutoTest run

Duration: Total length of time Periodic AutoTests run

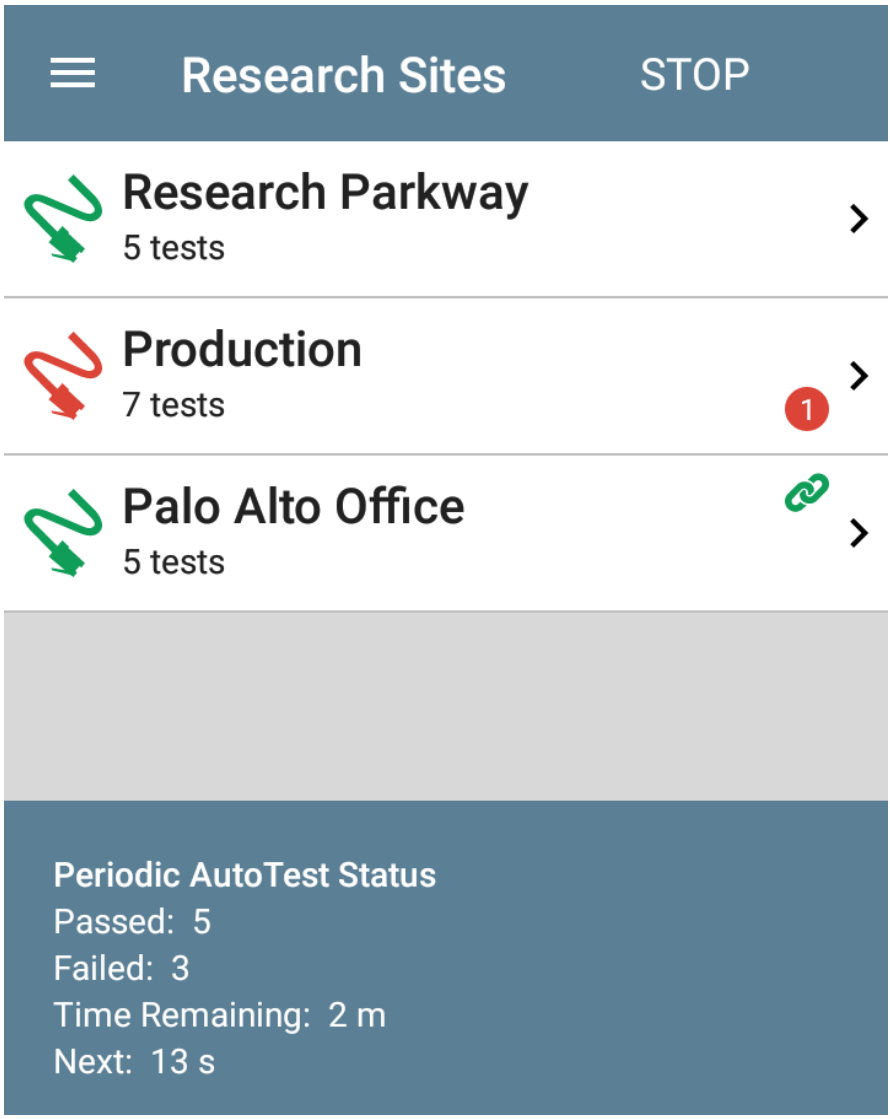
Add Comment: Enabling this setting allows you to attach a comment to the Periodic AutoTest result in Link-Live Cloud Service. The comment appears as a label on the Link-Live.com Results page. This setting and the **Comment** setting below are enabled by default.

Comment: This field appears if the **Add Comment** setting is enabled. Enter the label you want to be attached to the uploaded Periodic AutoTest result on Link-Live. The default is "Periodic AutoTest."

Append Date & Time: This field appears if the **Add Comment** setting is enabled and adds a numeric date and time to the end of the **Comment** above.

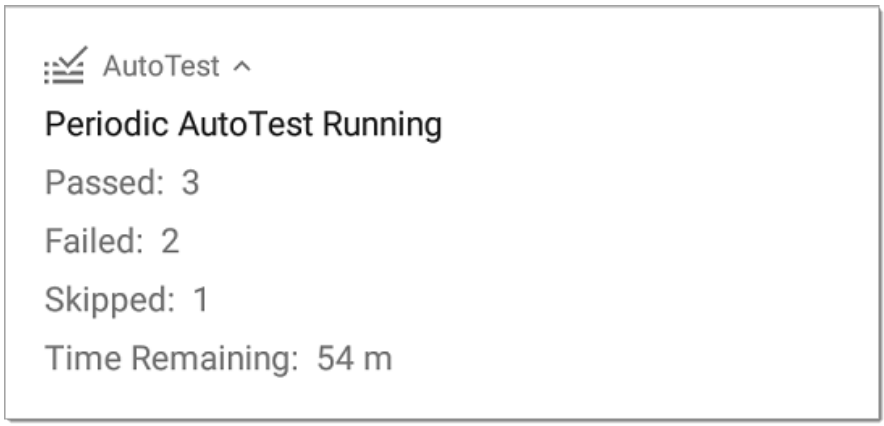
Running Periodic AutoTest

Tap **START** on the main AutoTest screen to begin Periodic AutoTests. AutoTest continues to run at the set Interval for the selected Duration or until you tap **STOP** in AutoTest.



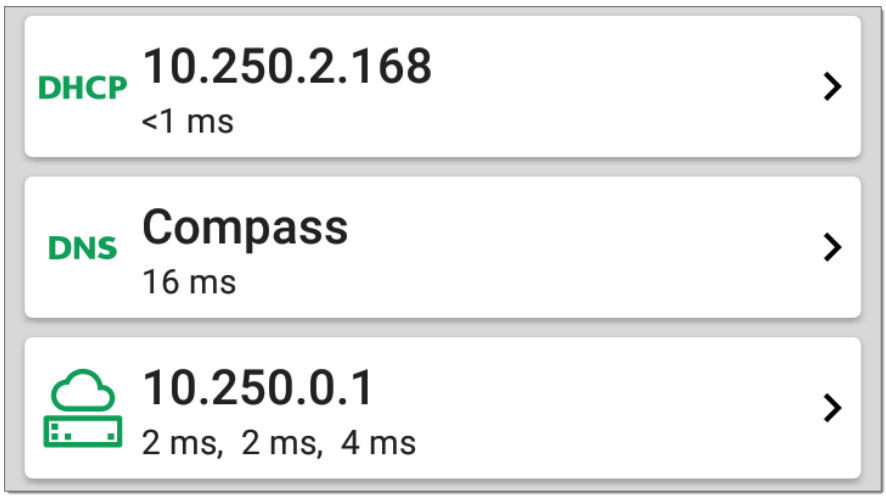
The Periodic AutoTest Status is summarized at the bottom of the AutoTest screens. Passes and failures are reported for each run of the entire Profile Group, rather than individual Profiles. Periodic AutoTests are skipped if the previous interval's test is still running when the next time interval occurs, such that the next run could not start.

The Periodic AutoTest icon  appears in the top Status Bar when Periodic AutoTest is running or has completed. Drag down on the Status Bar to view the corresponding notification.



NOTE: AutoTest has priority control of the Test Ports, so other apps, including Discovery, are paused while AutoTest completes.

DHCP, DNS, and Gateway Tests



These tests are included in Wired AutoTest Profiles.

Access AutoTest's DHCP, DNS, and Gateway tests from the Wired Profile settings screen, or by tapping the settings button from the full results screen for each test type.

Tap blue links or the blue action overflow icon ••• on the test results screens for additional actions.

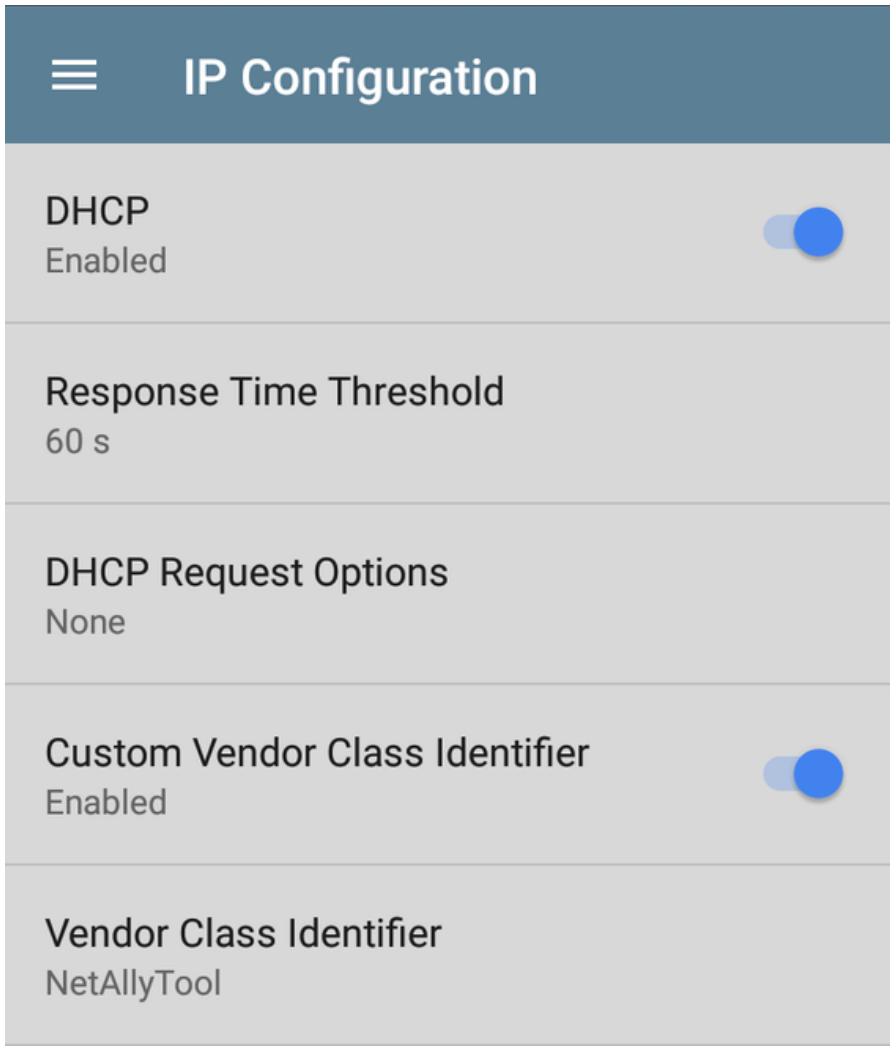
DHCP or Static IP Test

The DHCP (Dynamic Host Configuration Protocol) test indicates whether the LRAT receives an IP address assignment from the DHCP server.

DHCP Settings – IP Configuration

To open the IP Configuration screen, either:

- Open a Wired Profile, tap the DHCP summary card, and then tap the settings button  on the DHCP test results screen.
- Tap the main menu icon  , select **AutoTest Settings**, open a Wired Profile, and then tap **IP Configuration**.



DHCP

DHCP is enabled by default. Tap the toggle button to disable DHCP and enter static IP addresses, as described below.

(DHCP only) Response Time Threshold

(Appears only if DHCP is enabled.) Tap this field to select a value or enter a custom value to set

how long the LRAT waits for a DHCP server response before failing the DHCP test.

DHCP Request Options

(Appears only if DHCP is enabled.) Tap this field to select one or more DHCP request options.

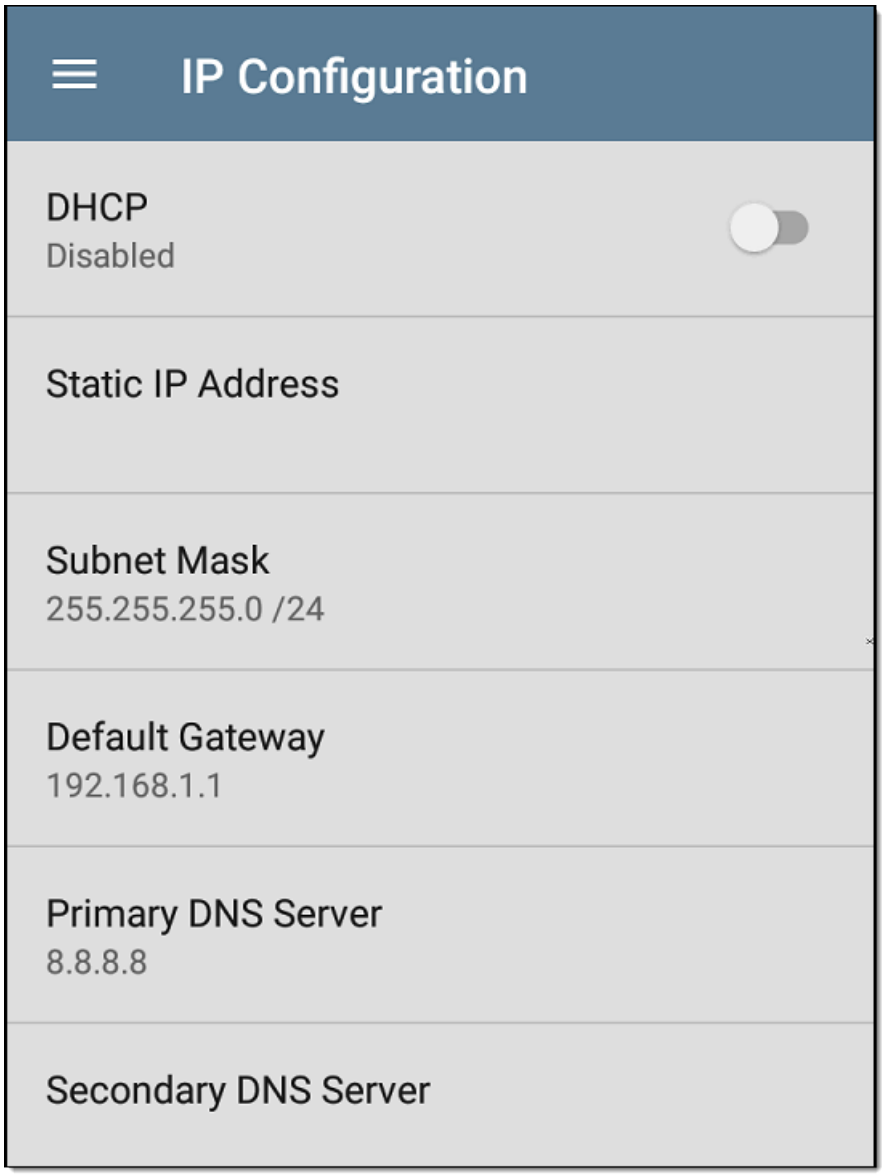
Custom Vendor Class Identifier

Custom Vendor Class Identifier is disabled by default. Tap the toggle button to enable the Vendor Class Identifier field, as described below.

Vendor Class Identifier

(Appears only if Custom Vendor Class Identifier is enabled.) Tap this field to type the vendor class identifier.

Static IP Address



The Static IP address fields for **Subnet Mask, Default Gateway**, and **Primary** and **Secondary DNS Servers** only appear if DHCP is disabled. Tap each field to open a pop-up number pad and enter the static addresses as needed. Tap **OK** to save your entries.

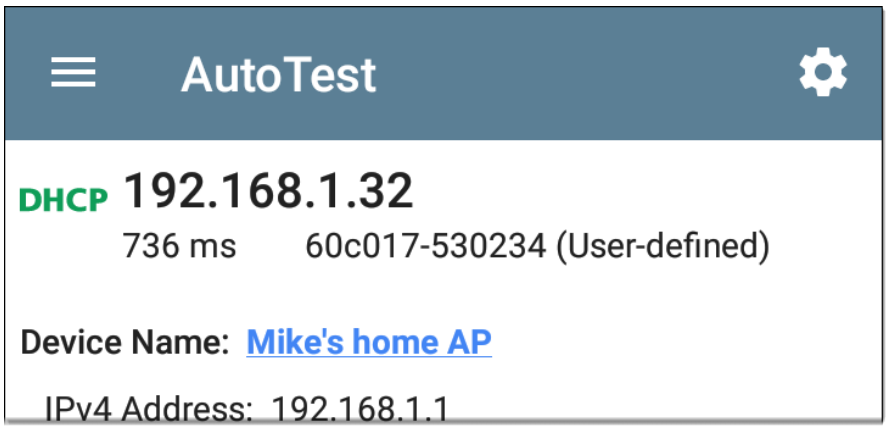
DHCP Test Results

When DHCP is enabled, the DHCP test card and results screen are displayed in the Profile.

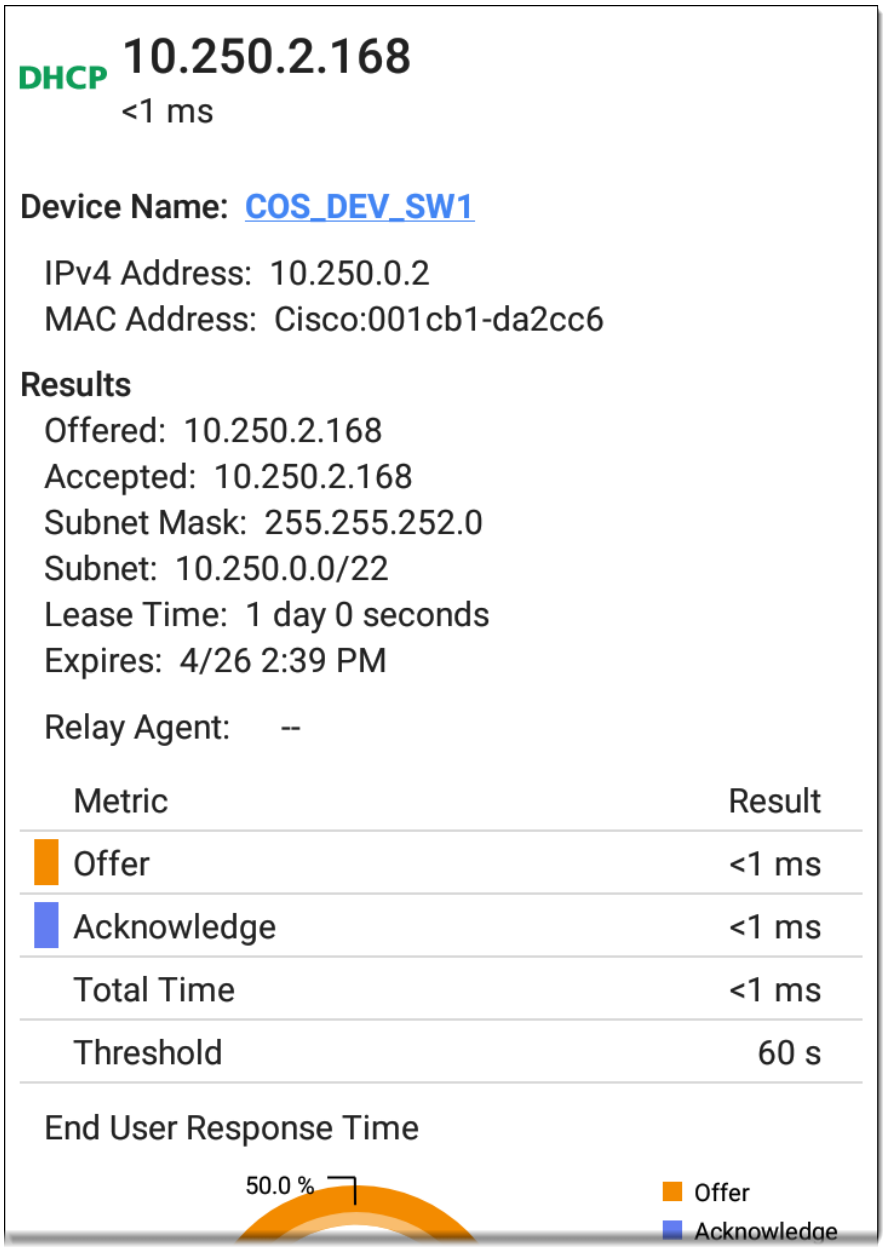
The DHCP Test card displays the DHCP server's IP address and the total time for the discover, offer, request, and acknowledgment to complete.

Tap the card to open the DHCP test screen.

> NOTE: If a **User-Defined MAC** is enabled for this connection in General Settings, (User-defined) appears next to the MAC address beneath the DHCP IP address on results screen.



DHCP Test Results Screen



Device Name: The discovered name of the DHCP Server, or, if no name could be discovered, the IP address

IPv4 Address: IP address of the server

MAC Address: Server's MAC address. Two dashes -- indicate that no MAC address was provided from the server.

Results

Offered: IP address offered by the DHCP server

Accepted: IP address accepted by the LRAT

Subnet Mask: Used to determine which addresses are local and which must be reached via a gateway

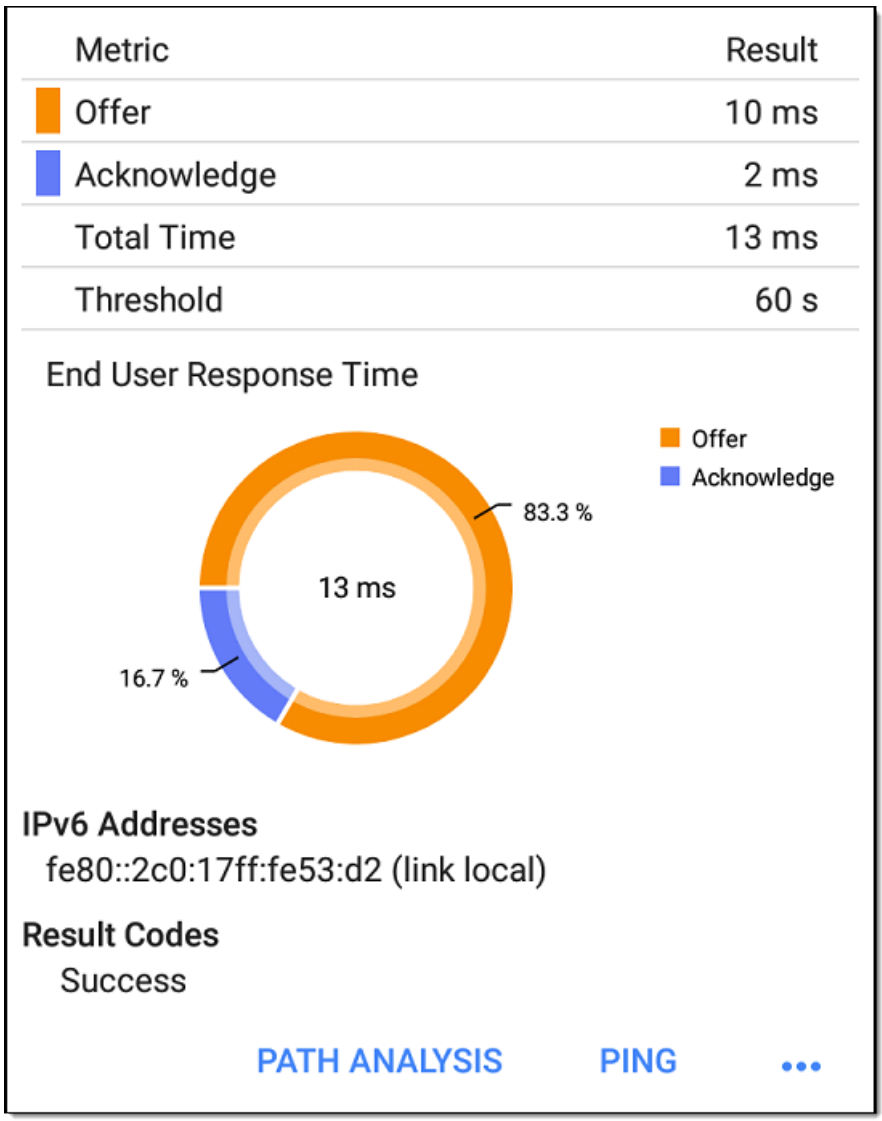
Subnet: Combination of the subnet mask and the offered IP address

Lease Time: The amount of time the IP address is leased to the LRAT by the DHCP server

Expires: Expiration date and time of the IP address

Relay Agent: If a BOOTP DHCP relay agent is present, this field shows its IP address. The relay agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

End User Response Time table and chart: Breakdown of the times for the process of acquiring a DHCP IP address



Offer: Time between when the LRAT sent the discovery and received an address offer from the DHCP server

Acknowledge: Time between LRAT sending the request and receiving the acknowledgment from the DHCP server

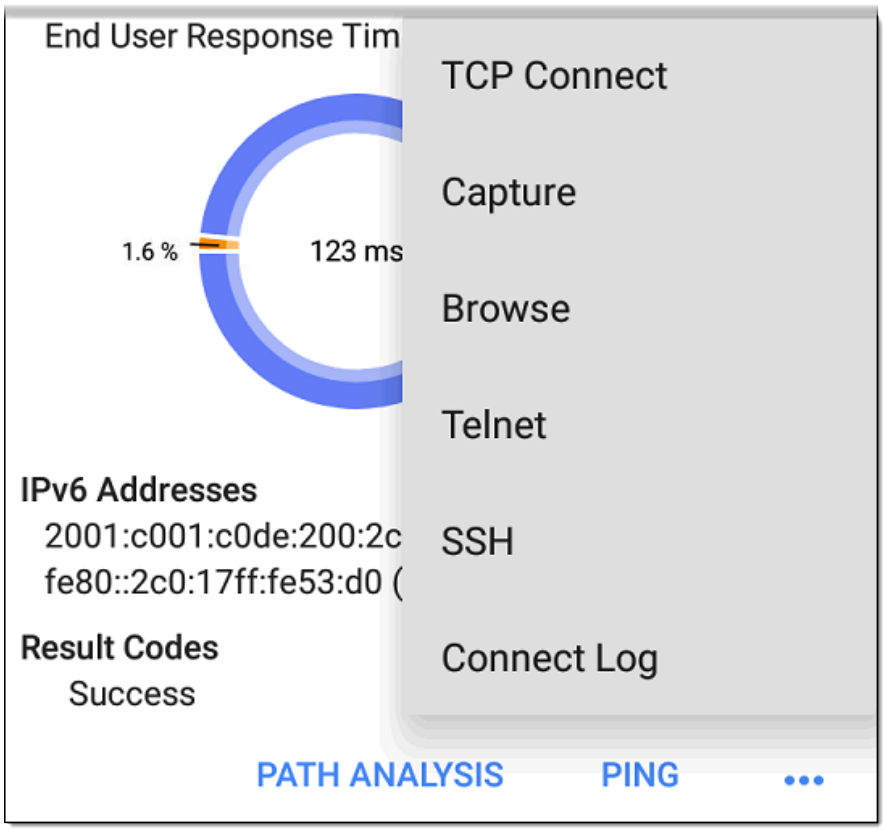
Total Time: Total amount of time consumed by the DHCP process

Threshold: The DHCP Response Time Threshold from the DHCP test settings, which controls how long the LRAT waits for a DHCP server response before failing the DHCP test.

End User Response Time: A pie chart showing the Offer and Acknowledgment times as percentages

IPv6 Addresses: Addresses obtained via router advertisement

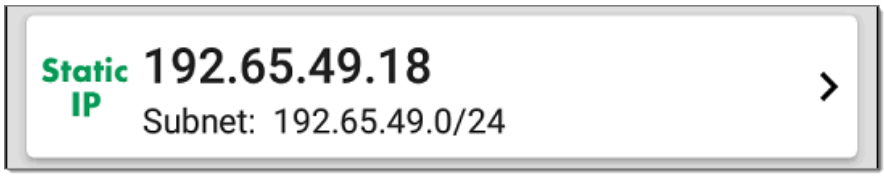
Results Codes: Final status of the test (Success or Failure)



The additional actions available on the DHCP test screen include opening the Path Analysis, Ping/TCP, or Capture apps populated with the DHCP server address, browsing to the IPv4 address in the web browser, starting a Telnet or SSH session, or viewing the Connect Log.

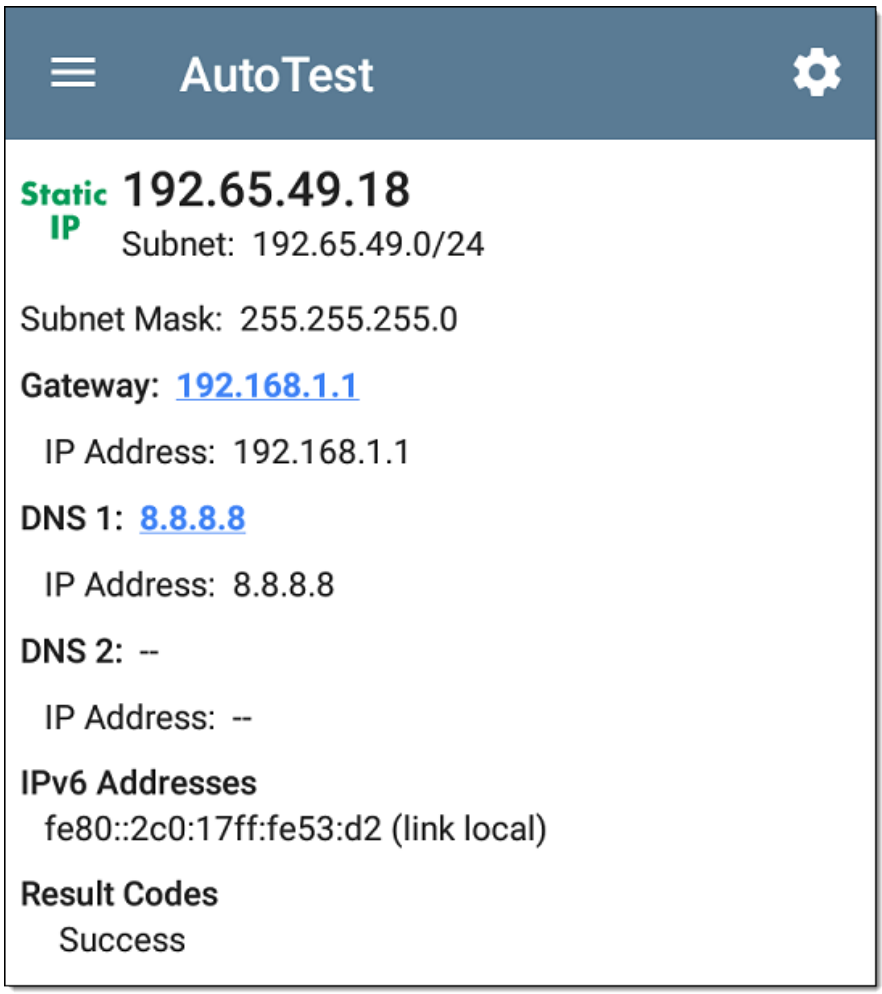
Static IP Test Results

If DHCP is disabled, the DHCP test becomes a "Static IP" test and the Subnet and addresses that were entered in the DHCP test settings are displayed.



The Static IP card displays the configured IP and Subnet addresses.

Tap the card to open the test results screen.



The Static IP test screen displays the configured addresses.

Subnet: Combination of the subnet mask and the offered IP address

Subnet Mask: Used to determine which addresses are local and which must be reached via a gateway

Gateway: Resolved hostname of the Gateway or its IP address if no name could be discovered

IP Address: IP address of the Gateway

DNS (1 and 2): Names and IP addresses of Primary and Secondary DNS servers

IPv6 Addresses: Addresses obtained via router advertisement

Results Codes: Final status of the test (Success or Failure)

Duplicate IP Address

The DHCP and Static IP tests also detect and report the presence of a device using the same IP address (duplicate IP). If the configured address is in use, the AutoTest fails.

IP Address In Use By: Shows the name of the device currently using the configured static IP address. Tap the blue underlined link to open a Discovery Details screen for the device.

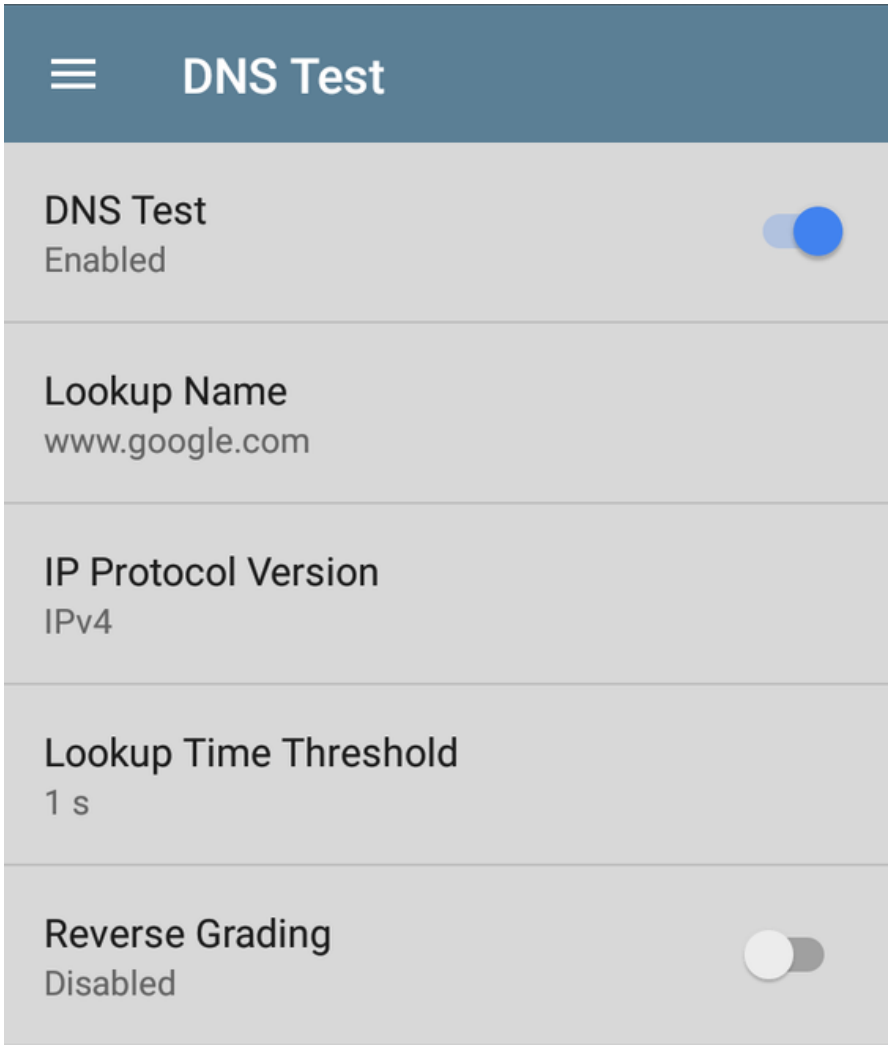
MAC Address: MAC of the device using the IP address

DNS Test

For overview information, see DHCP, DNS, and Gateway Tests.

The DNS (Domain Name System) server test checks the performance of DNS servers resolving the specified URL. The LRAT obtains DNS addresses through DHCP or static address configuration.

DNS Test Settings



DNS Test

To disable the DNS test in your current AutoTest, tap the top field on the this screen to set it to Disabled. The DNS card still appears on the main AutoTest results screen so that you can still see the addresses of the DNS servers. However, the

following lookup values are set to "--", and the Result Code is set to “Test is disabled”.

Lookup Name

This is the URL the DNS server(s) attempts to resolve. Tap the field to enter a URL other than the default: www.google.com.

IP Protocol Version

Tap the field to switch between IPv4 and IPv6.

Lookup Time Threshold

This threshold controls how long the LRAT waits for a response from the DNS server(s) before the test is failed. The default is 1 second. Tap the field to select or enter a new threshold.

Reverse Grading

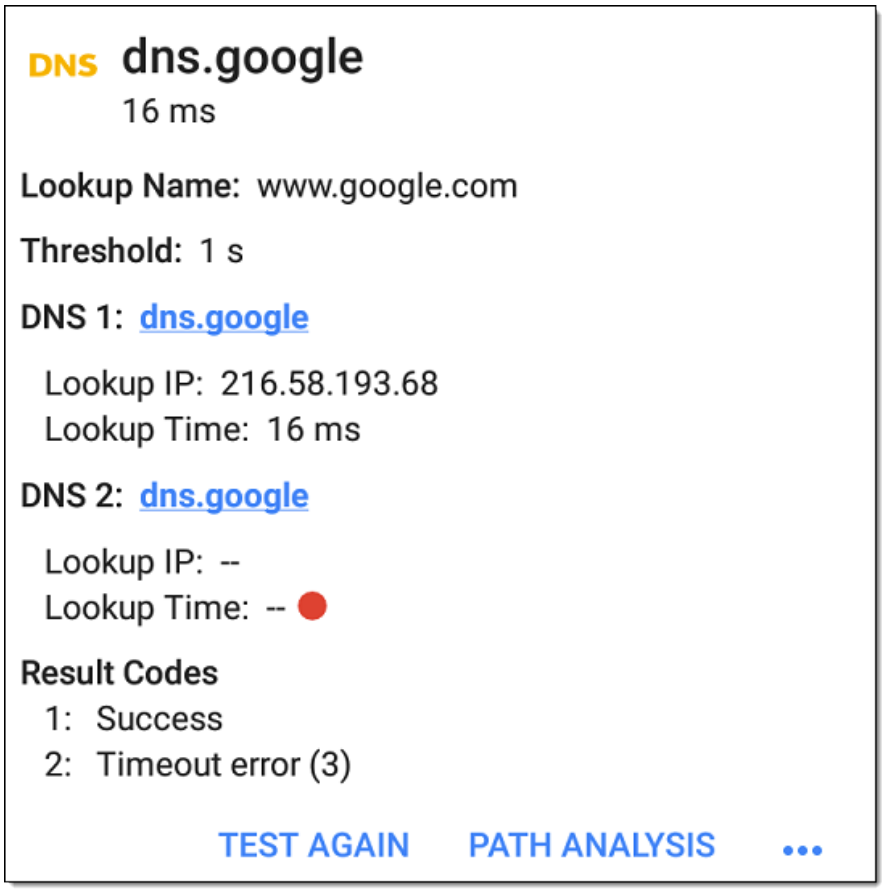
When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

DNS Test Results

The server name and lookup time for DNS 1 are shown on the DNS test card.

Tap the card to open the DNS test results screen.

DNS Test Results Screen



Lookup Name: Name resolved by the DNS servers

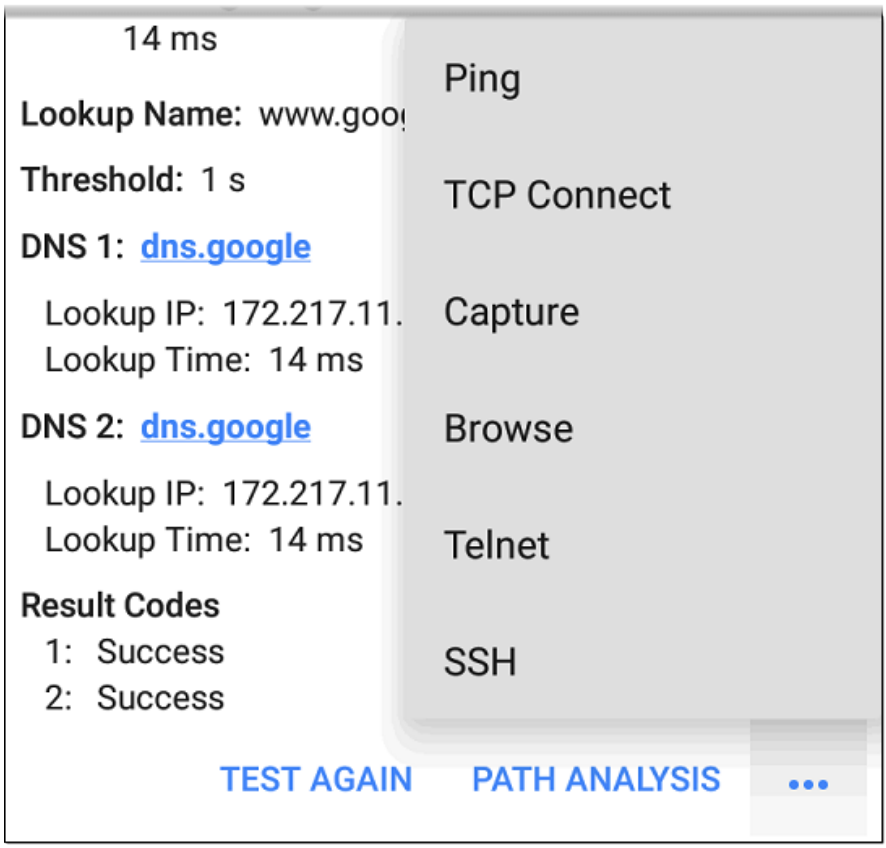
Threshold: Lookup Time Threshold from the DNS test settings

DNS #: Name of the listed DNS server

Lookup IP: Resolved IP address

Lookup Time: Time to receive the IP address after the lookup request sent

Results Codes: Final status of the test (Success or Failure) for each DNS server



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the DNS **Test Again**, open another app

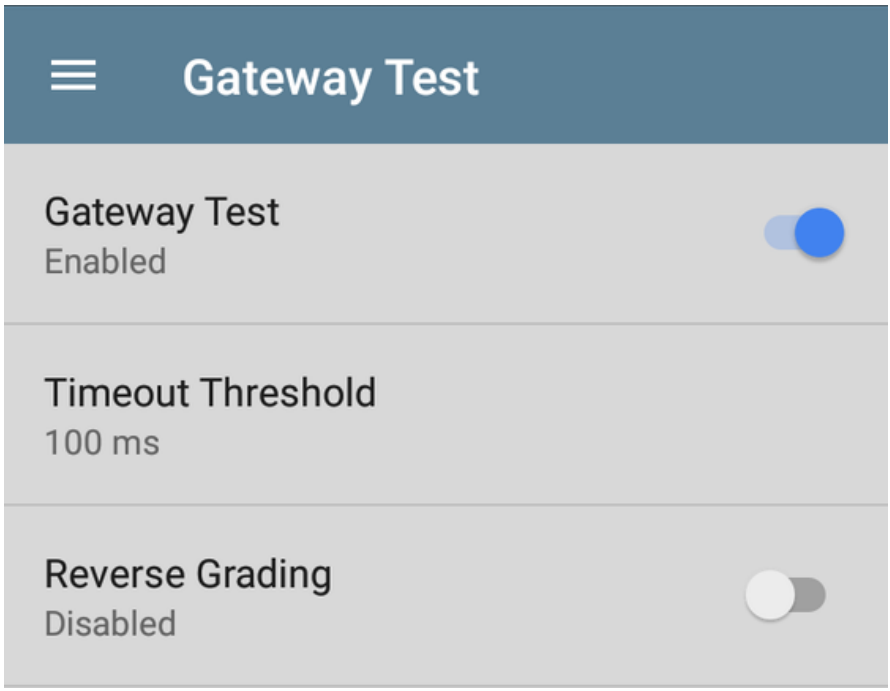
populated with the name and IP address of DNS 1, or **Browse** to the Primary DNS server in your web browser.

Gateway Test

For overview information, see DHCP, DNS, and Gateway Tests.

This test indicates whether the default Gateway could be successfully pinged and identifies the address of the current IPv4 and IPv6 routers.

Gateway Test Settings



Back to Title and Contents

Gateway Test

To disable the Gateway test in your current AutoTest, tap the top field on the this screen to set it to Disabled. The Gateway card still appears on the main AutoTest results screen so that you can still see the addresses of the Gateway servers. However, the following lookup values are set to "--", and the Result Code is set to “Test is disabled”.

Timeout Threshold

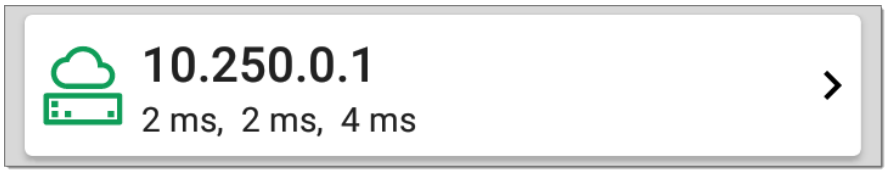
Indicates how long the LRAT waits for a response from the gateway before grading the test as a fail. Tap the field to select one of the value options, or enter a custom value.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

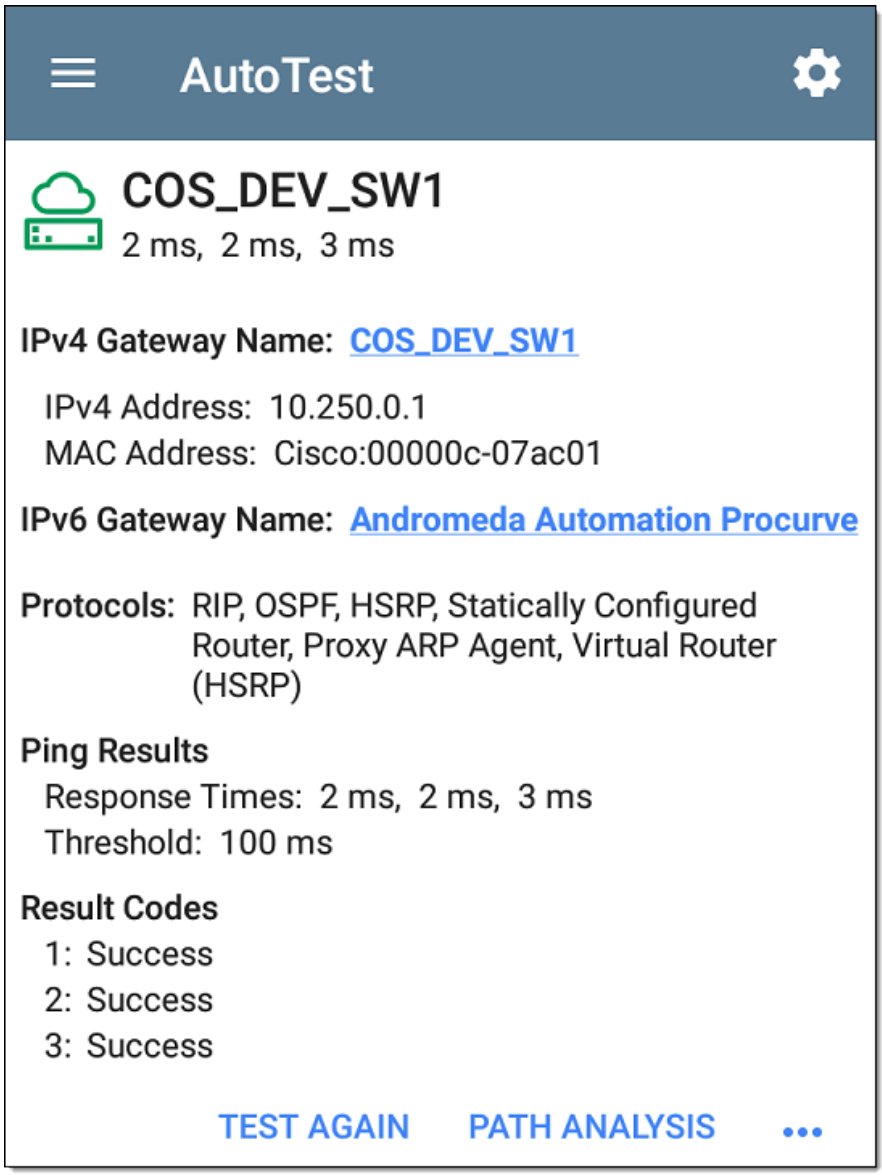
Gateway Test Results

LRAT gets the Gateway's IP address from DHCP or the static IP configuration, and uses SNMP to acquire system group information and statistics for the port that services the LRAT's subnet. See Discovery Settings for information about SNMP configuration.



The Gateway test card shows the gateway's IP address and the three Ping response times.

Gateway Test Results Screen



IPv4 Gateway Name: Resolved hostname of the Gateway or its IP address if no name could be discovered

IPv4 Address: Internal IPv4 address of the Gateway

MAC Address: Server's MAC address. Two dashes -- indicate that no MAC address was provided from the server.

IPv6 Address: Router's IPv6 address (if available)

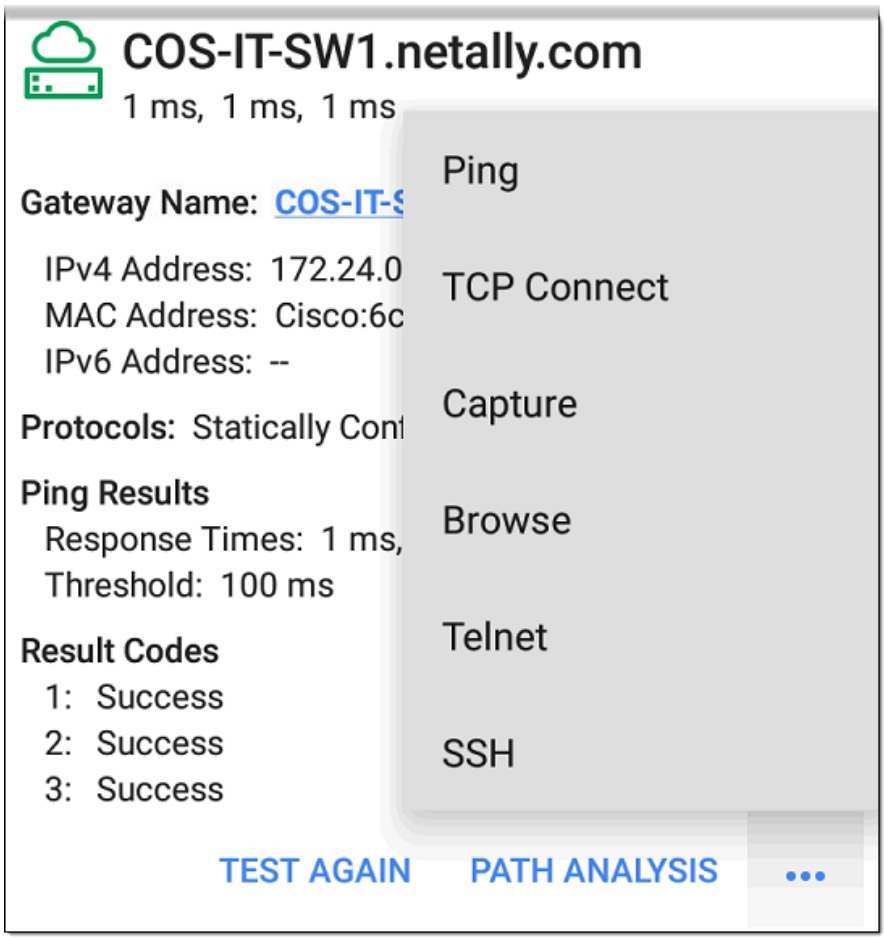
IPv6 Gateway Name: Name advertised by the IPv6 router (if available)

Protocols: Routing protocols the LRAT used to obtain the Gateway data

Ping Results

- **Response Times** from the three Pings sent to the gateway
- **Threshold**: Gateway Timeout Threshold configured in the gateway settings

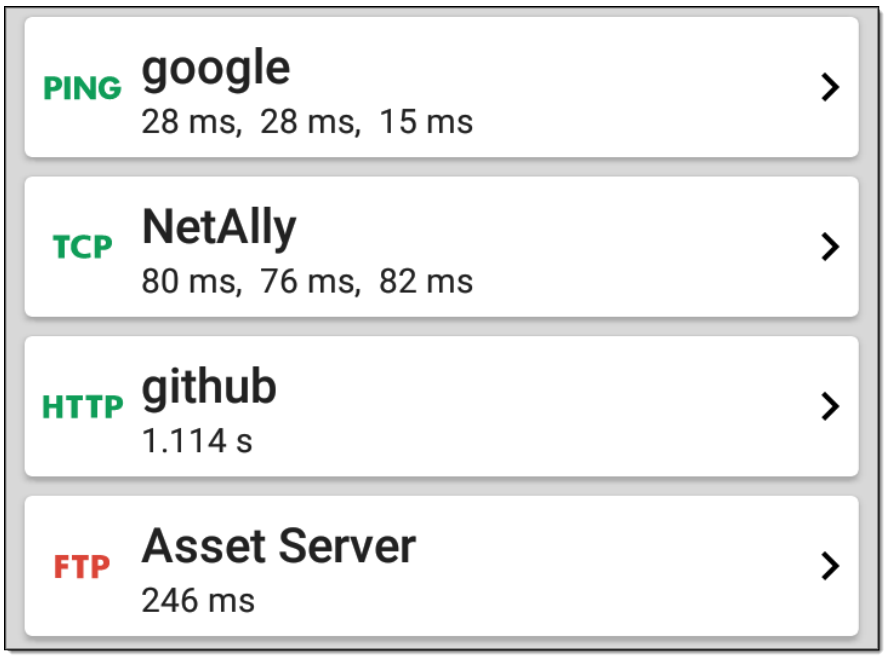
Results Codes: Final status of the test (Success or Failure) for each of the three Gateway Pings



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the Gateway **TEST AGAIN**, open another app, **Browse** to the Gateway's IPv4 Address, or start a Telnet or SSH session to the Gateway.

Back to Title and Contents

Test Targets for Wired AutoTest



AutoTest Target tests are user-assignable endpoints to which LRAT 3000-4000 attempts to connect each time the AutoTest profile runs. These tests ensure availability of internal or external websites, servers, and devices to users of your network.

Tap a link below to go to the test's topic:

Ping

TCP Connect

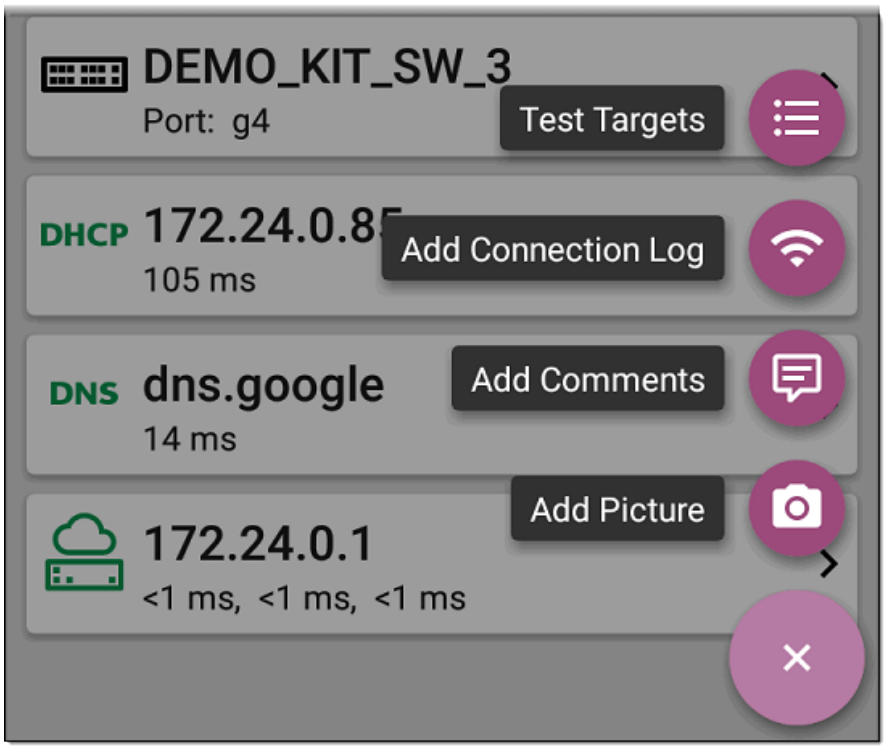
HTTP

FTP

NOTE: HTTP and FTP tests are available on the LinkRunner AT 4000 only.

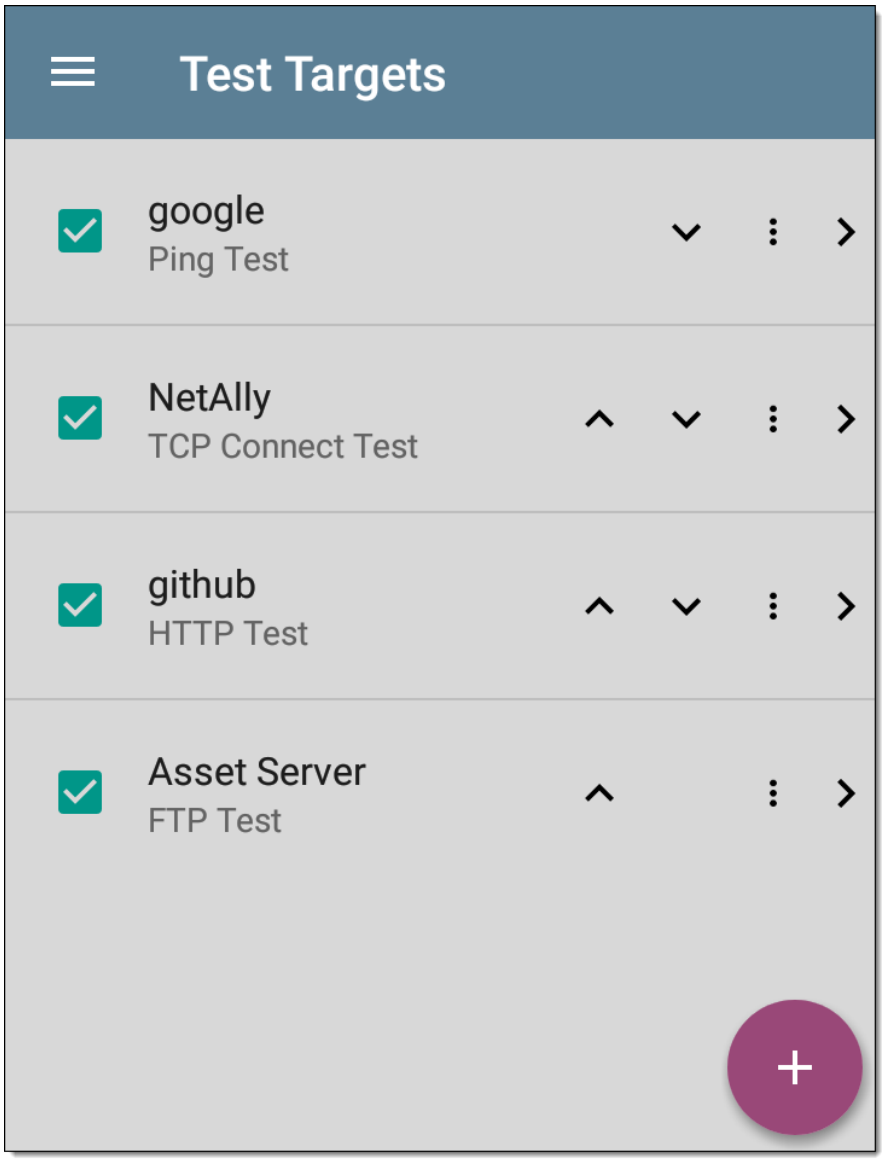
Adding and Managing Test Targets

To add test targets to AutoTest profiles and manage your saved targets, open the **Test Targets** screen from the Wired Profile Settings or by tapping the FAB + on the Wired results screens.



The Test Targets screen lists all of the defined and saved Test Targets. Checked boxes indicate the targets enabled in the current Profile. (Test

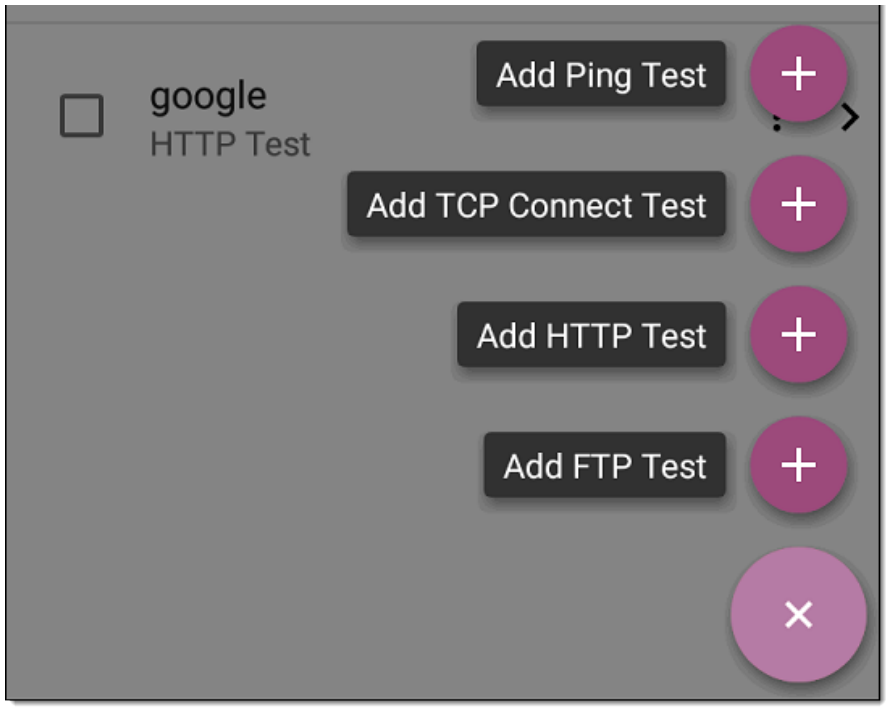
Targets can be added to and used in any number of Wired Profiles.)



On the Test Targets screen, you can perform these actions:

- Select the checkboxes for each Target you want to include in the current profile.

- Tap the up and down arrows to reorder the saved Test Targets on this screen and the main AutoTest Profile screen.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a target test.
  CAUTION: When you delete a Test Target, you delete it from all Profiles. To remove a Test Target from the current profile, simply uncheck it.
- Tap the FAB icon + to add a new target test: Ping, TCP Connect, HTTP, or FTP (FTP and HTTP available for LinkRunner AT 4000 only).

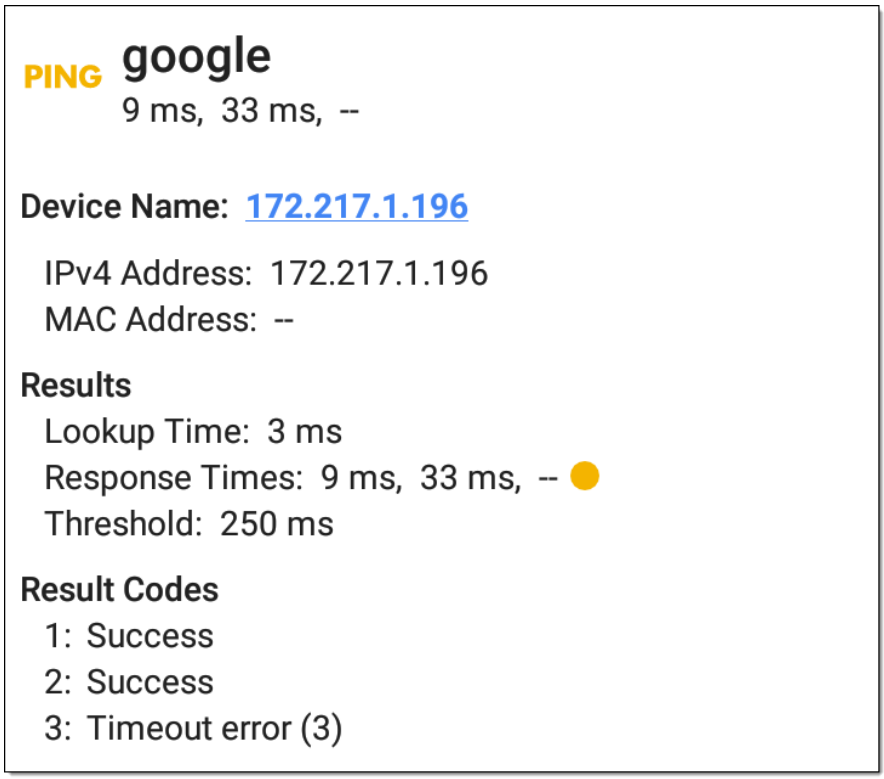


- Tap any target test name to open that test's settings. You can then enter a custom test name, target address, or thresholds. For more information on settings, see:
  - Ping Test
  - TCP Connect Test
  - HTTP Test (LinkRunner AT 4000 only)
  - FTP Test (LinkRunner AT 4000 only)

Target Test Results Screens

The Target Test type icons display green, yellow, or red to indicate the status (or grade) of the completed test portions: **Success**/**Warning**/**Fail**.

As an example, in the Ping test image below, the entire Ping test is graded with a Warning because the third Ping was not returned within the Timeout Threshold configured in the settings.



The third Response Time displays two dashes -- to indicate that no response was received, and under the Results heading, the yellow dot points out the third Response Time as the reason for the Warning. Additionally, the third Result Code lists "Timeout error" as the reason for the Warning.

Additional Target Test Actions

After the Target test has completed, tap any of the blue links to perform additional actions, including opening other testing apps.

- Tap the blue linked Device Name to open a Discovery Details app screen for the selected device. From there, you can open other apps and run additional tests.
- Tap TEST AGAIN to run just the target test again.
- Tap PATH ANALYSISto open the Path Analysis to app with the path destination configured with the current target.
- Tap the action overflow icon ••• to open the listed apps or tools with the target pre-populated, for example:
  - **Ping** or **TCP Connect** to open the Ping/TCP app with the current target address.
  - Capture traffic from the test target.
  - Browse to the target URL on the internet with your web browser app.

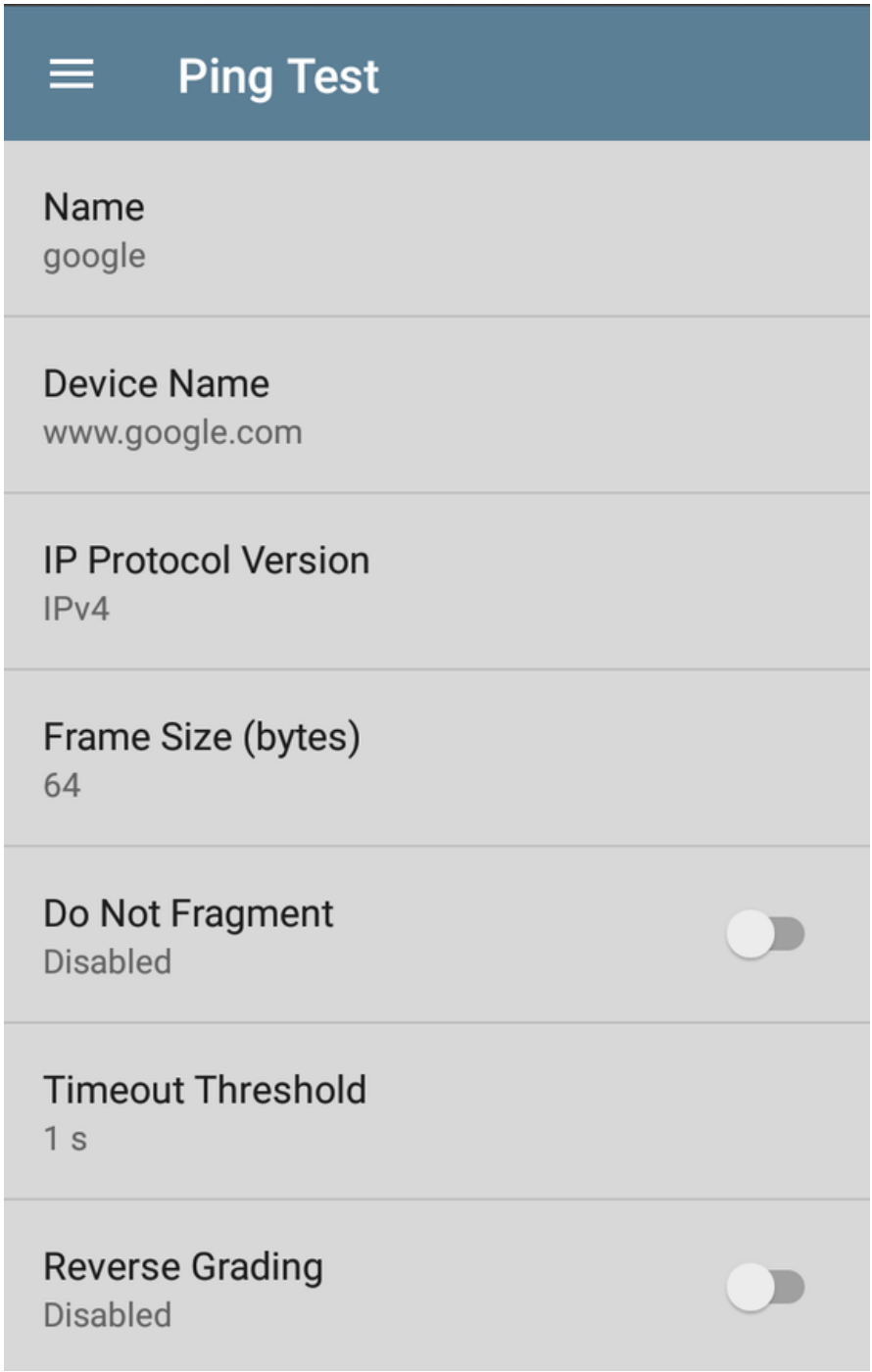
- **Telnet** or **SSH** to open the Telnet/SSH tools with the current target address.

AutoTest Ping Test

A Ping test sends an ICMP echo request to the selected target to determine whether the server or client can be reached and how long it takes to respond. The AutoTest Target Ping Test sends three Pings to the target and reports the response times. The target can be an IPv4 address, IPv6 address, or named server (URL or DNS).

Back to Title and Contents

Ping Test Settings



Name

This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

Device Name

Enter the IP address or URL of the target device. If you enter an IP address, the DNS lookup portion of the test is skipped.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Frame Size (bytes)

This setting specifies the total size of the payload and the header sent. Valid sizes are 64 bytes to 1518 bytes. To test the Maximum Transmission Unit (MTU) along a route to a target, select the MTU frame size you want to test, and set **Do Not Fragment** to **Enabled**.

Do Not Fragment

Tap the toggle button to enable.

Timeout Threshold

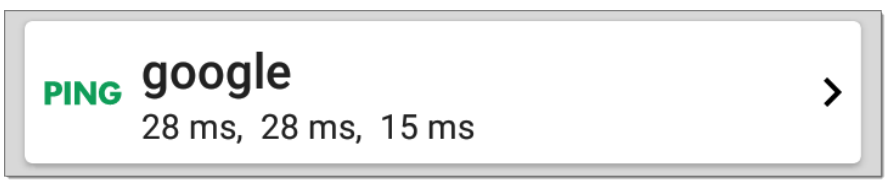
This threshold controls how long the LRAT waits for a response from the target before failing the test.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

For example, you might have a critical server used by an accounting department. This server must be accessible by the accounting VLAN but not by any other networks. To verify the configuration, you could set up a reverse-graded Ping test, and then run a Wired AutoTest profile to the server's guest SSID. The test reports a ping failure, which is the desired outcome.

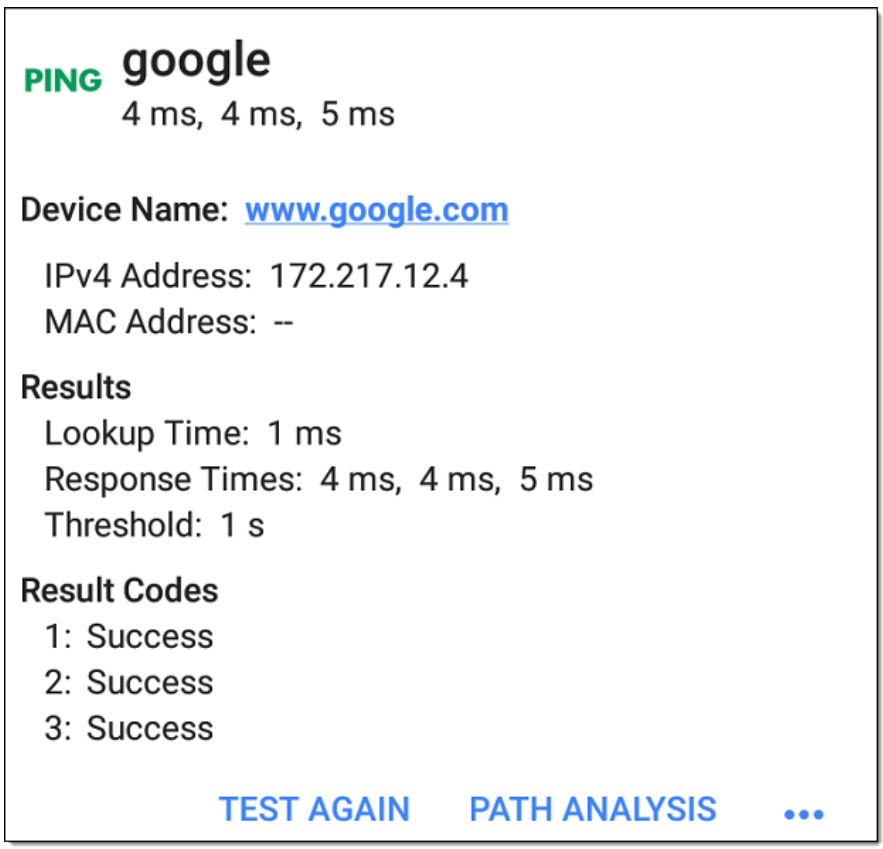
Ping Test Results



The Ping card shows the Ping test name entered in the Ping test settings and the three Ping response times from the target.

Tap the card to open the Ping results screen.

AutoTest Ping Results Screen



Device Name: Hostname or address of the target device.

- **IPv4 or IPv6 Address**: IP address of the target device.

- **MAC Address**: Target device's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

Results

- **Lookup Time**: How long it took to resolve the URL into an IP address.
- **Response Times**: How long it took for the LRAT to receive a response from the target after sending each of the three connections.
- **Threshold**: The Timeout Threshold indicated in the test's settings.

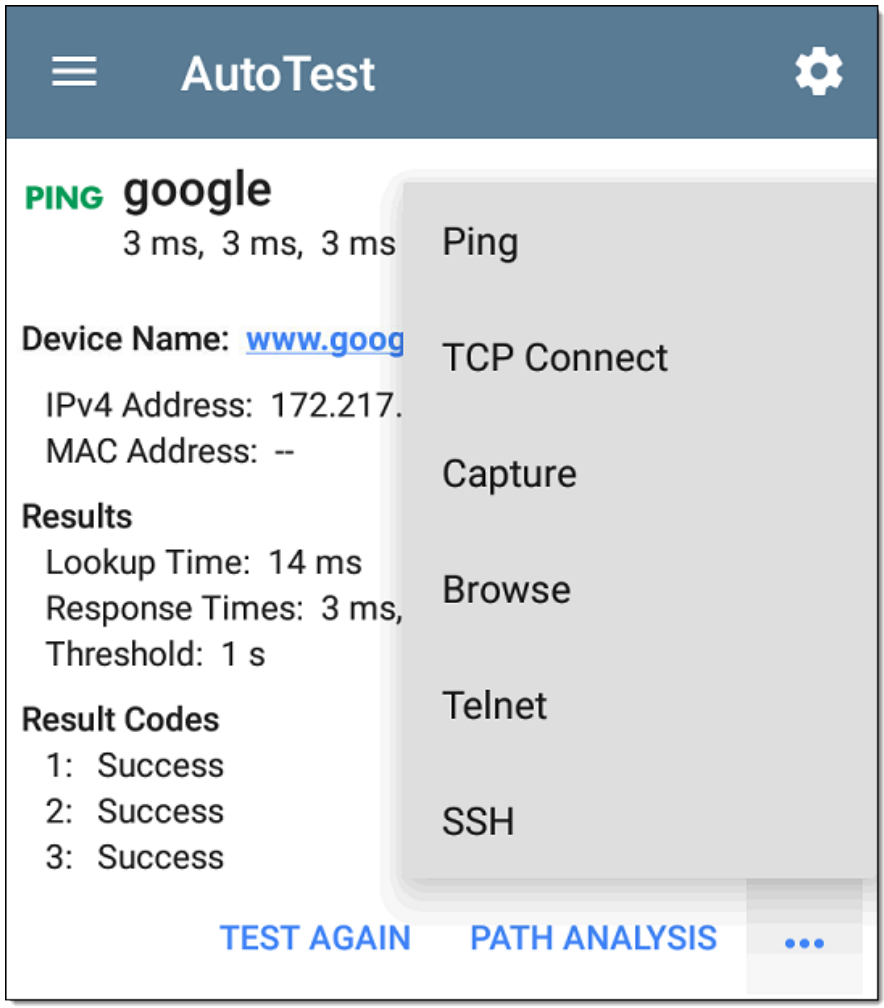
Results Codes: Final status of the test (Success or Failure) for each of the three connections.

Other Actions

Use the **blue links** or the blue action overflow icon ••• button at the bottom of the test results screens to perform other actions.

- Tap **TEST AGAIN** to run the Ping test again.
- Tap **PATH ANALYSIS** to open the Path Analysis app with the Ping test's information.

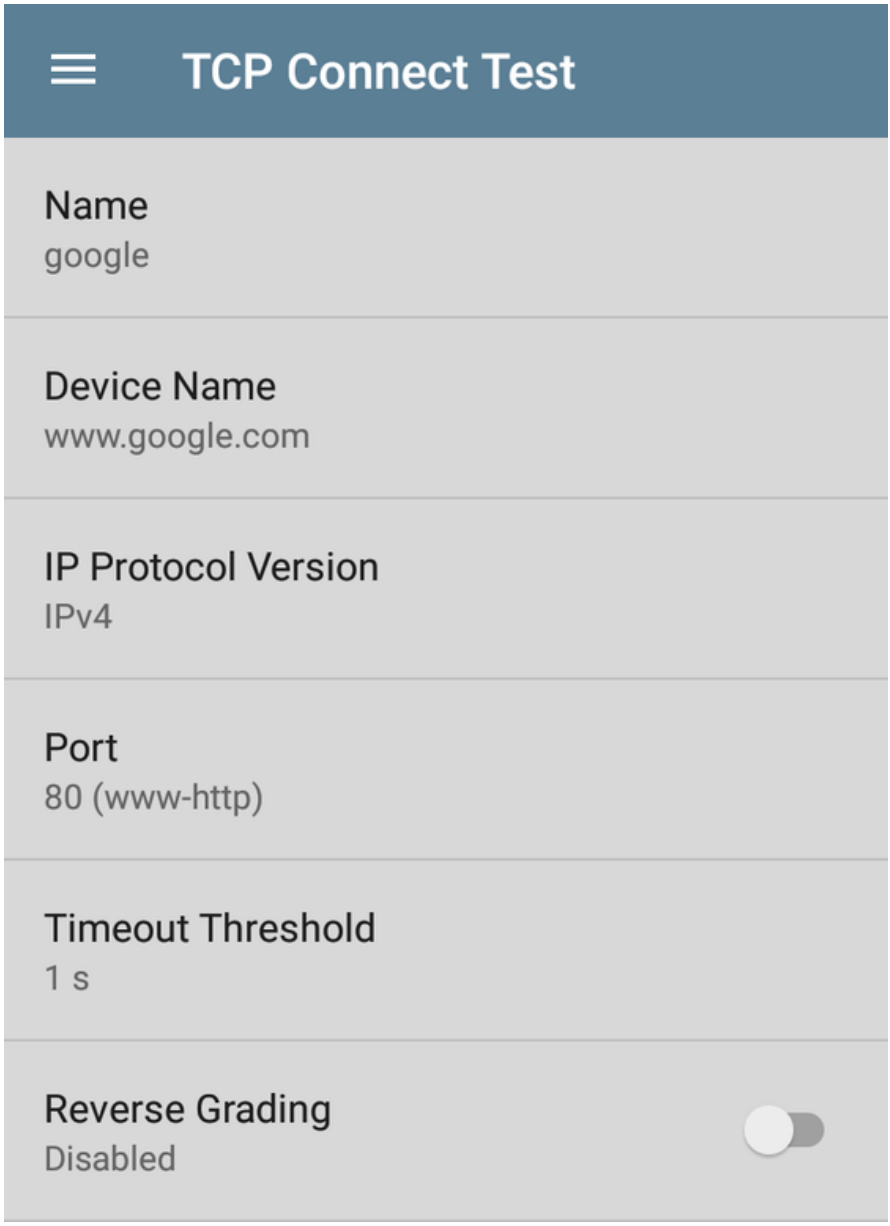
- Tap the blue action overflow icon ••• to open another testing app (Ping, TCP Connect, or Capture), to **Browse** to the Ping target address in your web browser, or to start a Telnet or SSH session.



AutoTest TCP Connect Test

A TCP Connect test opens a TCP connection with the selected target to test for port availability using a 3-way handshake (SYN, SYN/ACK, ACK). The AutoTest Target TCP Connect test runs three connection tests and reports the response times.

TCP Connect Test Settings



Name

This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

Device Name

Enter the IP address or URL of the server you want to ping. If you enter an IP address, the DNS lookup portion of the test is skipped.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Port

Specify the TCP port number for the LRAT to use to connect to the target.

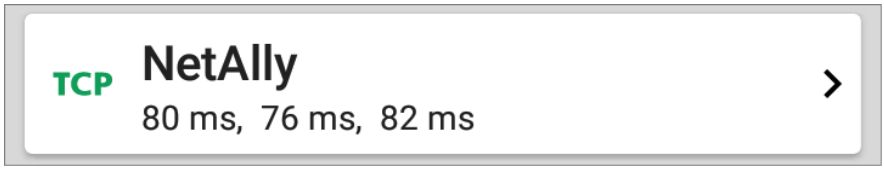
Timeout Threshold

This threshold controls how long the LRAT waits for a response from the target before failing the test.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

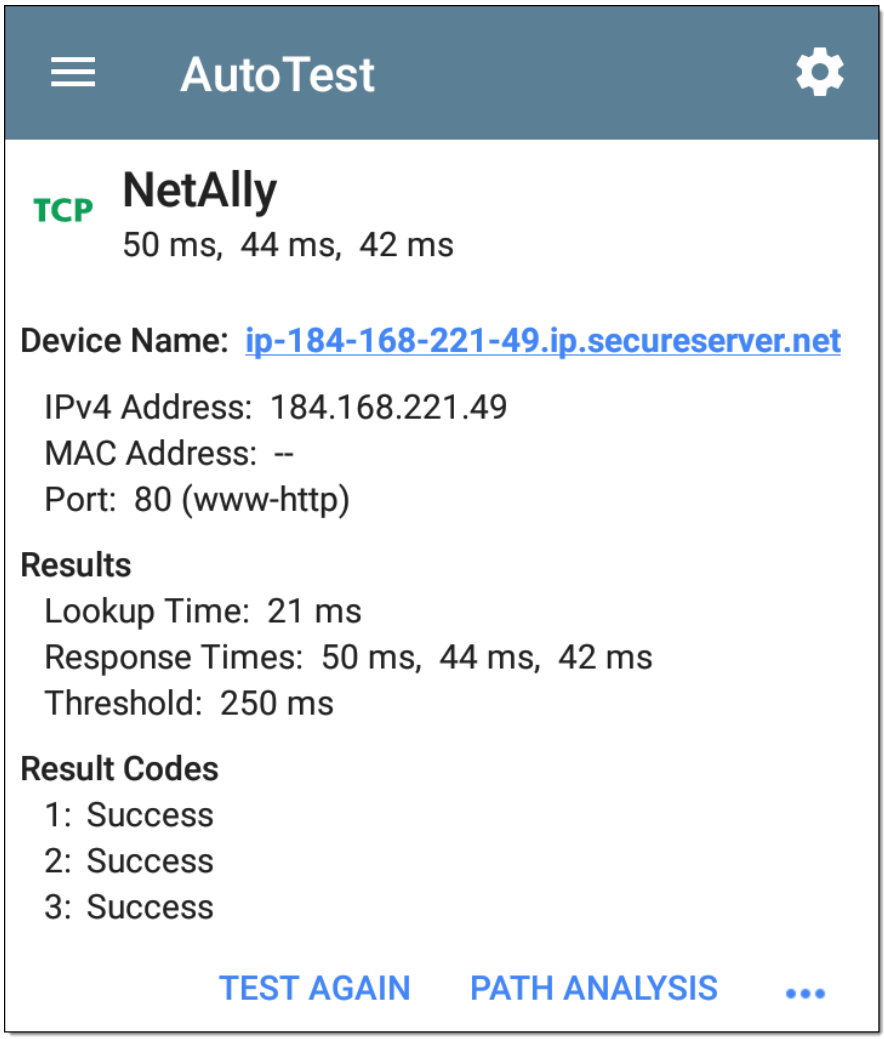
TCP Connect Test Results



The TCP card shows the test name entered in the settings and the three response times from the target.

Tap the card to open the TCP results screen.

AutoTest TCP Results Screen



Device Name: DNS name of the device tested

IPv4 or IPv6 Address: IP address of the target device

MAC Address: Device's MAC address. Two dashes -- indicate that no MAC address was provided.

Port: Port number tested

Results

Lookup Time: How long it took to resolve the URL into an IP address

Response Times: How long it took for the LRAT to receive a response from the server for each of the three connect tests

Threshold: The Timeout Threshold indicated in the test's settings

Results Codes: Final status of the test (Success or Failure) for each of the three Pings

Other Actions

Use the **blue links** or the blue action overflow icon ••• button at the bottom of the test results screens to perform other actions.

- Tap **TEST AGAIN** to run the Ping test again.
- Tap **PATH ANALYSIS** to open the Path Analysis app with the TCP test's information.
- Tap the blue action overflow icon ••• to open another testing app (Ping, TCP Connect, or Capture), to **Browse** to the target address in your web browser, or to start a Telnet or SSH session.

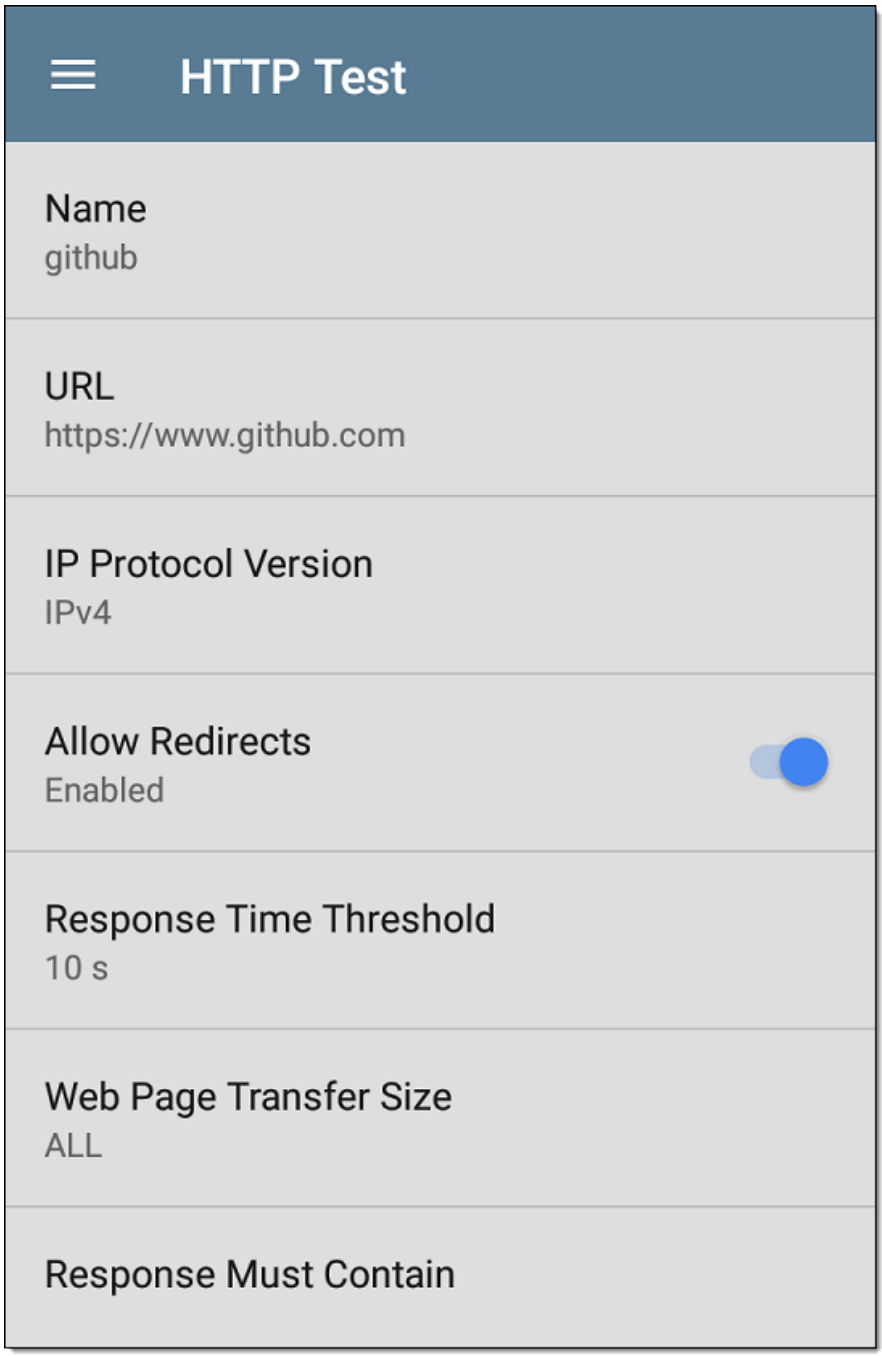
HTTP Test

NOTE: HTTP tests are available on the LinkRunner AT 4000 only.

The HTTP test performs a comprehensive end user response time (EURT) measurement when downloading the specified web page. The target can be an IPv4 address, IPv6 address, or URL.

HTTP Test Settings

HTTP settings allow test grading based on responses, return codes, and time threshold.



Name

Tap this field to assign a custom name to the test. The name appears on the target test card in the profile.

URL

Enter a target address. To reach web servers that operate on a non-default port, enter a colon (:) and specify the port number after the URL.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Allow Redirects

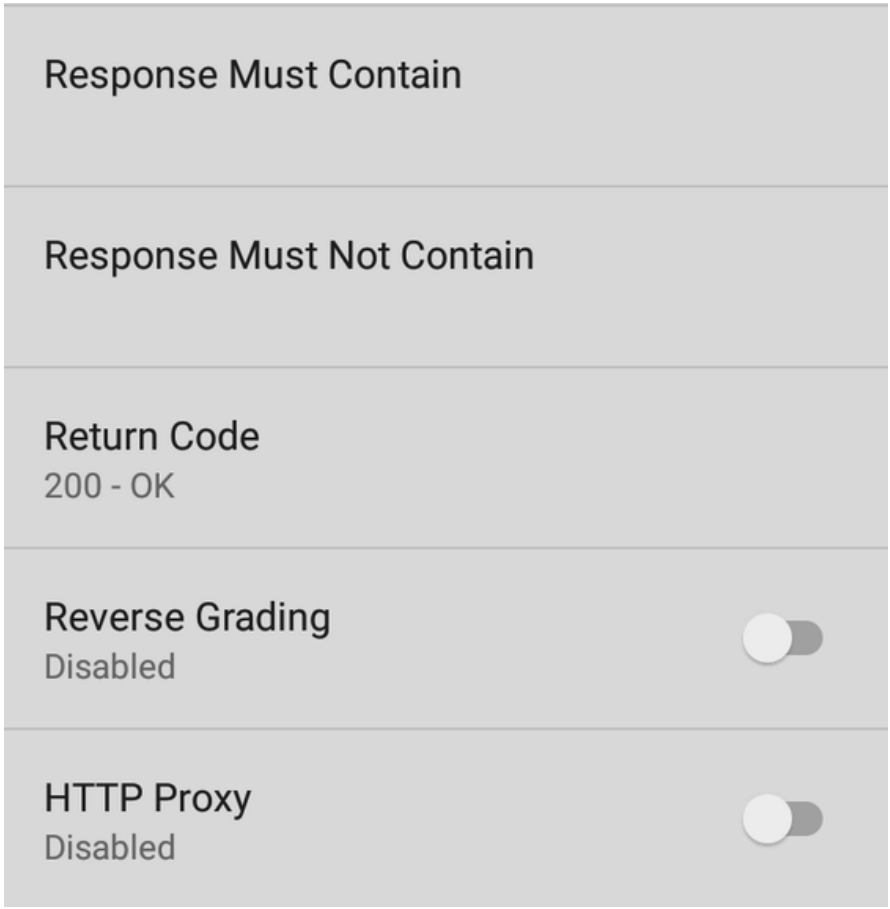
Tap the toggle button to permit web redirects when trying to connect to the target.

Response Time Threshold

This threshold controls how long the LRAT waits for a response from the URL before failing the test. Tap the field to change the value.

Web Page Transfer Size

This setting allows you to limit the amount of data downloaded, ranging from the HTML **Header Only** to the entire page (**ALL**). Tap the field to select a different transfer size.



Response Must Contain

Text entered here functions as **pass**/**fail** test criteria based on the presence of the text string on a specified server or URL. To construct a text string, enter a word or several words with exact spacing. When specifying several words, they must appear consecutively at the source. The test passes if the text string is found. If the string is not found, the test fails with the Return Code: "Response does not contain required text."

Response Must Not Contain

Like the setting above, except text entered here functions as **pass**/**fail** test criteria based on the *absence* of the text string on a specified server or URL. The test passes if the text string is not found. If the string is found, the test fails with the return code: "Response contains excluded text."

Return Code

The Return Code set here functions as **pass**/**fail** test criteria. The default is "OK (HTTP 200)." Tap the field to select a different Return Code from the list. If your selected Return Code value matches the actual return code value, the test passes, and if LRAT receives a different return code, the test fails.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

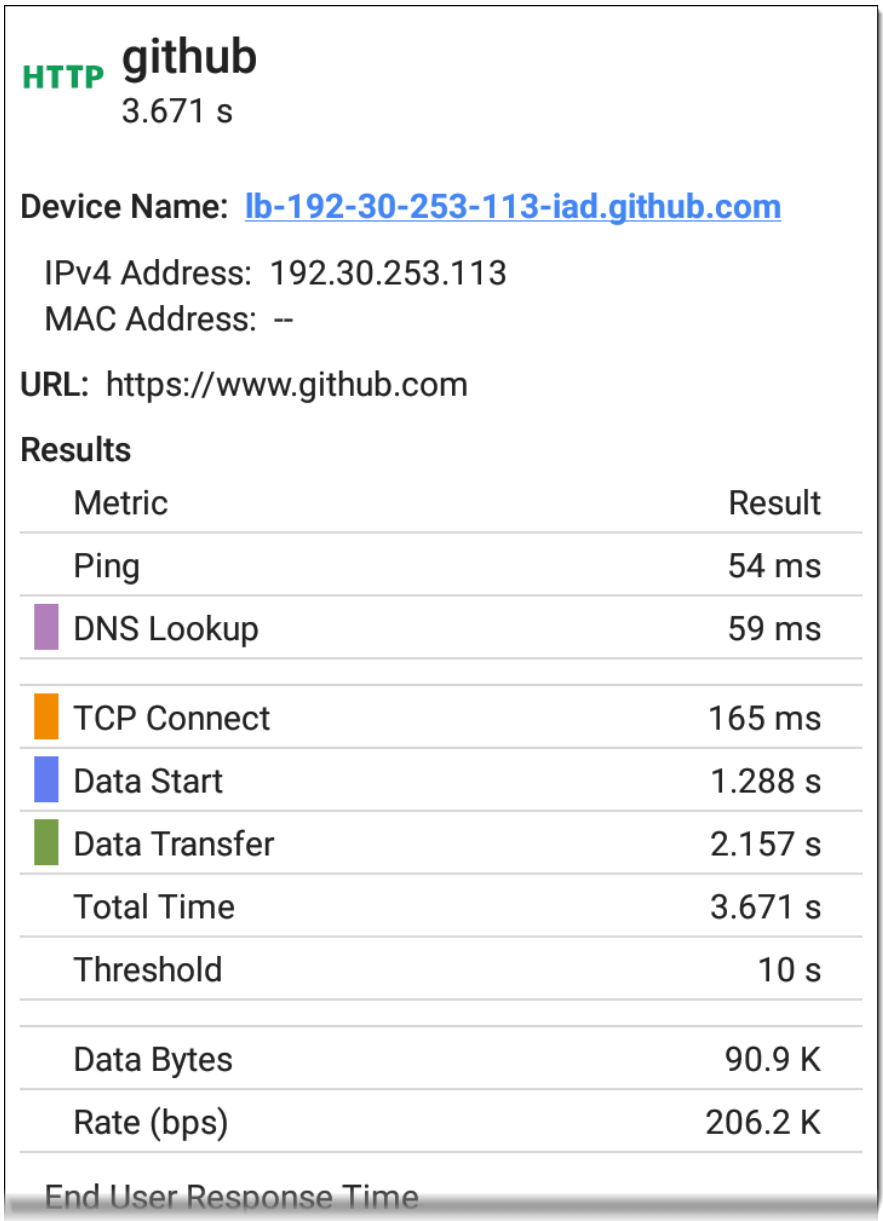
HTTP Proxy

The Proxy control in target test settings uses the server address and port specified in the main profile settings. Tap the toggle to use those Proxy settings. See Wired Profile Settings.

HTTP Test Results

The HTTP card shows the test name entered in the test settings and response time from the target.

HTTP Test Results Screen



Device Name: DNS name of the server tested

IPv4 or IPv6 Address: IP address of the server

MAC Address: Server's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

URL: The target URL

Results

Ping: A ping test runs simultaneously with the HTTP test, and this result field displays the Ping response time. If the HTTP test finishes before the ICMP echo reply packet arrives, dashes -- are displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

DNS Lookup: Amount of time it took to resolve the URL to an IP address. If you enter an IP address, DNS lookup is not required, so dashes are displayed to indicate that this part of the test was not executed.

TCP Connect: Amount of time it took to open the port on the server

Data Start: Time to receive the first frame of HTML from the web server

Data Transfer: Time to receive the data from the target server

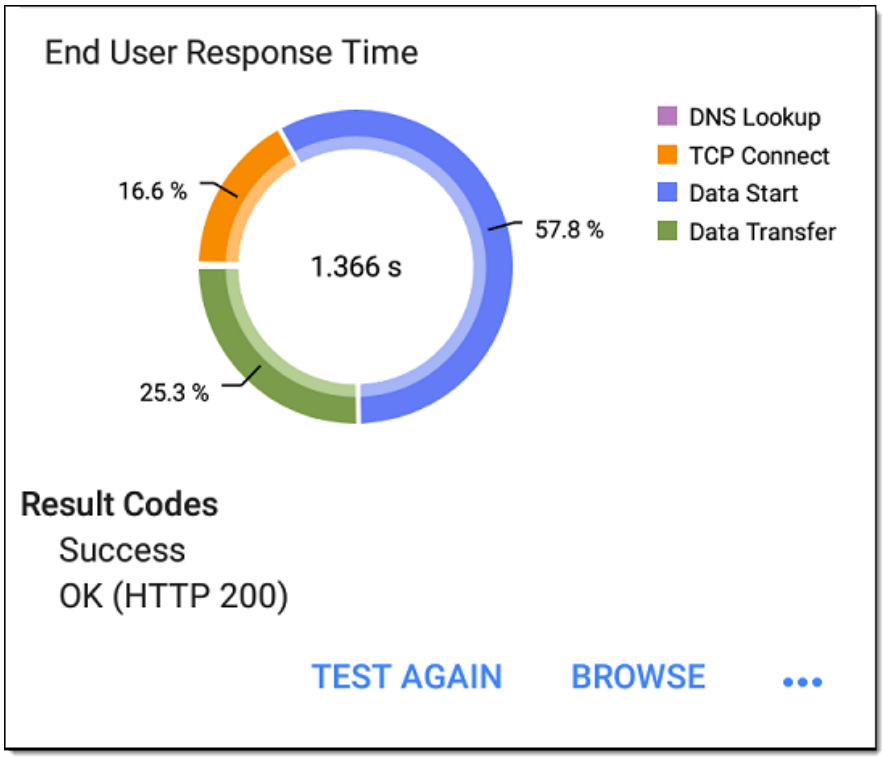
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

If the Response Time Threshold is exceeded during a step in the test, the current phase of the test (DNS Lookup, TCP Connect, Data Start, or Data Transfer) is denoted with a red dot, and the rest of the test is aborted.

Threshold: The Response Time Threshold from the test settings

Data Bytes: Total number of data bytes transferred. This does not include header bytes

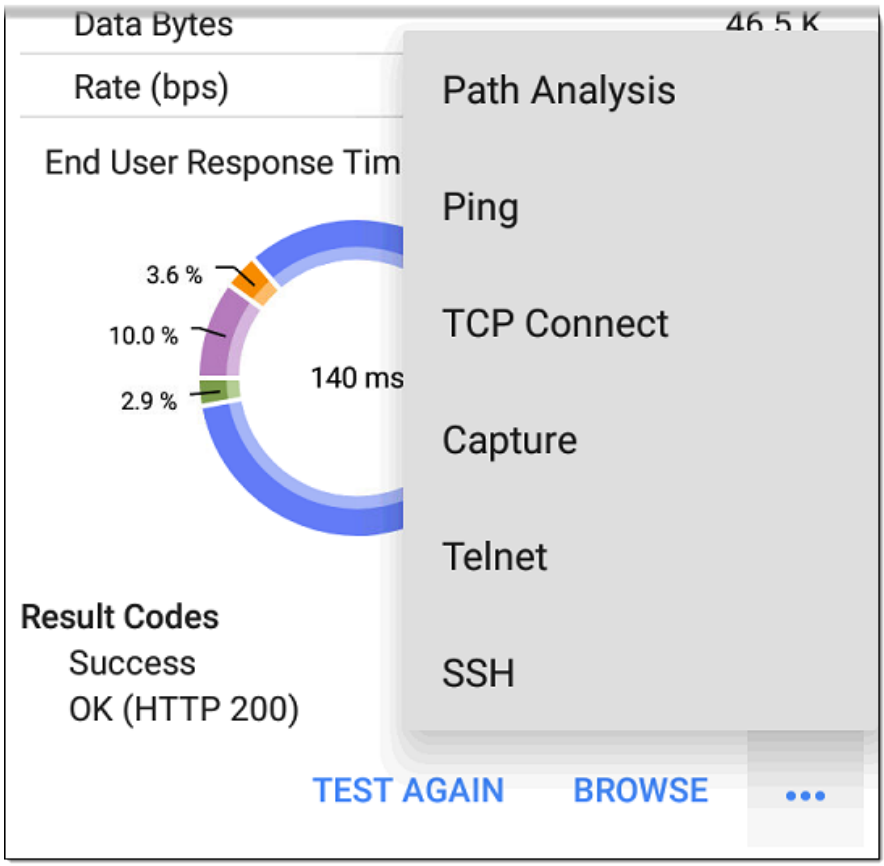
Rate (bps): The measured data transfer rate



End User Response Time : Pie chart of the times for each phase of the test (DNS Lookup, TCP Connect, Data Start, and Data Transfer)

Results Codes: Final status of the test (Success or Failure)

The HTTP test also shows the **Return Code** from the website server.



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the HTTP **TEST AGAIN**, open another testing app, or **Browse** to the target address in your web browser.

Back to Title and Contents

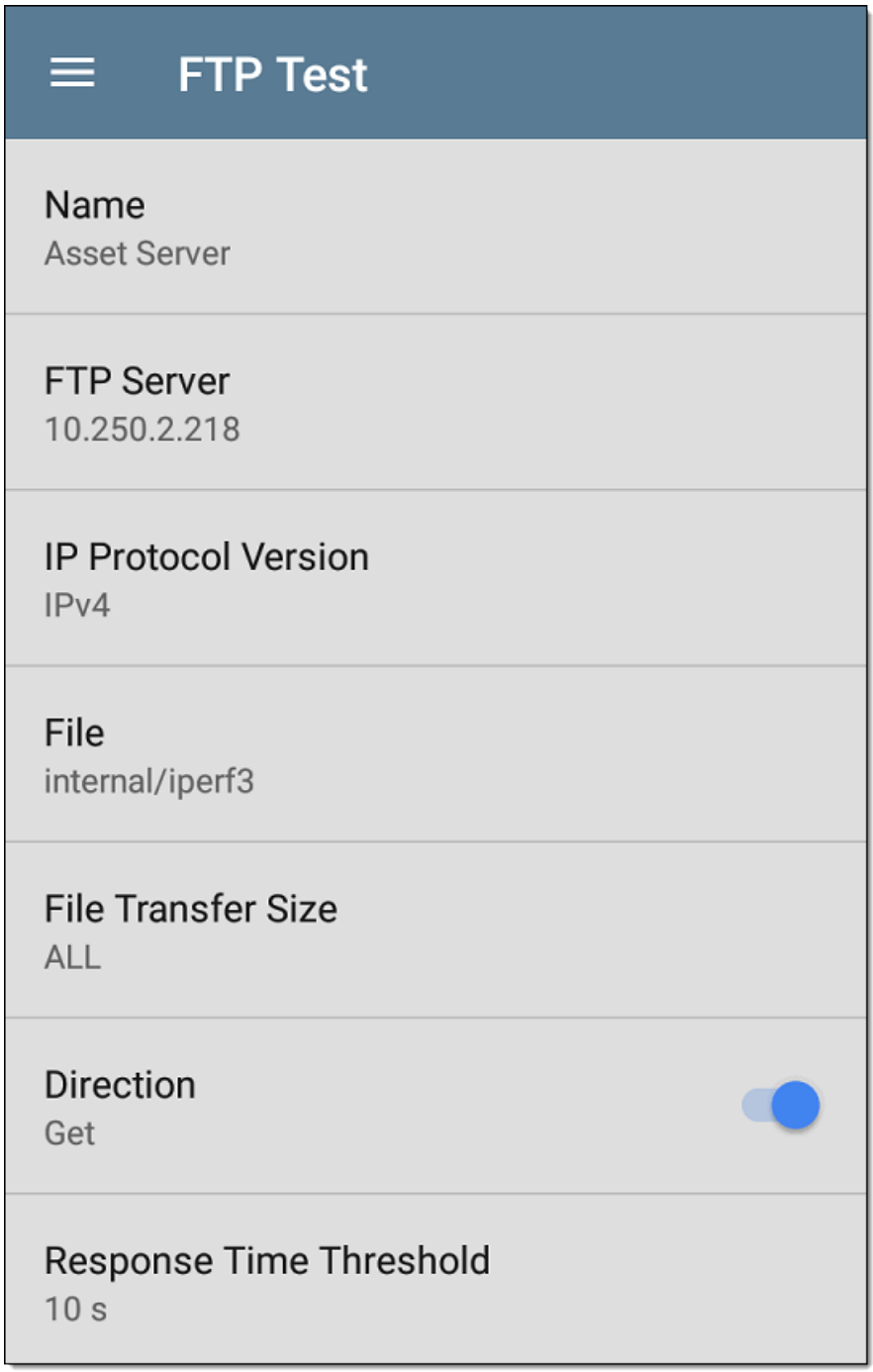
FTP Test

> NOTE: FTP tests are available on the LinkRunner AT 4000 only.

The FTP test performs a file upload to or download from an FTP server, allowing verification of server and network performance. The target can be an IPv4 address, IPv6 address, or URL. The results provide a complete breakdown of the overall file transfer time into its component parts.

FTP Test Settings

FTP settings allow you to specify a **Get** or **Put** test and the file path and name.



Name

This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

FTP Server

Enter the IPv4 address or URL of the FTP server you want to test. If you enter an IP address, the DNS Lookup portion of the test is skipped.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

File

This setting specifies the path and name of the file that is downloaded from (**Get**) or uploaded to (**Put**) the server, based on the **Direction** setting below. Tap the field to enter the file path and name.

File Transfer Size

This setting lets you limit the amount of data to be downloaded or uploaded. The default transfer size is **ALL**.

- When the **Direction** setting is **Get**, a transfer size of ALL causes the download to continue until the entire file is downloaded or the Response Time Threshold is exceeded.

Specifying a transfer size that is greater than file being retrieved does not cause the test to fail. The test stops when the file has finished downloading.

- When the **Direction** setting is **Put**, the default transfer size of ALL causes the LRAT to create and upload a file that is 10 MB.

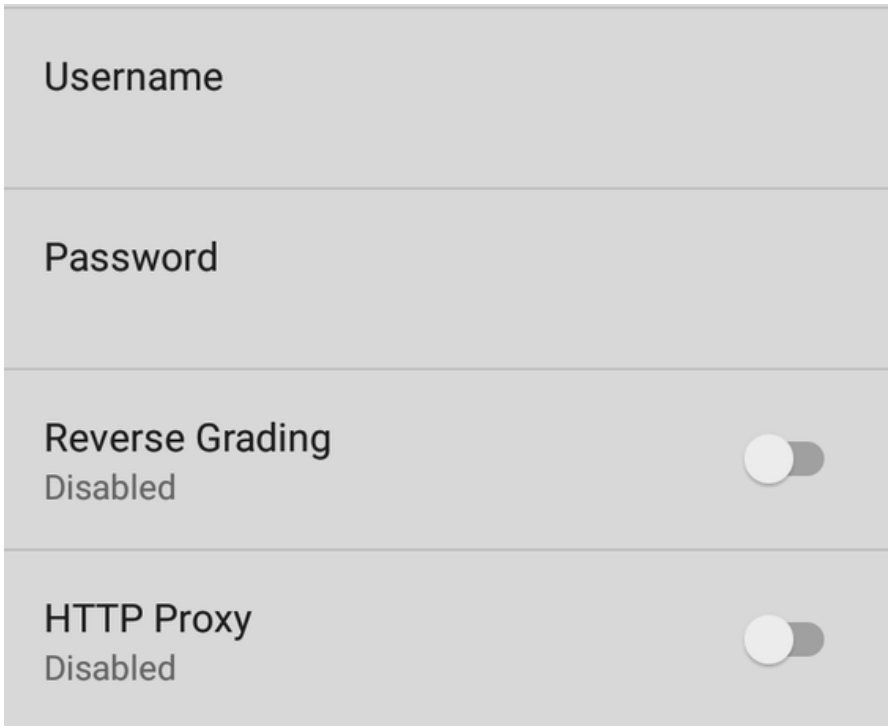
Direction

Tap the toggle button to switch between a **Get** (download the **File** from the server) or **Put** (upload the **File** to the server) test.

- If Direction is set to Get, the file is retrieved, and the size and data rate are calculated. This data is discarded as soon as it is downloaded and is not retained on the LRAT.
- If Direction is set to Put, the File named above is created on the FTP server. The size of this file is determined by the **File Transfer Size** setting. The file contains a text string indicating that it was sent from the LRAT, and the test string is repeated to produce the set file size.

Response Time Threshold

This threshold controls how long the LRAT waits for a response from the FTP server before failing the test. Tap the field to change the value.



Username and Password

Enter these credentials to access the target server you specified. Enter "anonymous" as the username to establish an anonymous connection. The test fails if the configured username or password are not valid on the target FTP server.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

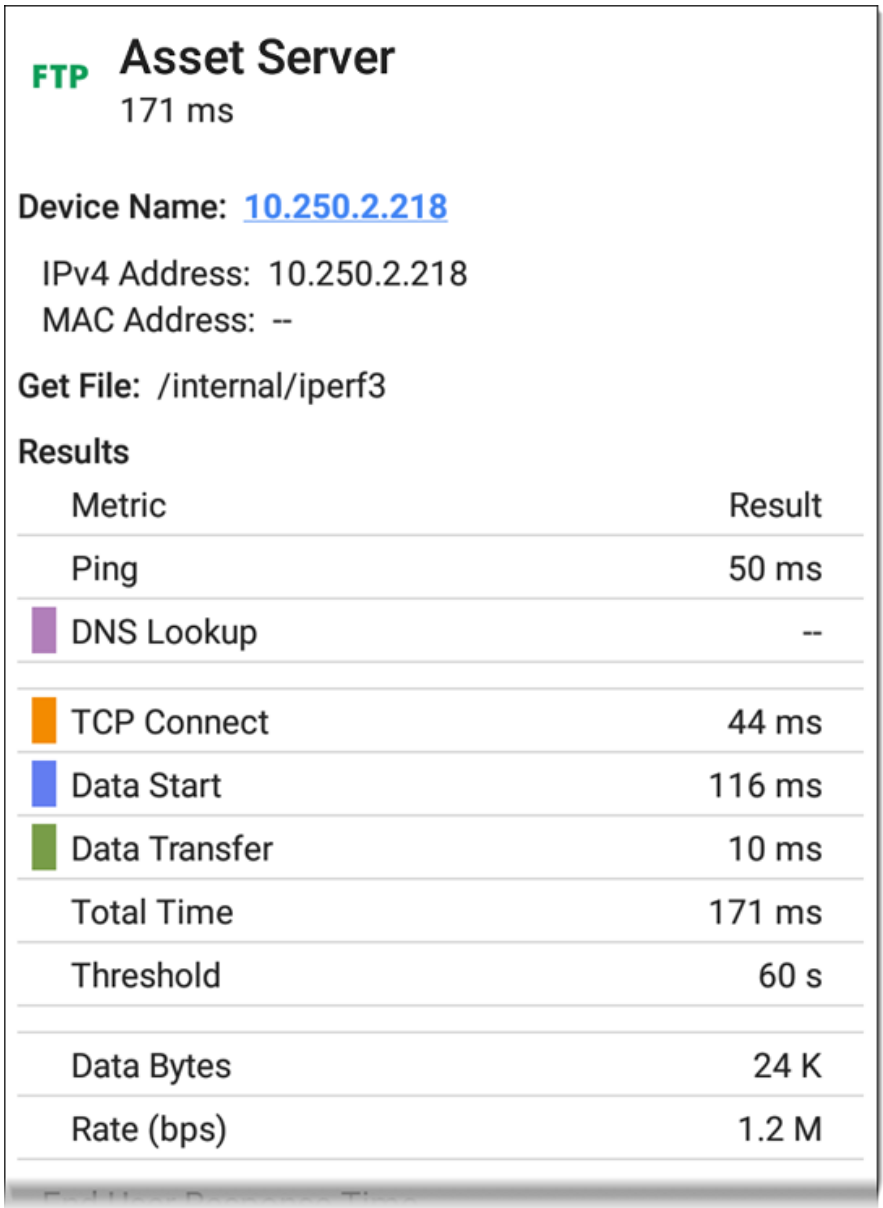
HTTP Proxy

The Proxy control in target test settings uses the server address and port specified in the main profile settings. See Wired Profile Settings.

FTP Test Results

The FTP card shows the test name entered in the test settings and response time from the target.

FTP Test Results Screen



Device Name: Hostname of the server tested

IPv4 or IPv6 Address: IP address of the server

MAC Address: Server's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

Get File: File path and name entered in the settings that was transferred to or from the FTP server.

Results

Ping: A ping test runs simultaneously with the FTP test, and this result field displays the Ping response time. If the FTP test finishes before the ICMP echo reply packet arrives, dashes -- are displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

DNS Lookup: Amount of time it took to resolve the URL to an IP address. If you enter an IP address, DNS lookup is not required, so dashes are displayed to indicate that this part of the test was not executed.

TCP Connect: Amount of time it took to open the port on the server.

Data Start: Time to receive the first frame from the FTP server.

Data Transfer: Time to receive the file from the target server.

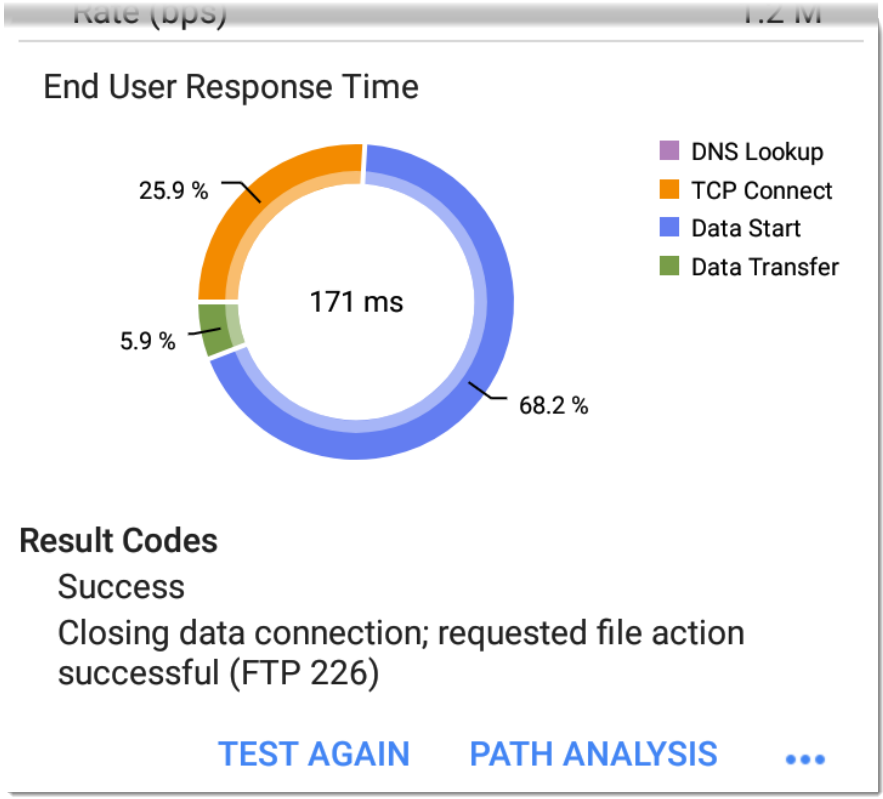
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

If the Response Time Threshold is exceeded during a step in the test, the current phase of the test (DNS Lookup, TCP Connect, Data Start, or Data Transfer) is denoted with a red dot, and the rest of the test is aborted.

Threshold: The Response Time Threshold from the test settings.

Data Bytes: Total number of data bytes transferred. This does not include header bytes.

Rate (bps): The measured data transfer rate.



End User Response Time: Pie chart of the times for each phase of the test (DNS Lookup, TCP Connect, Data Start, and Data Transfer).

Results Codes: Final status of the test (Success or Failure).

The FTP test also shows the **Return Code** from the server.

Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the FTP **Test Again**, open another testing app, or **Browse** to the FTP server in your web browser.

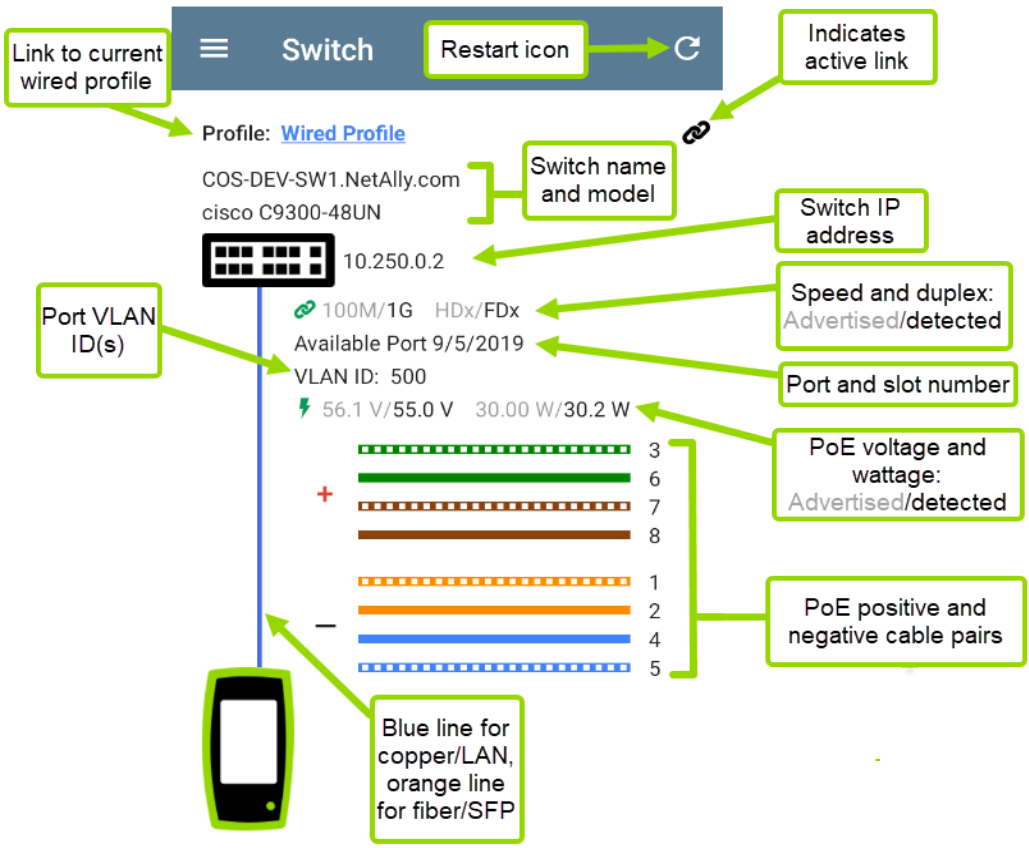
Back to Title and Contents

Switch App

The Switch application displays a summary of AutoTest's Wired Profile results from the Link, PoE, and Nearest Switch result screens. This gives you a fast way to display information about how your LinkRunner AT 3000/4000 is connected.

Running Switch

Before running switch, use AutoTest to start a wired profile so that Switch has information when you need it. To run Switch, simply tap the Switch app icon. This opens the main Switch screen.



The main Switch screen has only a few controls and no settings.

- Tap the Restart icon to update the switch information. The app displays results from the nearest switch for the wired AutoTest profile that was last run or is currently running.
  - A black Link icon in the upper right corner of the screen appears when the tester is actively linked.
  - A "no cable" icon displays if no connection is available:

NOTE: Displayed results are retained even after the cable is disconnected. Just tap Restart to capture and displays the newest information from the switch.

- To open the AutoTest profile, tap the Profile link:

  For detailed information, tap the AutoTest cards that display the Link icon , the PoE icon , or the Switch icon .

Back to Title and Contents

Cable Test App

LRAT 3000-4000's Cable Test can help you determine cable length and fault status, verify wiremapping of patch and structured cabling, and locate cable connections using toning. The cable testing port is the RJ-45 port on the left side of the LRAT unit. Connect a cable to this port for testing and tracing with the tone function.

Cable Test Settings

The Cable Test app has limited settings. Tap the navigation menu icon or swipe from the left-side drawer to open the Cable Test Settings.

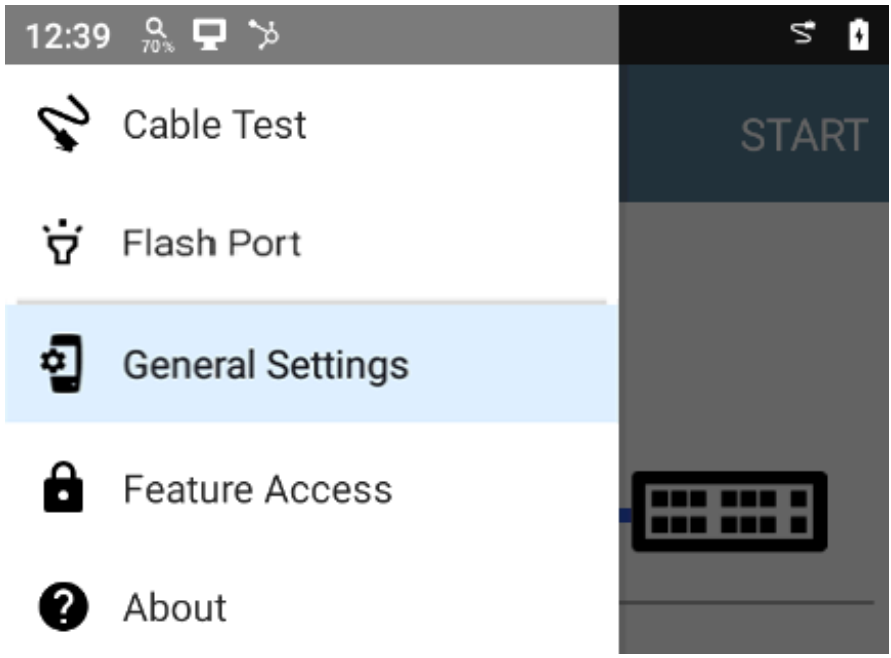
Flash Port

Tap this setting choice to activate the Flash Port function, which flashes port LEDs to help you locate cables and ports. See Running Cable Test for instructions on using this function.

Distance Unit

The **Distance Unit** setting is contained in the General Settings menu. The setting designates Feet or Meters.

1. To access General Settings, tap the menu icon on the Cable Test app screen, and select **General Settings**.



2. Scroll to the bottom of the Settings list under the **Preferences** heading.
3. Tap the **Distance Unit** field, and select either **Feet** or **Meters** as needed, and then tap **OK**.
4. Tap the Back button at the bottom of the screen to return to the Cable Test screen.

Running Cable Test

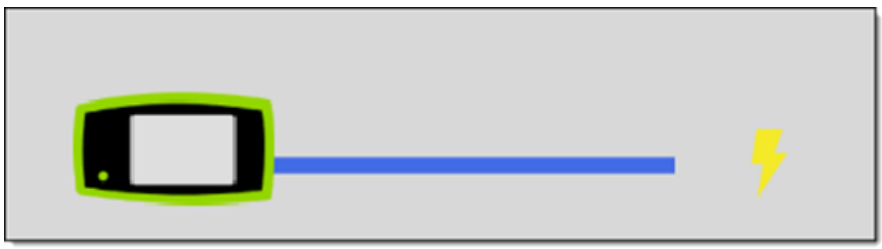
The Cable Test app has general tests for cables as well as a toning function and a flash port function to help you trace cables and ports. You can also upload your results to Link-Live.

General Cable Tests

Refer to LRAT 3000-4000's Buttons and Ports as needed.

- With an open or unterminated cable connected to the RJ-45 cable test port (top of the unit), you can measure length, identify shorts and splits, and locate opens.
- Using a cable terminated with a WireView Cable ID accessory, you can measure cable length and identify shorts, opens, split pairs, crossover cables, normal or negative pair polarity, and shielded cables.
- LRAT 3000-4000 cannot perform a cable test on a cable that is connected to a switch; however, you can still use the toning function to trace the cable to the connected port.

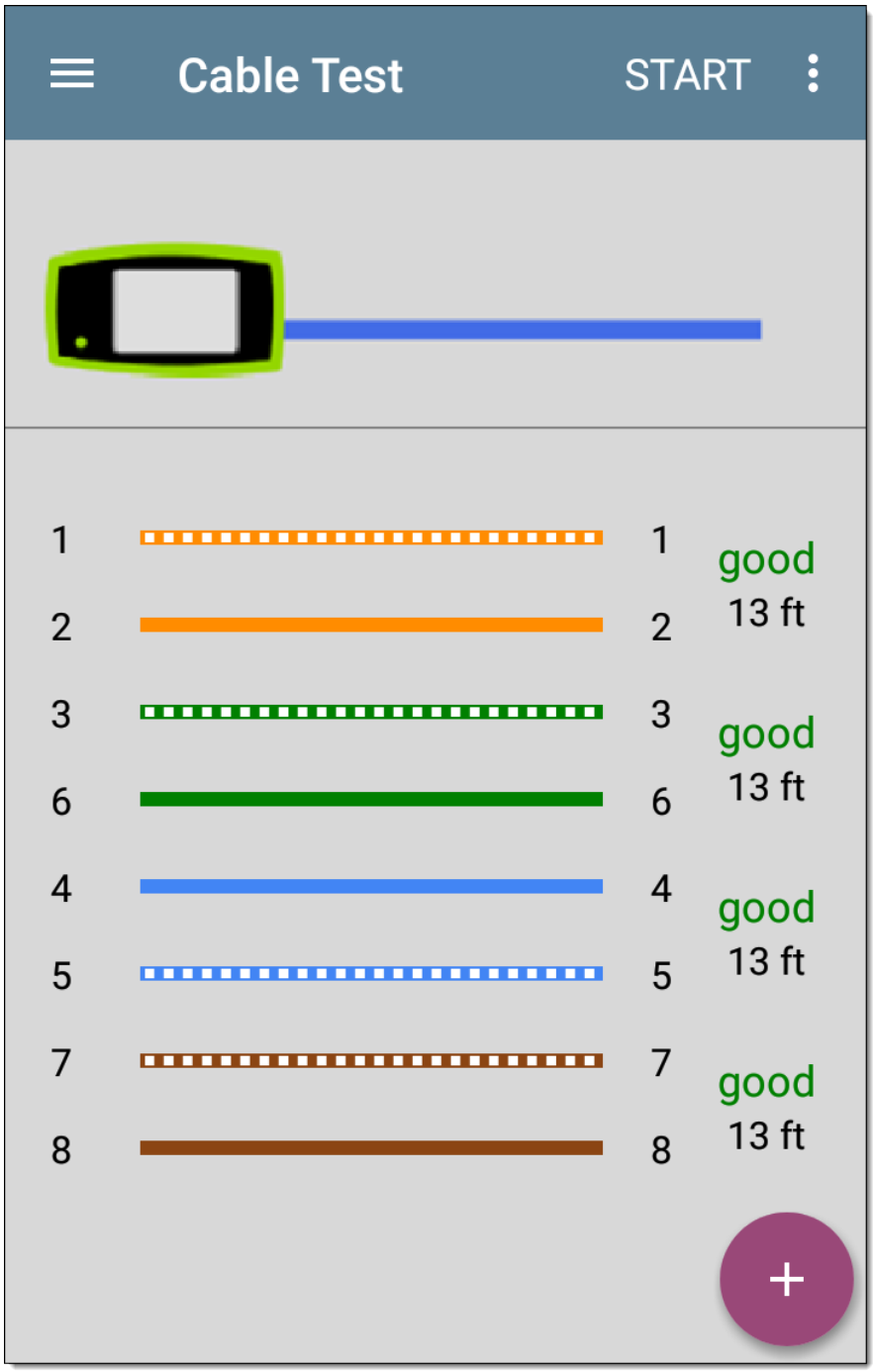
- Additionally, you cannot run a cable test or use the toning feature if the unit detects voltage on the connected cable. The lightning bolt icon on the Cable Test screen indicates detected voltage.



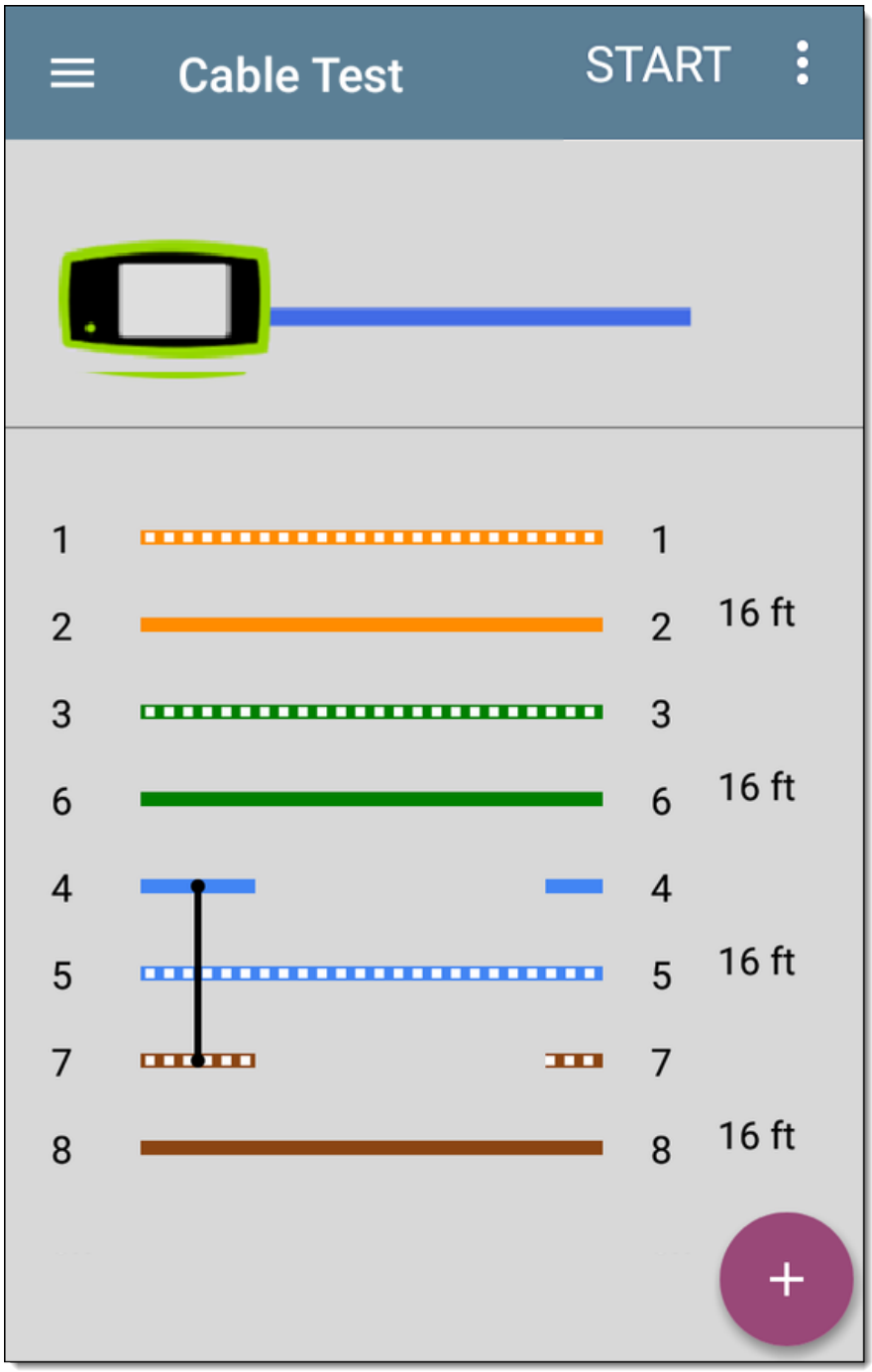
To start the cable test, tap **START** at the top right of the Cable Test app screen.

Open Cable TDR Testing

LRAT 3000-4000 can measure the length of a cable and detect some faults by measuring the electrical reflections of the cable using Time Domain Reflectometry (TDR). Connect an open cable (unterminated) into the RJ-45 port on the top of the LRAT unit to measure its length and view any shorts, opens, or splits.



When a cable has no detected faults, "good" is shown next to each pair above the length measurement. Cable tests that detect a "split" or "open" in the cable also display the corresponding words.



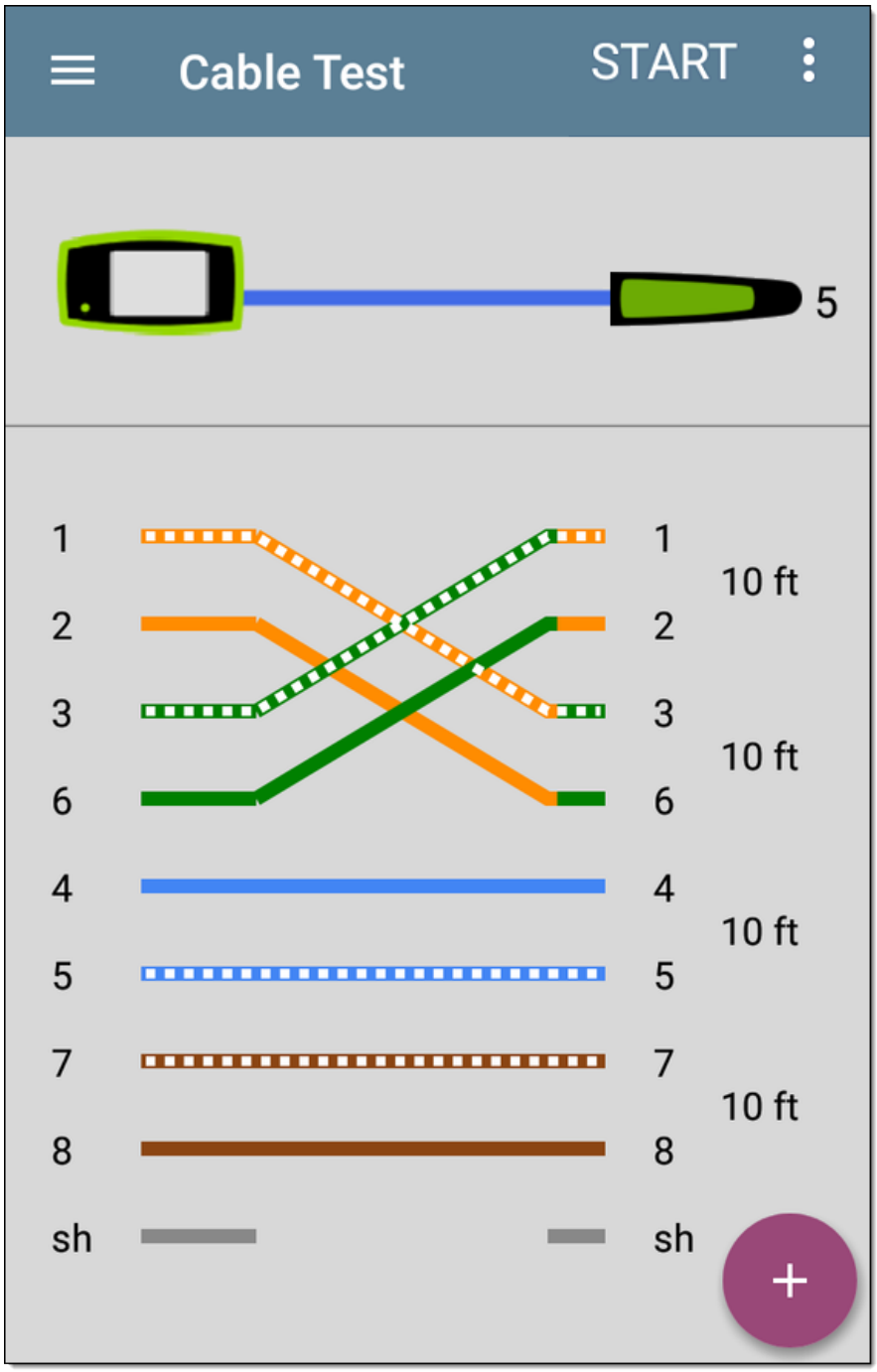
This unterminated cable test image shows a shorted cable between pins 4 and 7.

Terminated WireView Testing

Using a WireView accessory provides more detailed, per-wire results. A WireView #1 is included with your LRAT 3000-4000. Additional WireViews 2-6 are available for purchase.

To run a terminated cable test, connect the top RJ-45 port to a cable terminated with an external WireView Cable ID accessory.

The terminated cable test screen displays the number of the WireView attached, unless a cable fault prevents the LRAT from detecting the WireView.

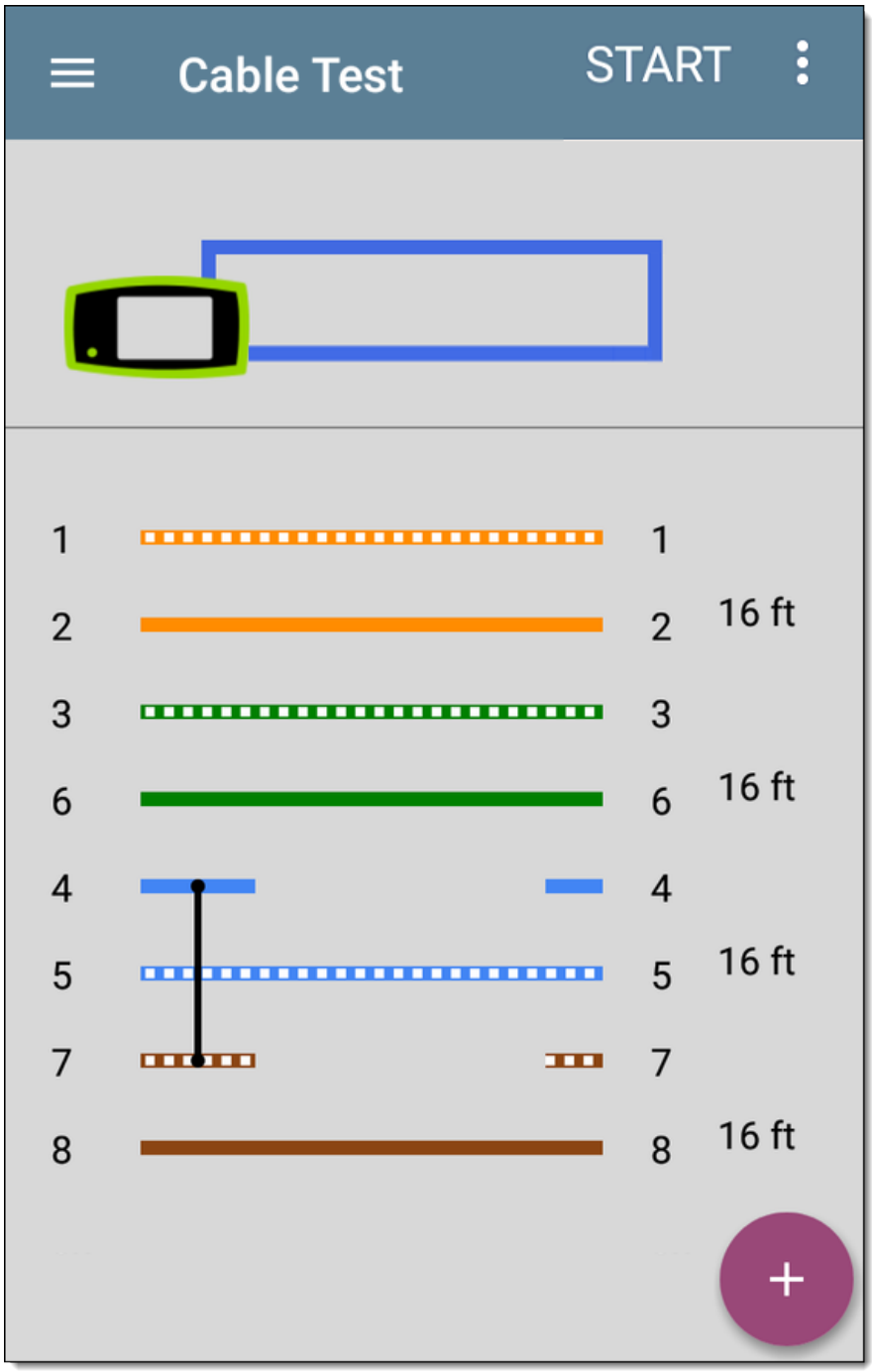


The image above indicates a crossover between pairs 1, 2 and 3, 6 and a WireView accessory number 5.

The last row of WireView results indicates whether the cable is shielded: an unbroken line between **sh** means a shielded cable is detected.

Patch Cable Testing

Connect a cable from the top RJ-45 LAN test port into the side RJ-45 WMAP wire map port to calculate the cable length and wire mapping, including any faults. The following image shows the cable length and a shorted cable between pins 4 and 7.



Toning Function

You can also trace a cable using a Fluke Networks IntelliTone™ Probe*, an analog probe, or the Tone function.

* IntelliTone is a trademark of Fluke Networks.

1. Connect a cable into the top RJ-45 port.
2. Tap the floating action button (FAB)  to display the tone menu:

3. Select a Tone option from the menu. The LRAT 3000-4000 emits the tone through the cable, and the probe detects it, allowing you to trace the wire or locate it in a switch closet or rack.

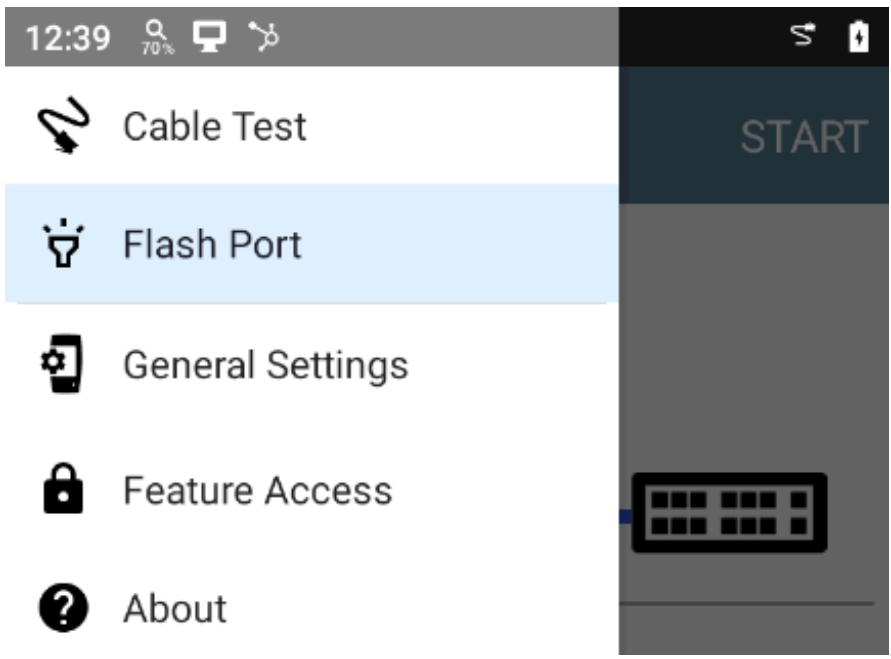
Flash Port Function

Flash Port gives you the ability to make the LEDs blink on your unit's RJ-45 test port and on the switch to which your unit is connected. This

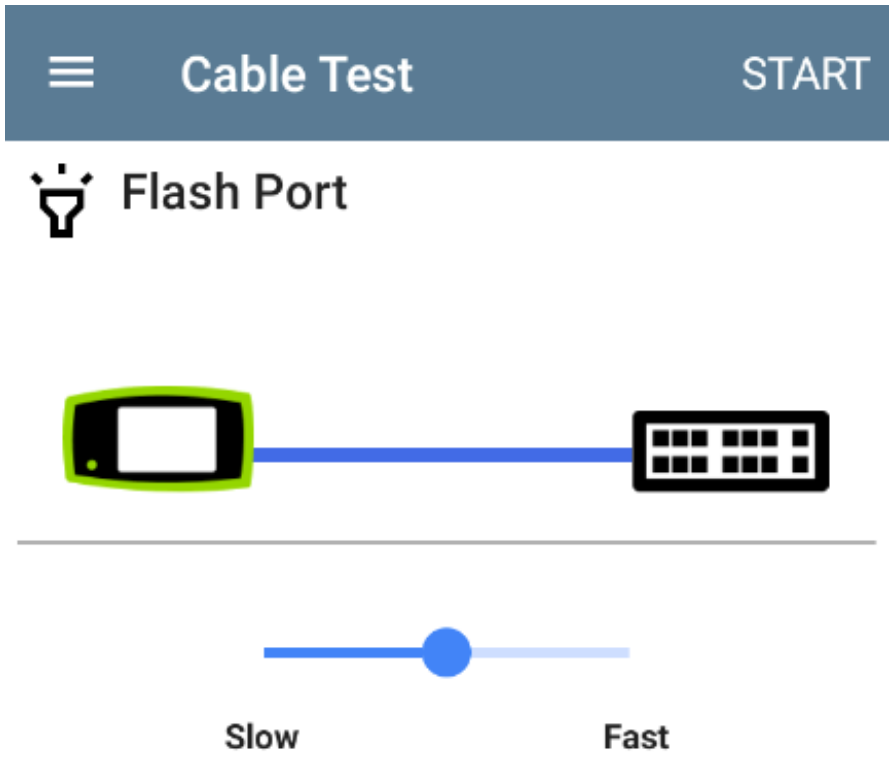
helps make the connected port easier to locate on the switch.

To use the flash port feature:

1. Connect the top RJ-45 port to an active network cable.
2. Tap the navigation menu icon or swipe from the left-side drawer to open the Cable Test Settings.



3. Tap **Flash Port** to open the Flash Port screen. If the connection to the switch is good, a blue line connects a test unit icon to a switch icon.

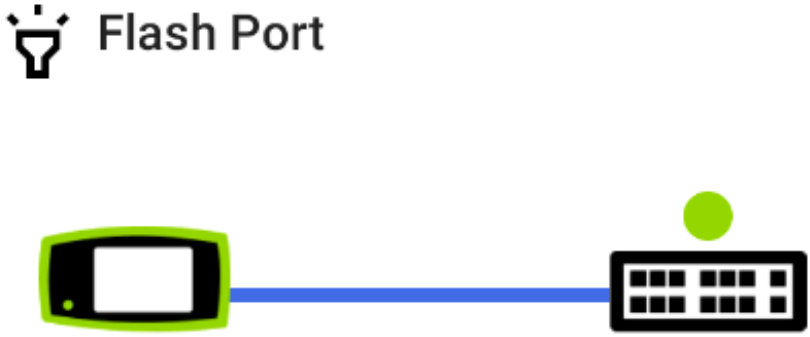


4. Use the slider to set the rate of the flash.

   TIP: Some port LEDs may have trouble flashing at a very fast rate. Setting a rate slower than the maximum may work better.

5. Tap the **Start** button. When the flash function begins, a green circle appears over the switch icon and flashes at the rate you set with the slider. The green circle, the LEDs on the top RJ-45 port of your test unit, and the LEDs for the connected port on the

switch all blink in unison.



6. When you finish using the Flash Port function, tap the **Stop** button.

Uploading Results to Link-Live

Tap the action overflow icon ⋮ at the top right of the Cable Test screen, and select **Upload to Link-Live** to send the current Cable Test result to the Results page ☰ on Link-Live.com.

See the Link-Live for more information.

Ping/TCP Test App

The Ping/TCP test app runs a Ping or TCP Connect test to your chosen target, allowing you to monitor connectivity changes.

A Ping test sends an ICMP echo request to the selected target to determine whether the server or client can be reached and how long it takes to respond. A TCP Connect test opens a TCP connection with the selected target to test for port availability using a 3-way handshake (SYN, SYN/ACK, ACK).

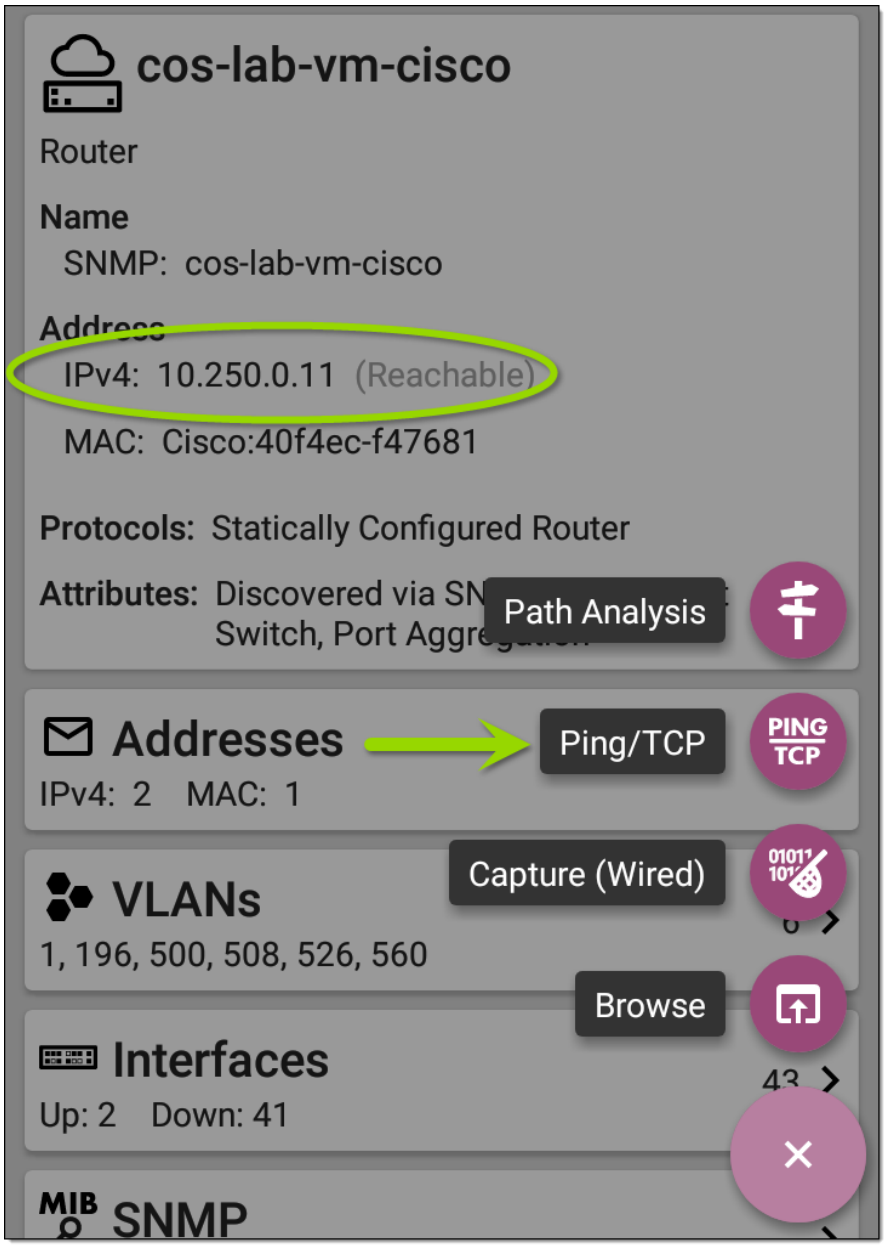
You can open the TCP/Ping app from the Home screen, or you can select **Ping** or **TCP Connect** from another app, such as AutoTest or Discovery, while viewing a device's details.

Ping/TCP Settings

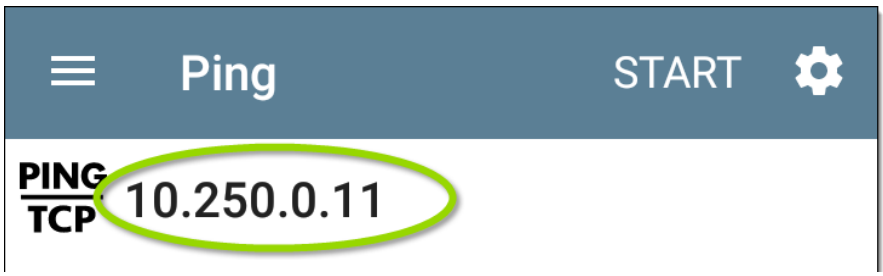
To configure a test, you can manually enter a hostname or IP address in the settings, or you can select Ping or TCP Connect from another testing app's device screen.

Populating Ping/TCP from Another App

When you open the Ping/TCP app from another app, the address is pre-populated as the Ping or TCP target device. For example, the floating action button (FAB) menu on the Discovery app screen shown below contains the option to open the Ping/TCP app.

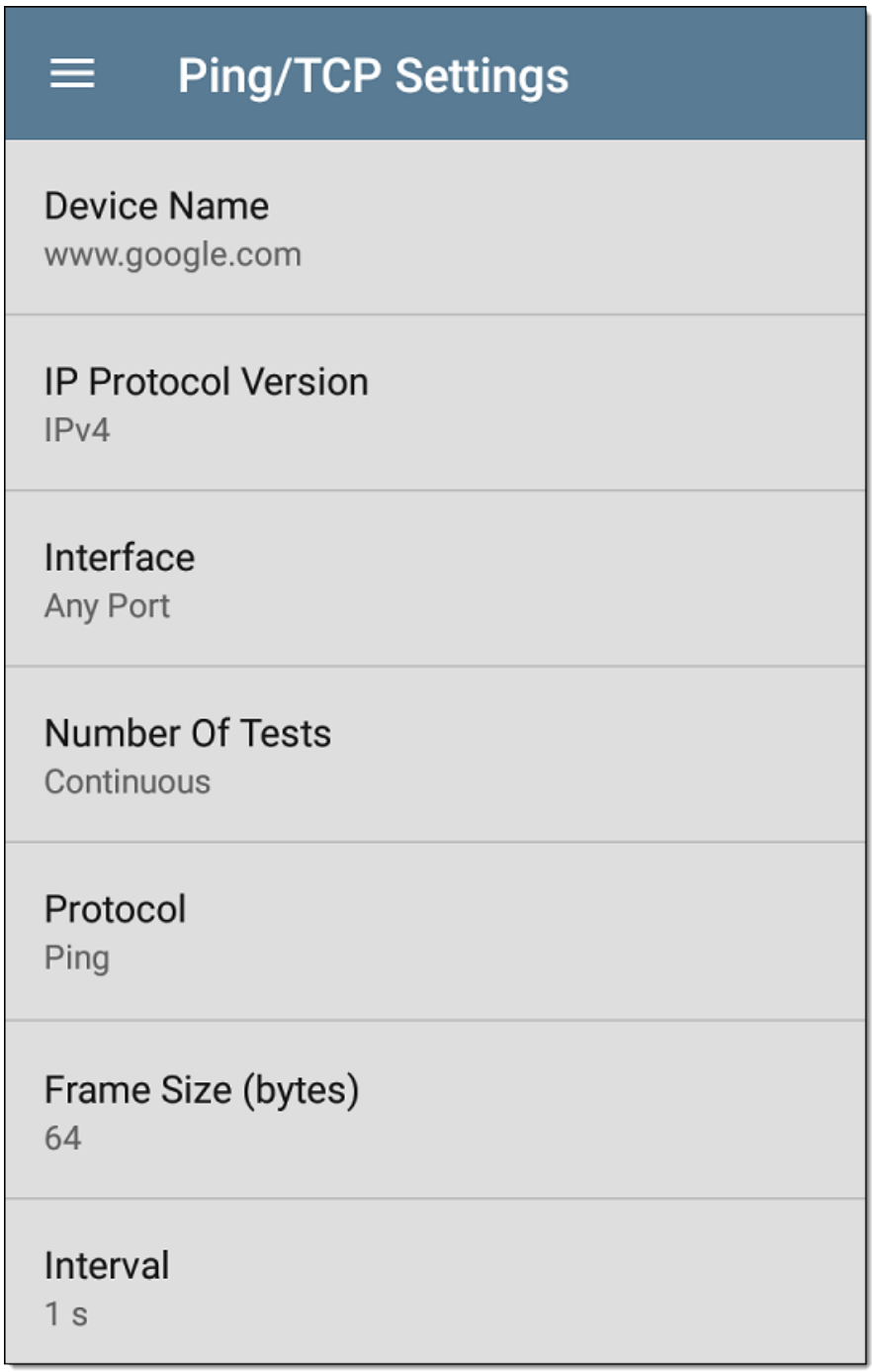


If you open the Ping/TCP app from this screen, the IPv4 address from the Discovery app is already configured as the Ping/TCP target.



Configuring Ping/TCP Settings Manually

To configure the target and settings manually, open the app's settings .



Device Name: Enter the IP address or DNS name of the target.

IP Protocol Version: IPv4 is used by default. Tap the field to enable IPv6 instead.

Interface: This setting determines the LRAT port from which the port scan runs. Tap the field to select the port. (See Selecting Ports for explanations of the different ports.)

Number of Tests: Tap to select the number of Ping or TCP connect tests you want to run. The default setting of **Continuous** keeps running tests until you tap the **STOP** button.

Protocol: Tap to select the **Ping** or **TCP Connect** protocol for the test.

Some of the following settings depend on the selected protocol.

Frame Size (bytes): (Appears only if the **Ping** Protocol is selected.) Specifies the total size of the payload and header the LRAT sends. Tap a radio button to select a new size, or enter a Custom Value from 64 to 1518 bytes.

To test the Maximum Transmission Unit (MTU) along a route to a target, select the MTU frame

size you want to test, and set the **Do Not Fragment** setting (below) to **Enabled**.

Interval: (Appears only if the **Ping** Protocol is selected.) Controls how much time passes between each Ping sent from the LRAT. By default, Pings are sent once every second (1 s). Tap a radio button to select a different interval, or enter a Custom Value between 100 and 10,000 milliseconds.

Port: (Appears only if the **TCP Connect** Protocol is selected.) Indicates the port number your LRAT uses to connect to the target address for a TCP Port Open test. If needed, tap the **Port** field to open a pop-up number pad and enter a new port number. Tap **OK** to save it.

Timeout Threshold: This threshold controls how long the LRAT waits for a response from the target before the test is failed.

Do Not Fragment: (Appears only if the **Ping** Protocol is selected.) Tap the toggle button to enable. See the Frame Size setting description above.

Back to Title and Contents

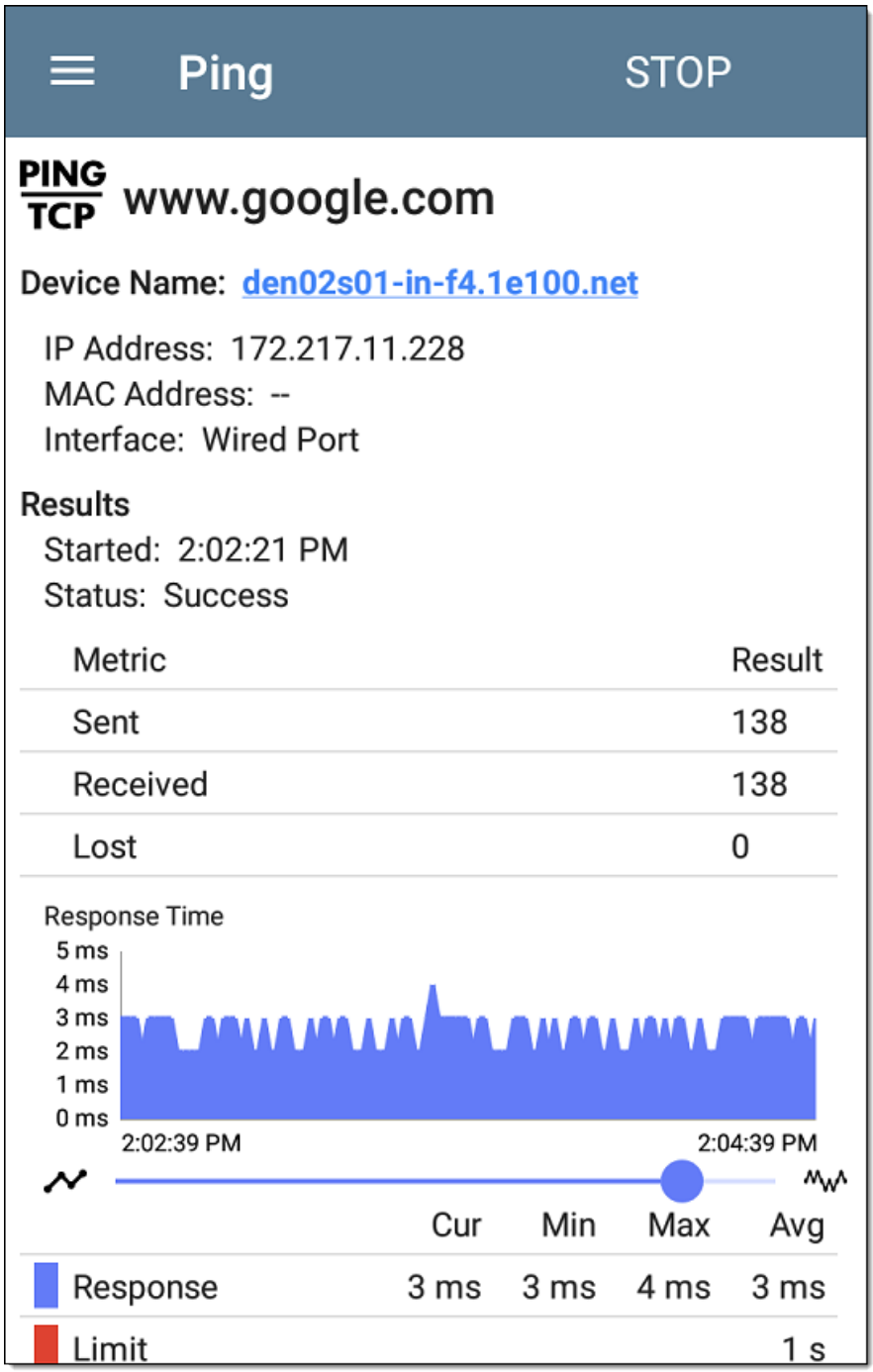
Running Ping/TCP Tests

Your unit must be connected to an active network (Test or Management Port) to run Ping and TCP Connect tests. Icons in the top Status Bar indicate whether and how your LRAT is connected. See Connection Notifications for descriptions of the connection status icons, and select the appropriate **Interface** (or Any Port) from the Ping/TCP settings.

The default target is google.com. Open the app settings  to enter a new target.

To begin the test, tap **START**.

If the Number of Tests setting is set to **Continuous**, the Ping/TCP app runs tests to your selected target until you tap **STOP**.



Device Name: Hostname or address of the target device

IPv4 or IPv6 Address: IP address of the target device

MAC Address: Target device's MAC address. The two dashes -- indicate that no MAC address was provided from the device.

Port: The port number used for the TCP Connect test. This field does not appear in Ping test results.

Interface: The LRAT Test or Management Port from which the test is running

Results

- **Started**: Time the test started
- **Status**: Most recent test status
- **Sent**: Number of Pings or TCP SYN packets sent to the target
- **Received**: Number of Ping or TCP SYN/ACK packets returned from the target
- **Lost**: Number of Pings or TCP packets that were not returned from the target

Response Time graph: Plots the target device's response times in milliseconds. The graph saves and displays data for up to 24 hours in the past if the unit stays linked.

To pan and zoom on the graph, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

Response: Table display of the Current, Minimum, Maximum, and Average response time measurements

Limit: The **Timeout Threshold** from the Ping/TCP app's settings

Back to Title and Contents

Capture App

Packet capture is the process of recording network traffic in the form of packets as data streams back and forth over the the wired connection. Packet captures can help you analyze network problems, debug client/server communications, track applications and content, ensure that users are adhering to administration policies, and verify network security.

The capture process uses the Wired Test port.

You can open the Capture app from the Home screen or using a link from another app, such as AutoTest or Discovery.

> NOTE: This application applies to the LinkRunner AT 4000 only.

Capture Settings

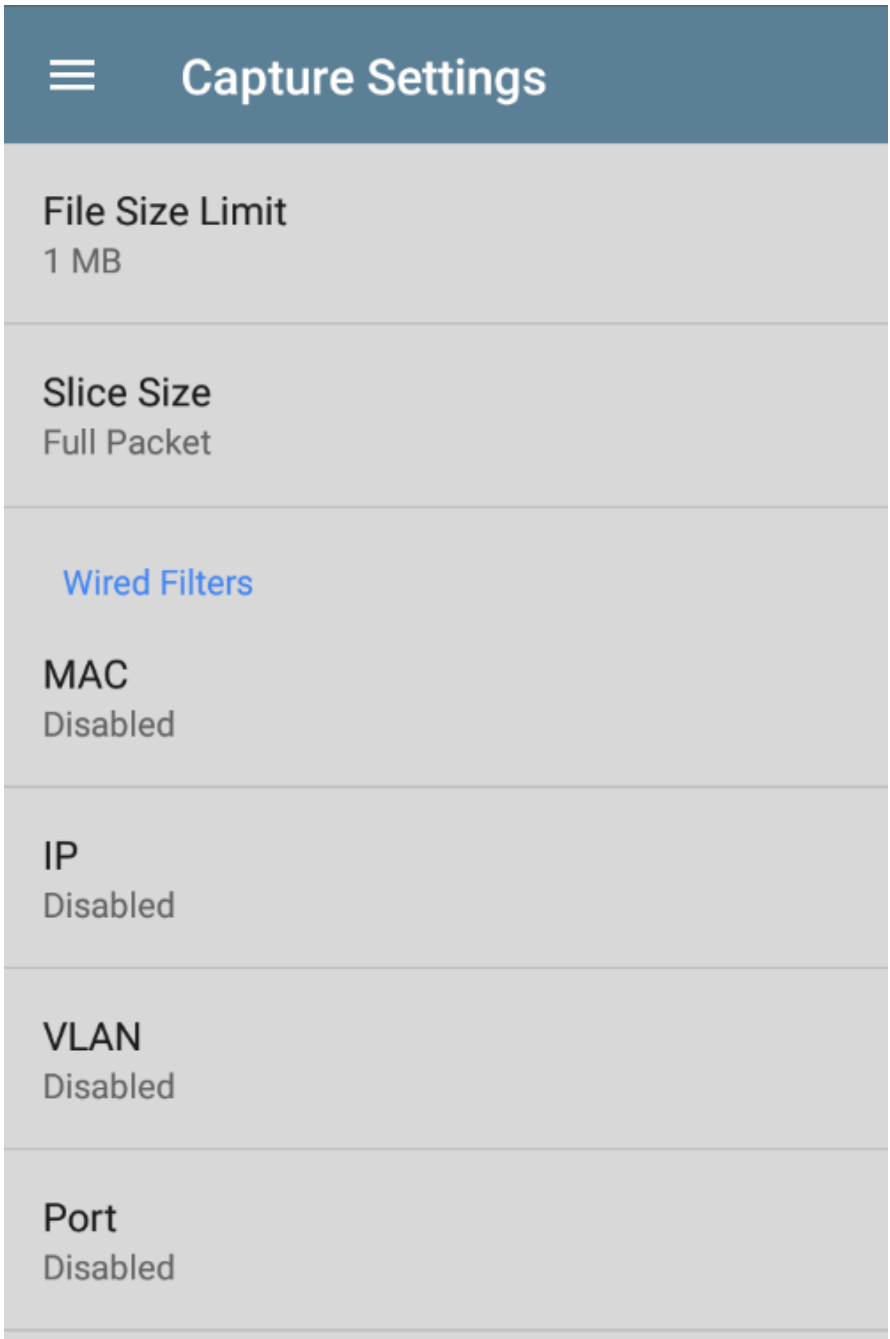
The Capture app settings allow you to designate file and slice sizes, and apply filters to capture and analyze only certain packet types. For example, you can set a filter to capture only packets related to a specific application (based on IP address and port number).

When you open Capture from Home and do not configure any filters, all packets from the switch are captured. The default capture saves all the packets sent from the local switch to the LRAT.

If you open the Capture app from another NetAlly test app, Capture filters are automatically applied. Filters that can be applied from other apps include Wired IP and MAC.

The Capture settings are saved until you clear the filters or open the app with new filters applied.

Tap the settings icon  in the Capture screen to configure capture settings.



File Size Limit: Tap this field to specify a size for the capture file. The default size is 1 MB, and largest size allowed is 1 GB (1,024 MB). The capture stops when the captured file reaches this size. When capture is running, the capture

screen displays the current file size as data is captured.

Slice Size: Tap this field to select a specific frame slice size or enter a custom value. The Slice Size setting limits how much of each packet is captured. A smaller slice size is useful when you are interested in the packet's header but do not need to see all the payload data. The default is 1,518 bytes.

Wired Filters

All filters are disabled by default unless you open Capture from another app. Tap the fields below to enable the filter and enter filter values.

MAC: Enter the MAC address of a host to capture only packets that contain the host's MAC address as the source or destination.

IP: Enter the IPv4 or IPv6 address of a host to capture only traffic to and from the host.

VLAN: Enter a VLAN number to capture only traffic tagged for that VLAN.

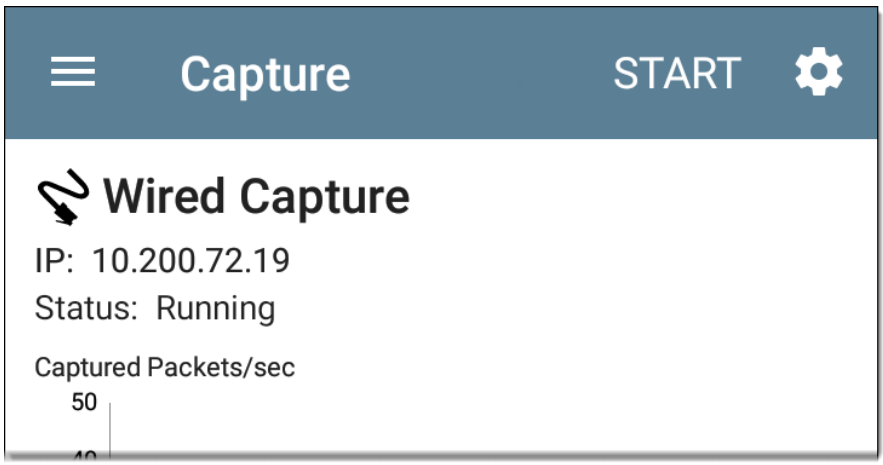
Port: Specify a port number to capture only traffic from that UDP or TCP port. For example, select port 80 to capture HTTP traffic only.

NOT: Sets up a logical NOT to use with capture values you have set up with other filters. For example, if you set up a filter to capture traffic to and from IP 10.250.0.70 on Port 80, and then you enable NOT, the LRAT 3000-4000 captures all traffic *except* traffic to and from 10.250.0.70 on port 80.

Back to Title and Contents

Running and Viewing Captures

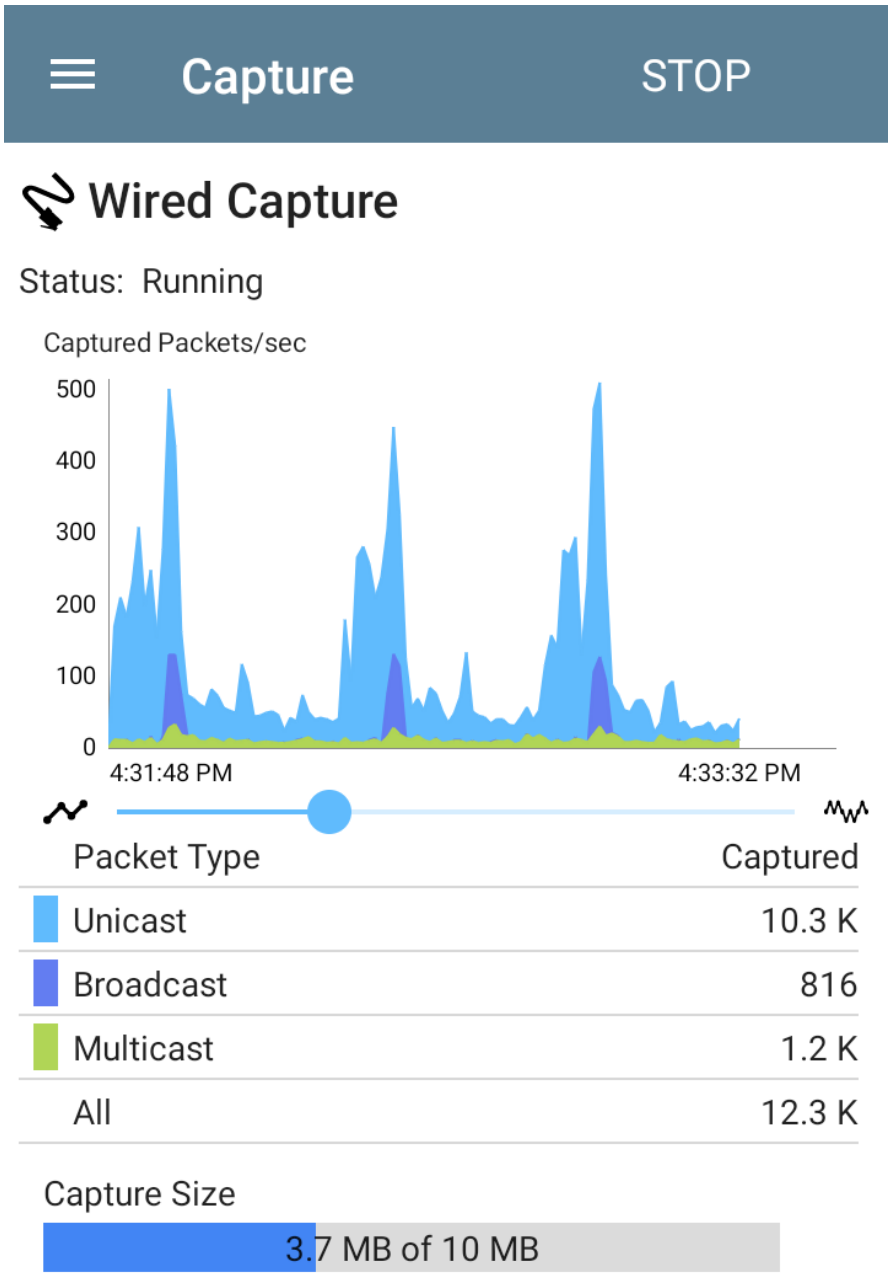
To start Capturing, tap **START** at the top of the app screen.



The current Status of the capture and any applied filters are shown under the capture type. The image above indicates that the app captures traffic for IP 10.200.72.19 only.

The Capture screen shows the real-time status of the capture as it runs.

The Wired graph plots the type and number of packets being captured while the capture is running and includes Unicast, Broadcast, and Multicast packet types.

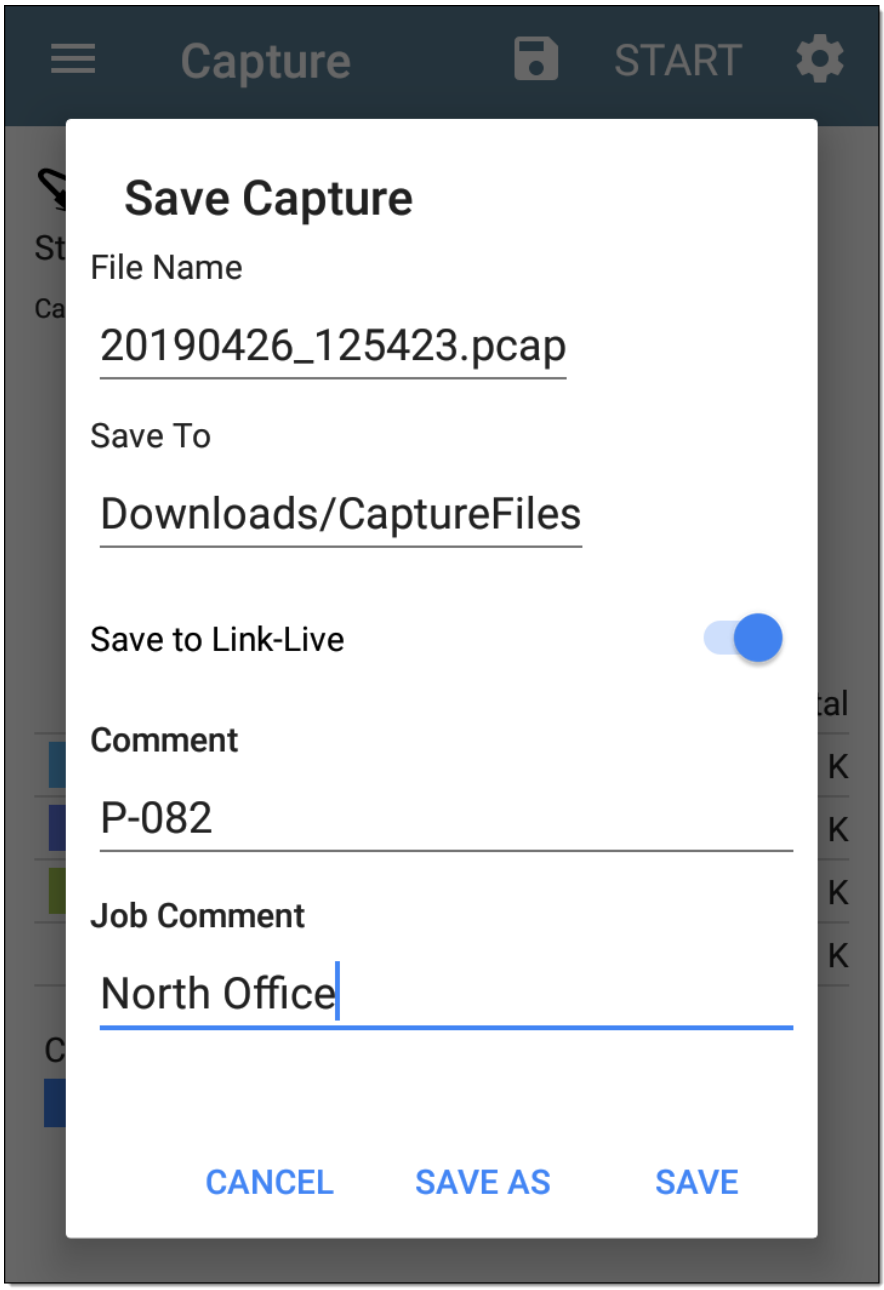


- If you navigate away from the Capture app, the capture process continues to run in the background until the File Size Limit (see Capture Settings) is reached.

- To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.
- Tap **STOP** to stop the running capture before it reaches the File Size Limit.

Once a capture is completed, the **Save Capture** dialog appears automatically.

Tap the Save icon  to reopen this dialog.



Captures are saved as .pcap files. Tap any of the fields in the dialog to enter changes.

File Name: Capture files are automatically named using the date and time. Tap this field to enter a custom name.

Save to: By default, capture files are saved in the **Downloads** folder in the LRAT file system. You can also save them to a USB storage device or choose a different folder by tapping the **Save to** field. See also Managing Files.

Save to Link-Live: You can also upload capture files to Link-Live and then download them for analysis on a PC. Capture (.pcap) files appear on the Uploaded Files page in Link-Live.

Comment: This comment is attached to your capture file when it is uploaded to Link-Live.

Job Comment: This is the persistent Job Comment that uploads to Link-Live with all test results and files, until you change it. Changing the Job Comment here changes it throughout your unit.

Back to Title and Contents

Discovery App

The Discovery application creates an inventory of the devices on your networks along with their attributes: device types, names, addresses, interfaces, VLANs, resources, and other connected or associated devices. The app allows you to identify and analyze network devices and acts as a jumping-off point for further analysis using other apps, such as Path Analysis, and connection tests.

NOTE: This application applies to the LinkRunner AT 4000 only.

Discovery Chapter Contents

This chapter describes how the Discovery process and app screens work, shows examples of Discovery data, and details the Discovery settings.

Introduction to Discovery

Discovery uses Ethernet and fiber to find, classify, and display the details of network components. Information provided by Discovery can include the following:

- IP, BSSID, and MAC addresses
- Device Names
- Device Connectivity
- SNMP Data
- Network Problems
- Interface Details and Statistics

Devices are discovered via ARP and Ping sweeps; SNMP, DNS, mDNS, and netBIOS queries; and passive traffic monitoring. Discovery classifies each device as it is found. Up to 2,000 devices can be reported.

The Discovery app also detects Problems with discovered devices, including **Warning** and **Failure** conditions.

The LRAT's discovery process begins when the unit is powered on. Once a network connection

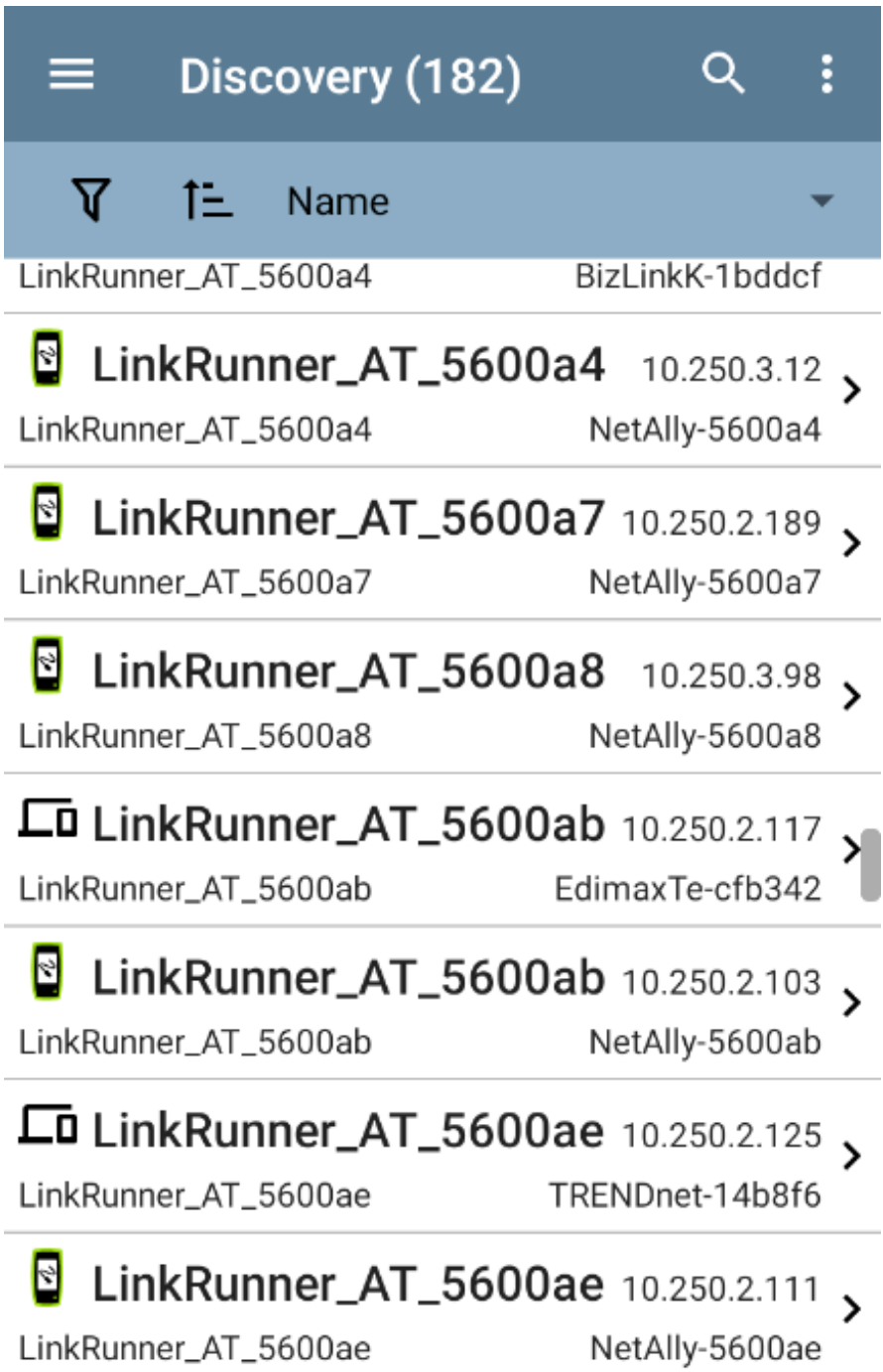
(test or management) is established, the active discovery process begins.

Discovery notification icons  indicate the progress of active discovery. This icon  indicates that no links are currently available for active discovery, either because none of the ports enabled for discovery are connected or because AutoTest is running.

The Discovery app consistently monitors network traffic, but the active discovery process reruns every 90 minutes by default. You can select a different Refresh Interval in the Discovery Settings.

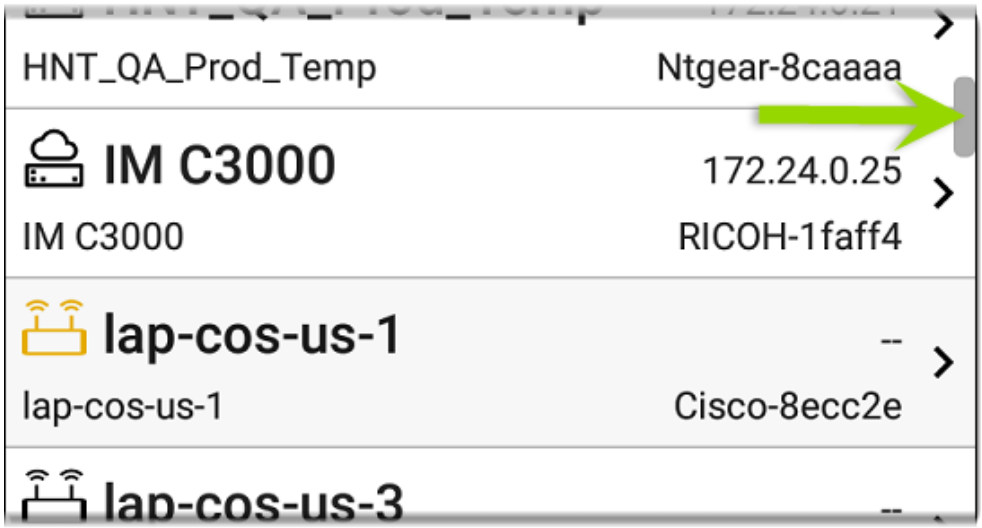
Main Discovery List Screen

The main Discovery screen lists all the devices the LRAT has discovered.



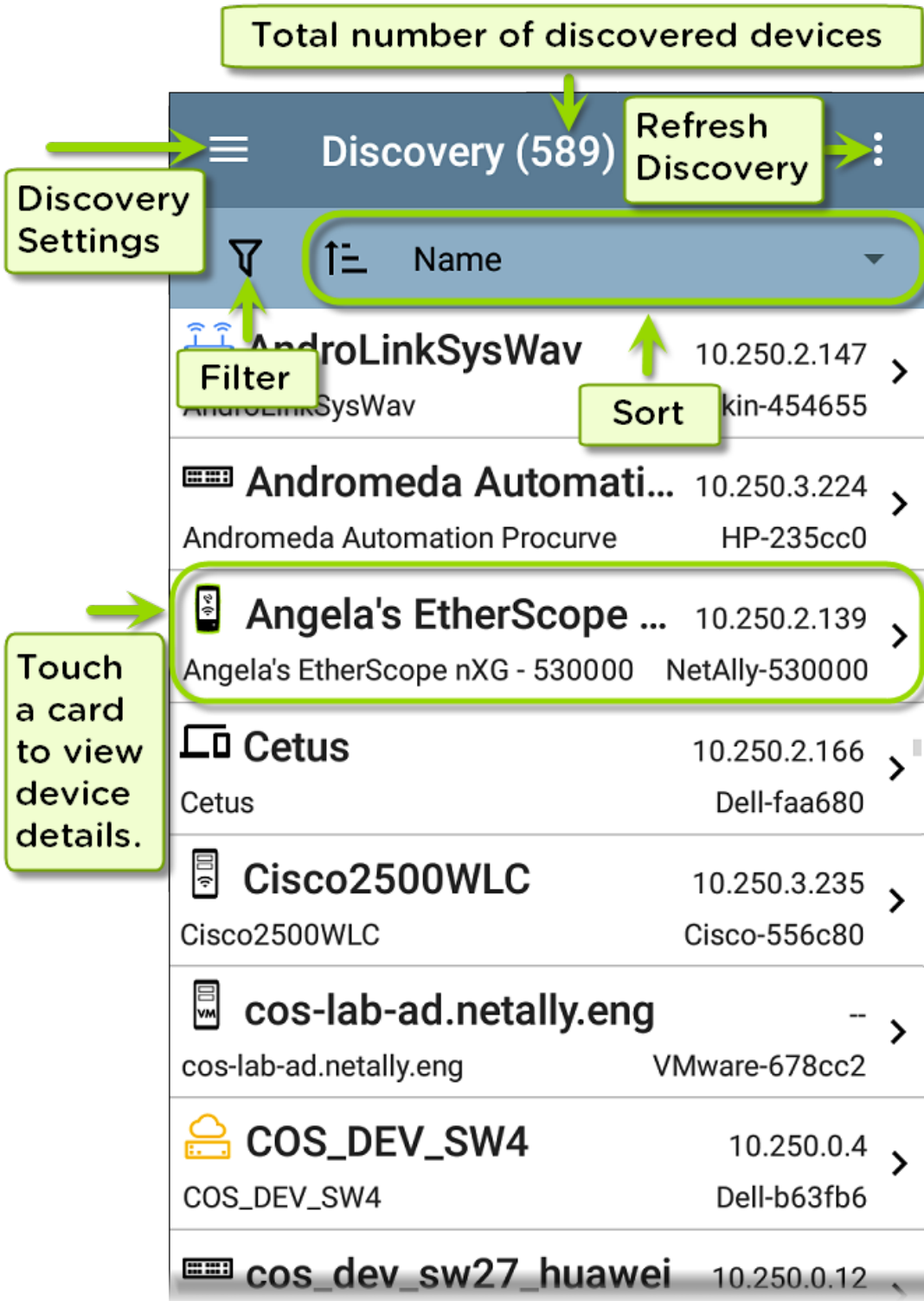
Like in AutoTest and other LRAT screens, the icons in Discovery change color to indicate a **Warning** or **Failure** condition. Discovery also displays device icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous Problem has been resolved. (See the Problem Settings to adjust enabled Problems and thresholds.)

The Discovery screen, and other app screens with long lists, supports fast scrolling. Touch and drag the scrollbar handle to the right of the list to scroll quickly up and down.



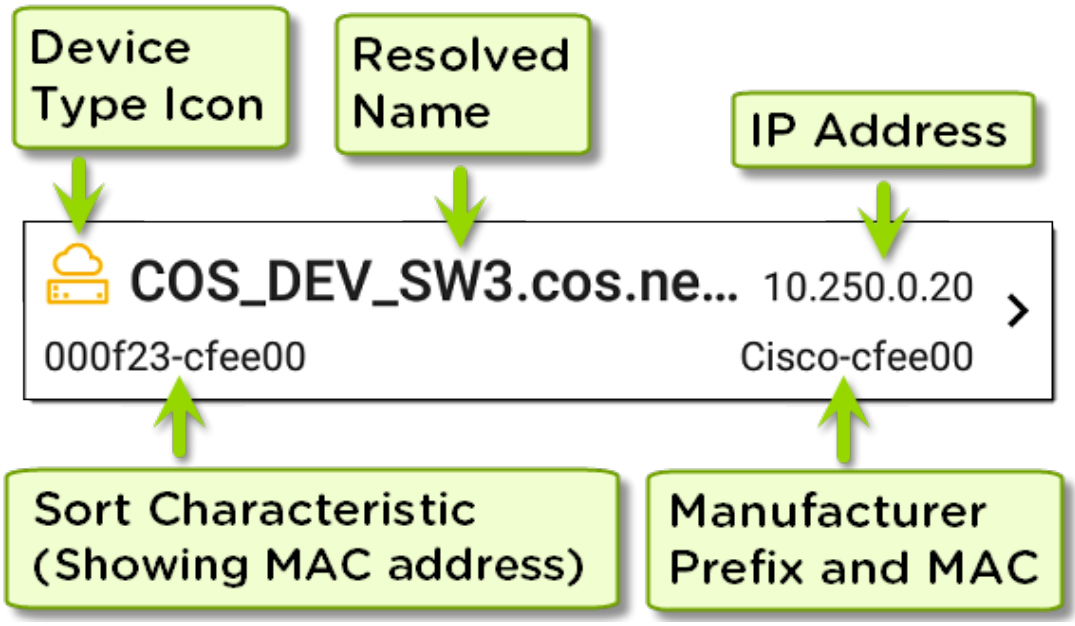
From the main Discovery screen, you can filter and sort the listed devices, open the left side

navigation drawer to configure settings, and tap a device's card to view its details.



Discovery List Cards

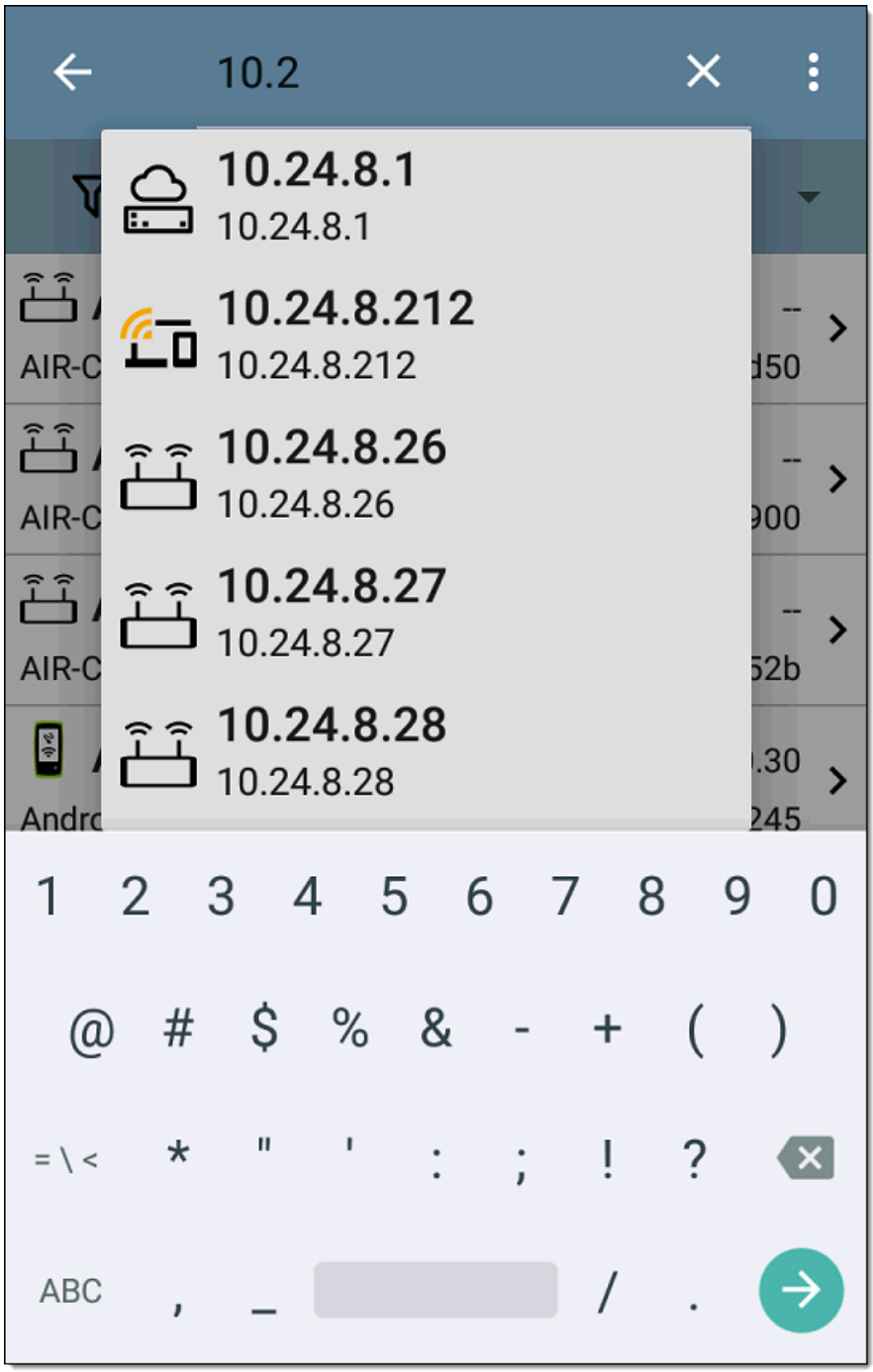
The information displayed on each device card varies depending on the selected Sort element and the data the LRAT was able to discover.



The lower left field displays the characteristic by which the Discovery list is currently sorted. In the image above, the list is sorted by MAC address. See Discovery Sorts in this topic for more about sorting.

Searching the Discovery List

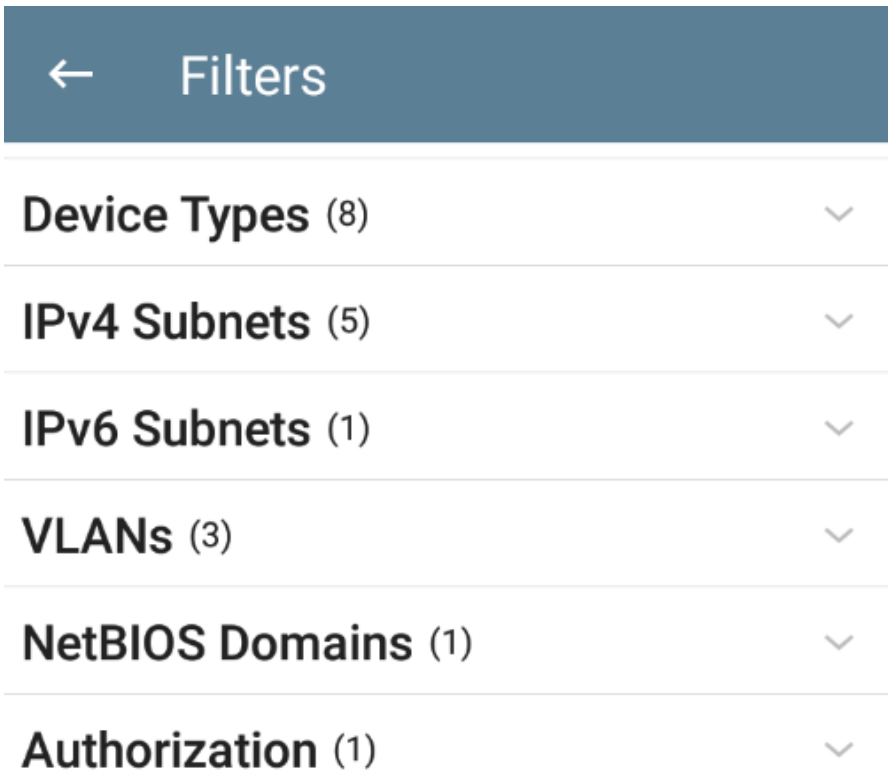
The main Discovery screen offers a search feature. Tap the search icon at the top of the screen to search discovered devices.



Filtering the Discovery List

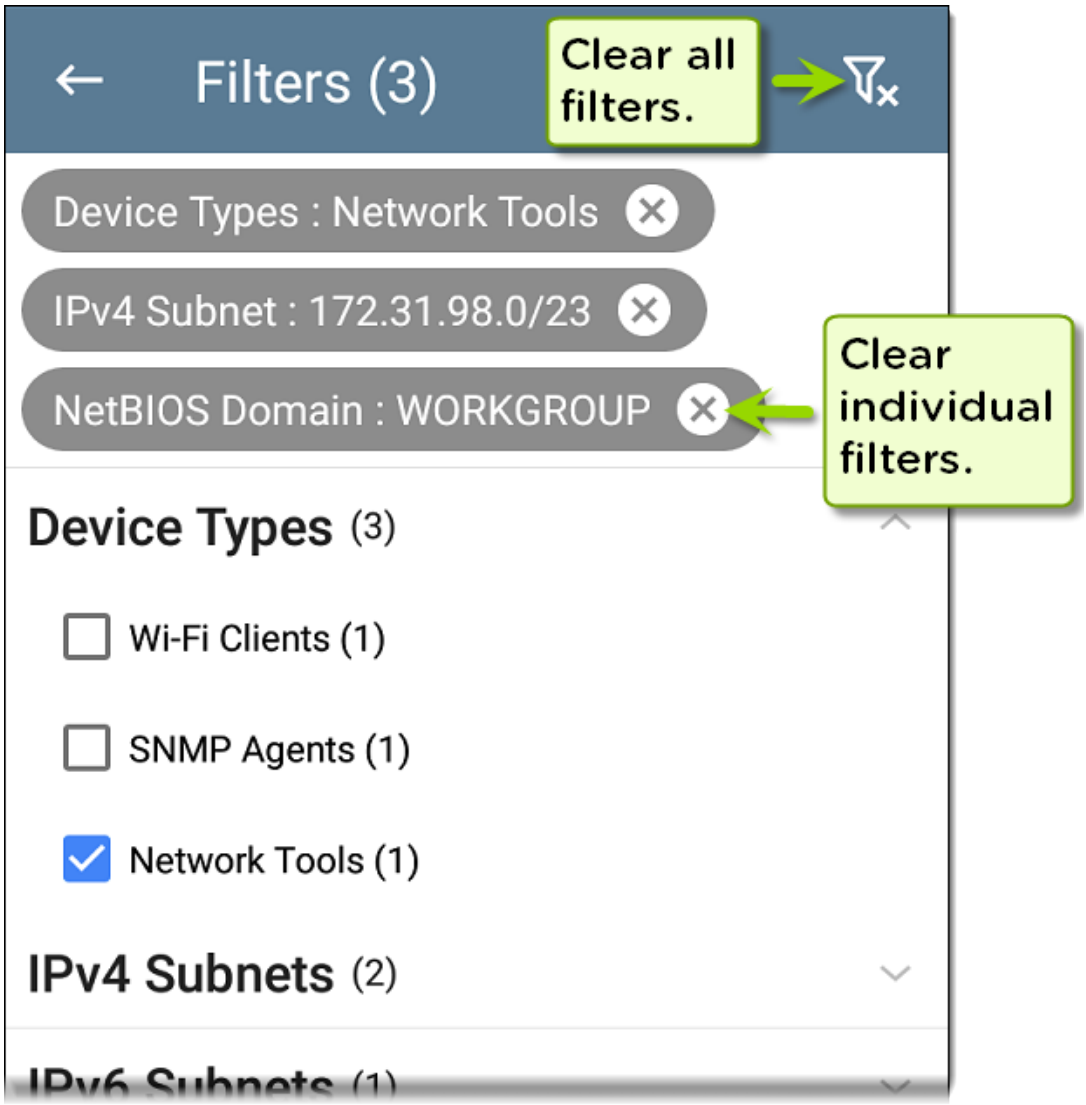
Tap the filter button near the top left of the main Discovery screen to set filters that control

which devices are displayed in the list.



The Filters screen displays the number of devices or domains discovered for each category. Tap a category name to select filters by checking the boxes. The main Discovery screen shows only those devices or IDs that fall under your chosen filter parameters.

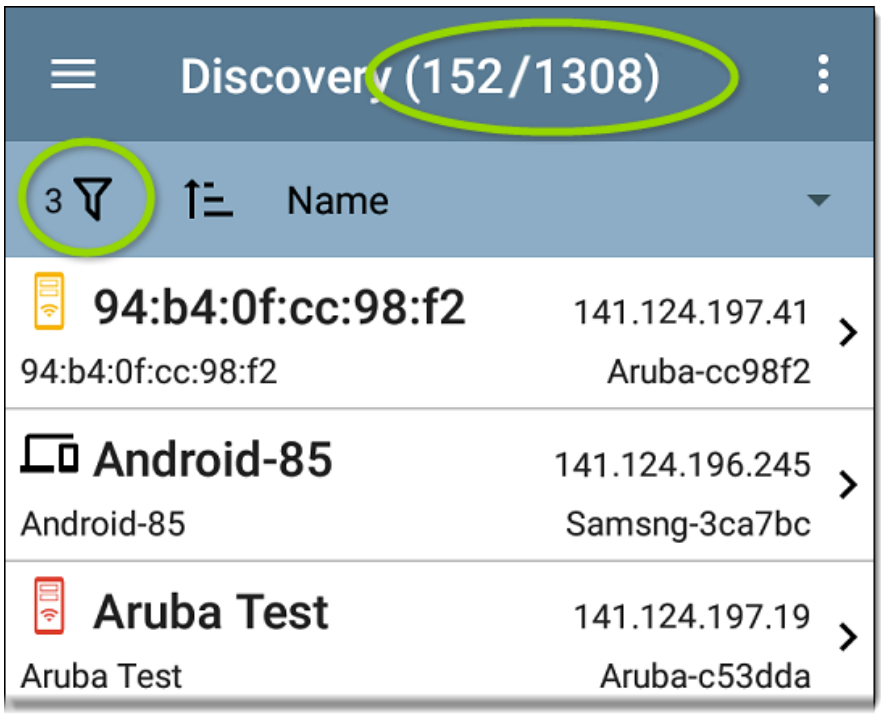
When filters are selected, those active filters are displayed at the top of the Filters screen.



- Tap the ✕ button to the right of each filter to clear it.
- Tap the clear filter icon at the top right to clear all filters.

After you select a filter, the Filters screen displays results filtered for that characteristic. For example, in the image above, the user has selected the **Network Tools** device type. As a

result, only those subnets, addresses, etc., with a discovered Network Tool remain selectable in the filters list.

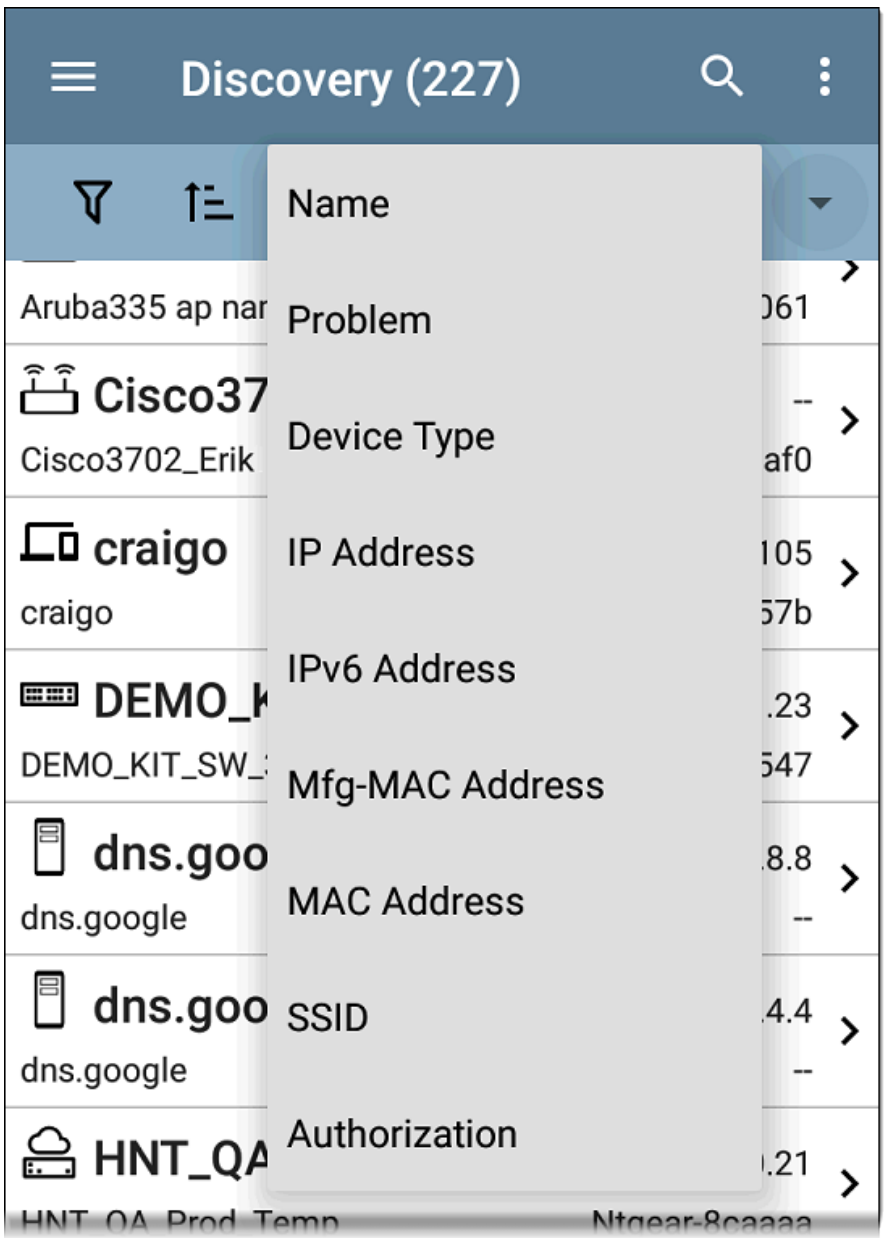


Back on the main Discovery screen, the screen title shows the number of filtered devices out of the total discovered devices (in the image above, 152 filtered devices out of 1308 total).

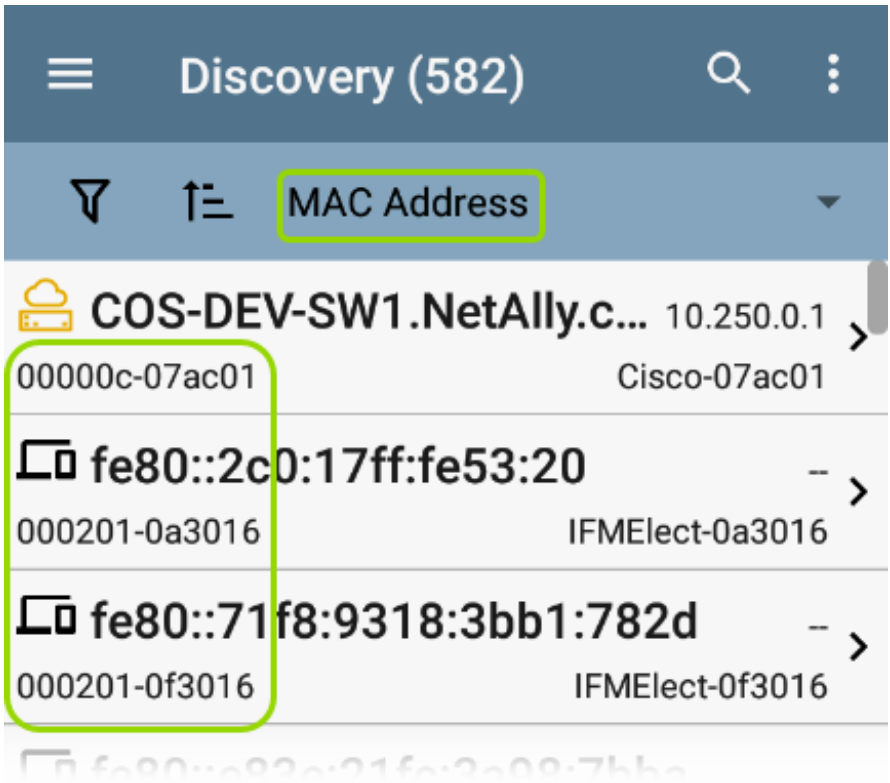
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

Sorting the Discovery List

Tap the Sort bar or down arrow to open the Sort drop-down menu.



Select a Sort option to order the devices based on your selected characteristic.



The selected Sort option displays in the Sort bar above the device list, and the sort characteristic for each device is shown under the device type icon. In the image above, all devices are sorted in order of the MAC Address.

Tap the sort order icon to switch the sort order between normal and reverse order.

Devices are sorted in groups. Those with resolved names appear at the top (in normal order), and then devices with only IPv4, IPv6, and MAC addresses appear below, respectively. Reversing the normal sort order reverses the

devices within the groups but does not change the order of the groups.

Security Auditing – Batch Authorization

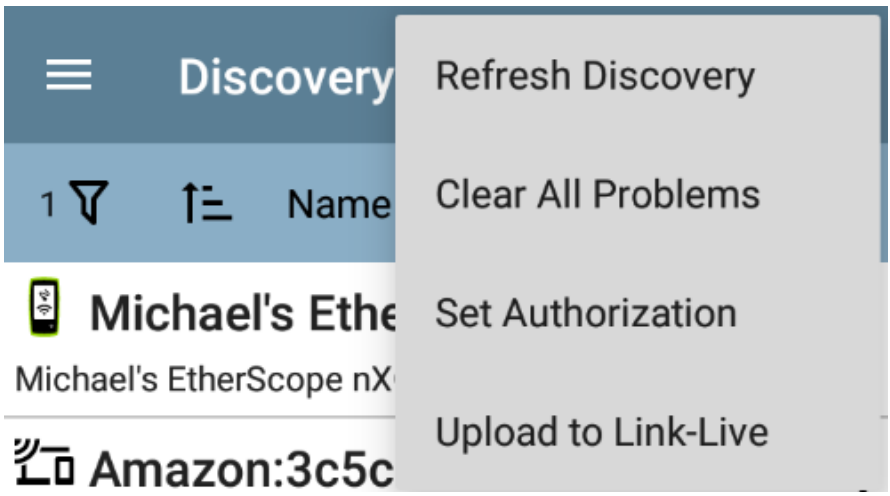
Batch Authorization lets you extend filtering to organize devices into the following security categories:

- **Authorized**: For devices approved for use on your network
- **Neighbor**: For devices owned and controlled by neighboring organizations
- **Flagged**: To give visibility to a specific device
- **Unknown**: For devices that have not been identified or classified
- **Unauthorized**: For devices that should not be on the network and may present a security risk
- **Unspecified**: Default unassigned Authorization status

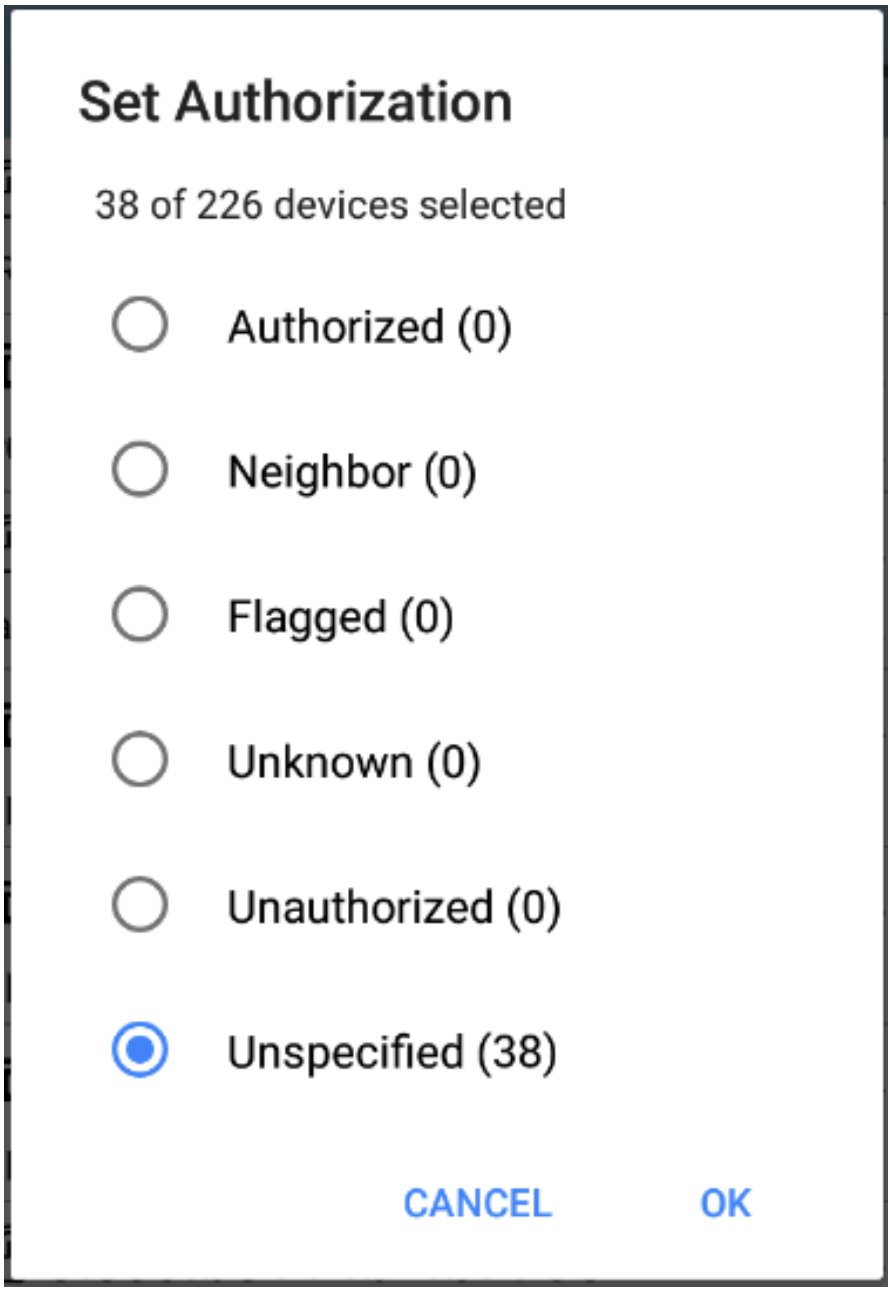
Once categorized, it is simple to immediately identify any new devices on the network by

filtering according to Authorization type. New devices are identified as Unspecified.

To use the Batch Authorization feature, create a filter that identifies the devices you want to categorize. For example, you could filter on IP Addresses used by other offices in your building. After you filter the list of discovered devices, select the overflow menu.

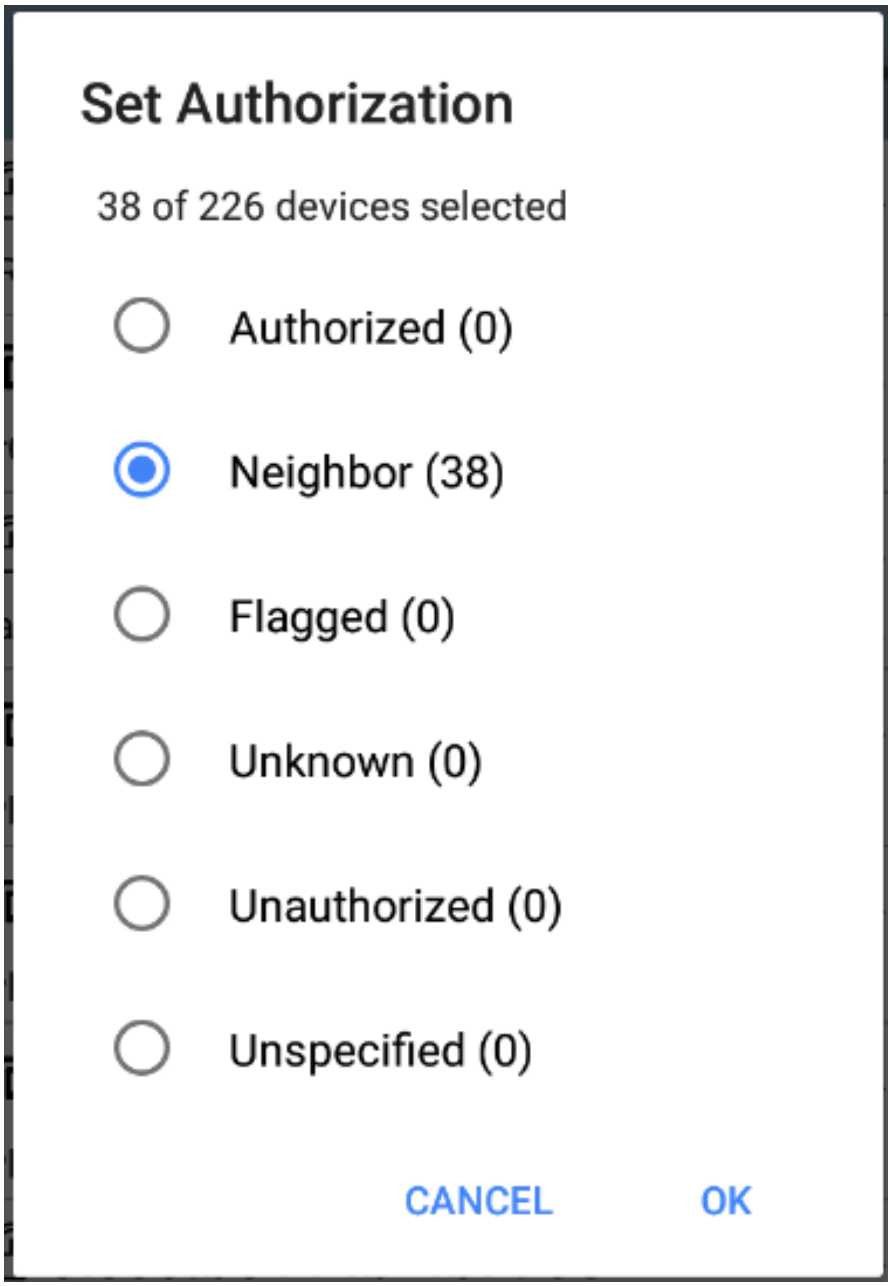


Select **Set Authorization** to see how these devices are currently categorized and the number of devices in each category. In the example below, 38 devices belong to other offices and have an Unspecified authorization.



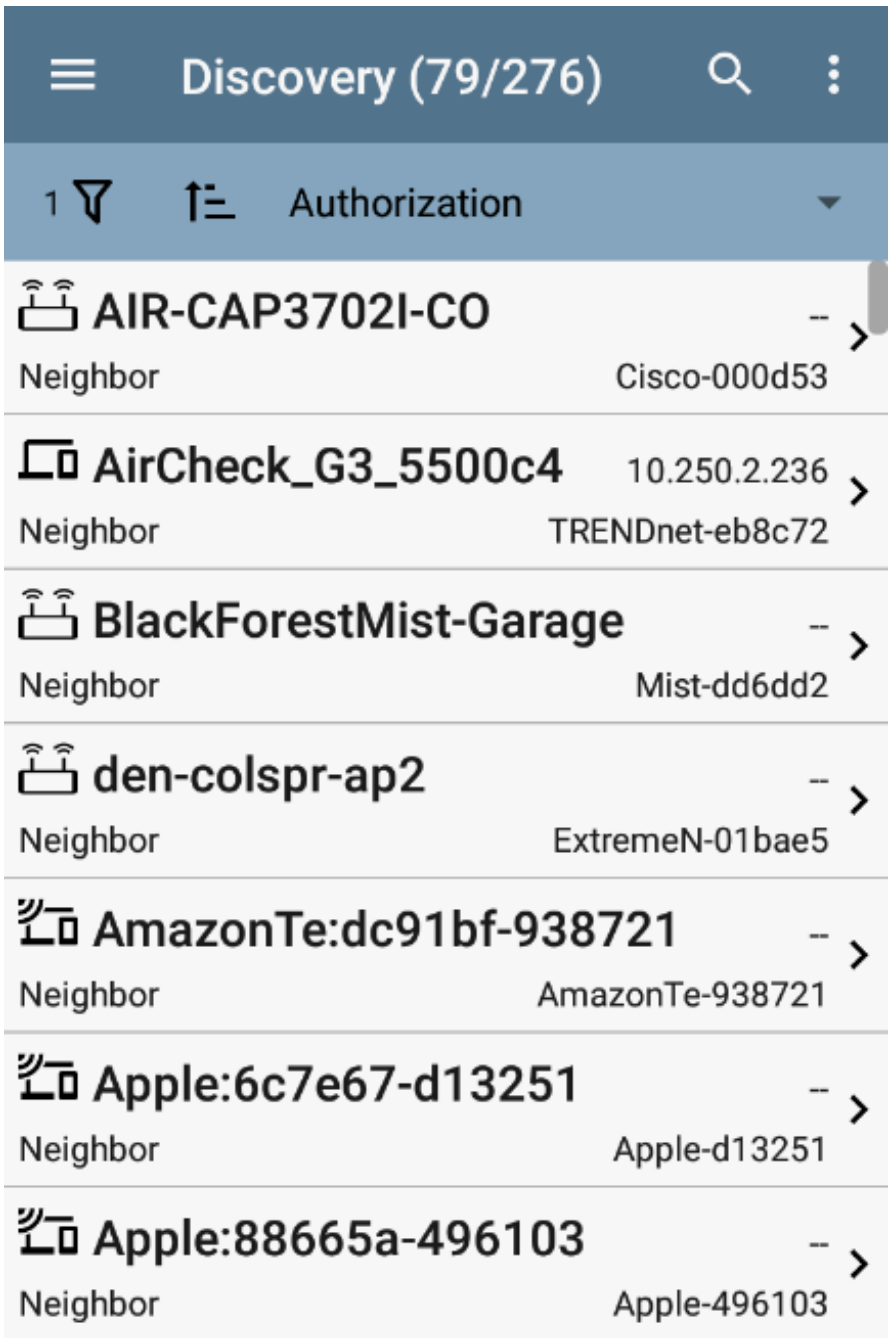
NOTE: The initial selection on this screen defaults to the category with the highest count. If other categories have non-zero counts, select **OK** to change the authorization settings for all devices to the selected category.

Select the appropriate security category. To continue the example above, you can select **Neighbor**, and then tap the **OK** button to identify the Unspecified devices from other offices as Neighbor.



You can filter the list by tapping the Filter icon , tapping **Authorization**, and then tapping

Neighbor to show only the Neighbor devices. You can also sort the list by Authorization to display the discovered devices with the Neighbor category clearly identified.



NOTE: Batch Authorization operates on the default MAC address of a device. If a device has multiple MACs, authorization is set only on the default MAC address. Devices that do not have a discovered MAC address, such as unknown switches and off-net devices, cannot have an authorization setting.

Refreshing Discovery

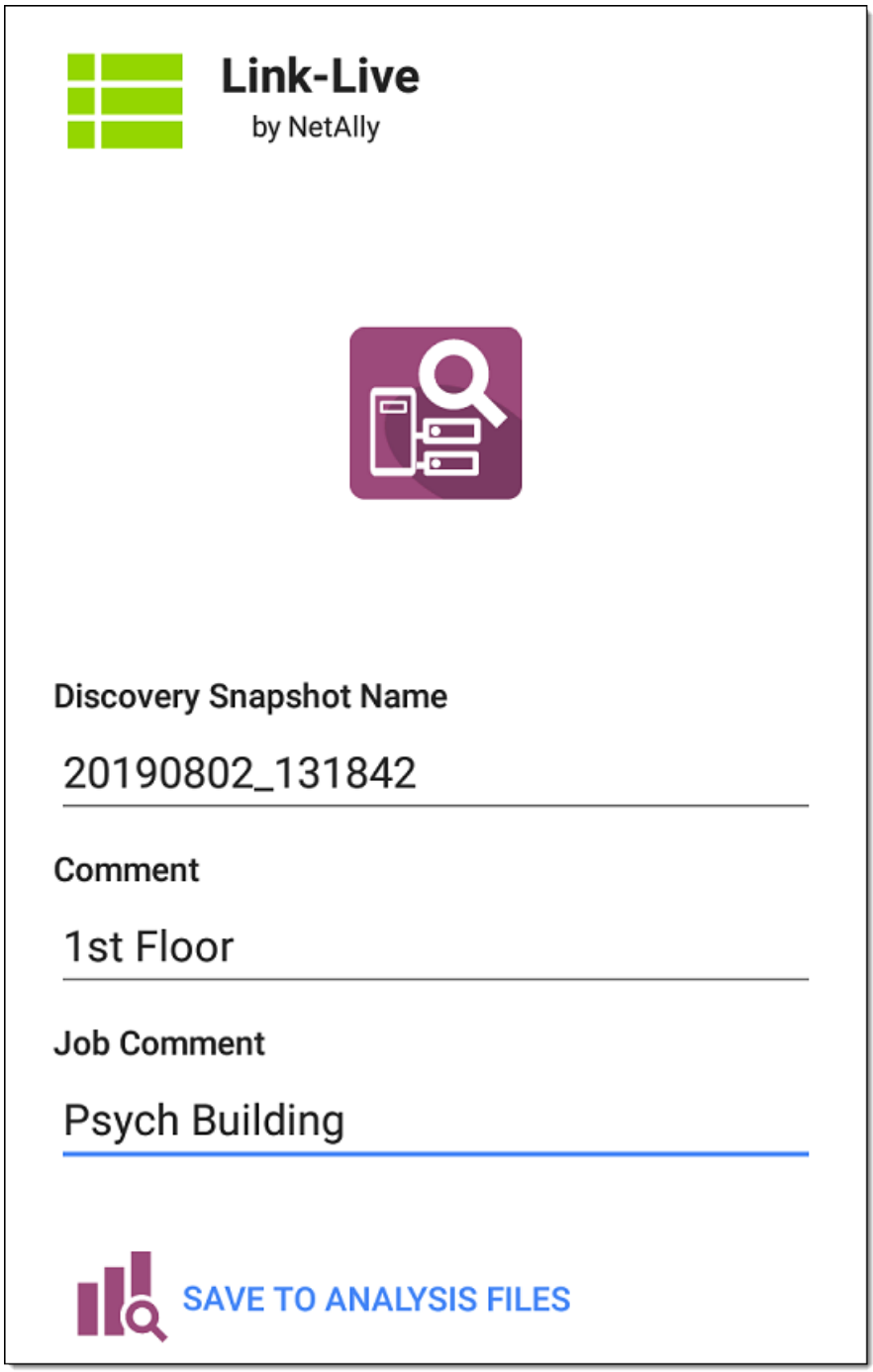
Tap the action overflow icon ⋮ at the top right of the main Discovery screen, and select **Refresh Discovery** to refresh the active Discovery process.

REFRESH DISCOVERY restarts the active discovery process without clearing the already discovered devices.

CLEAR AND RERUN DISCOVERY clears the accumulated results and restarts the discovery process.

Uploading Results to Link-Live

Tap the action overflow icon  at the top right of the main Discovery screen, and select **Upload to Link-Live** to send the current Discovery results to the Analysis page  on Link-Live.com.



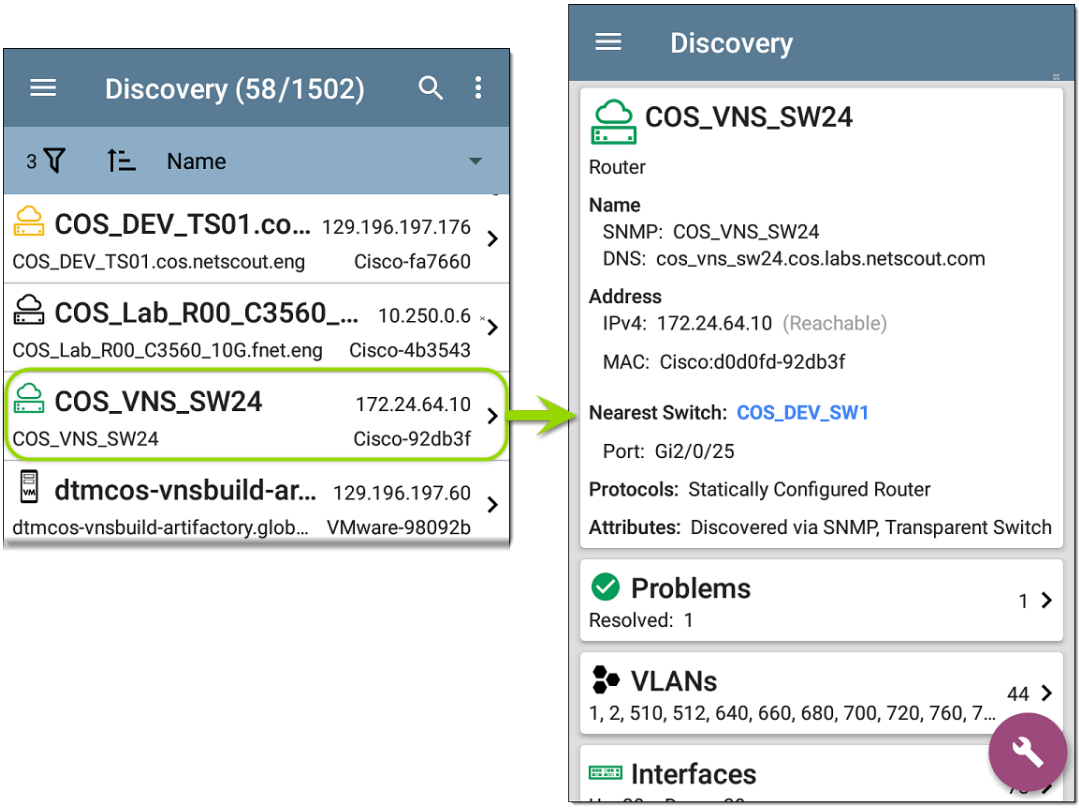
See the Link-Live chapter for more information.

Back to Title and Contents

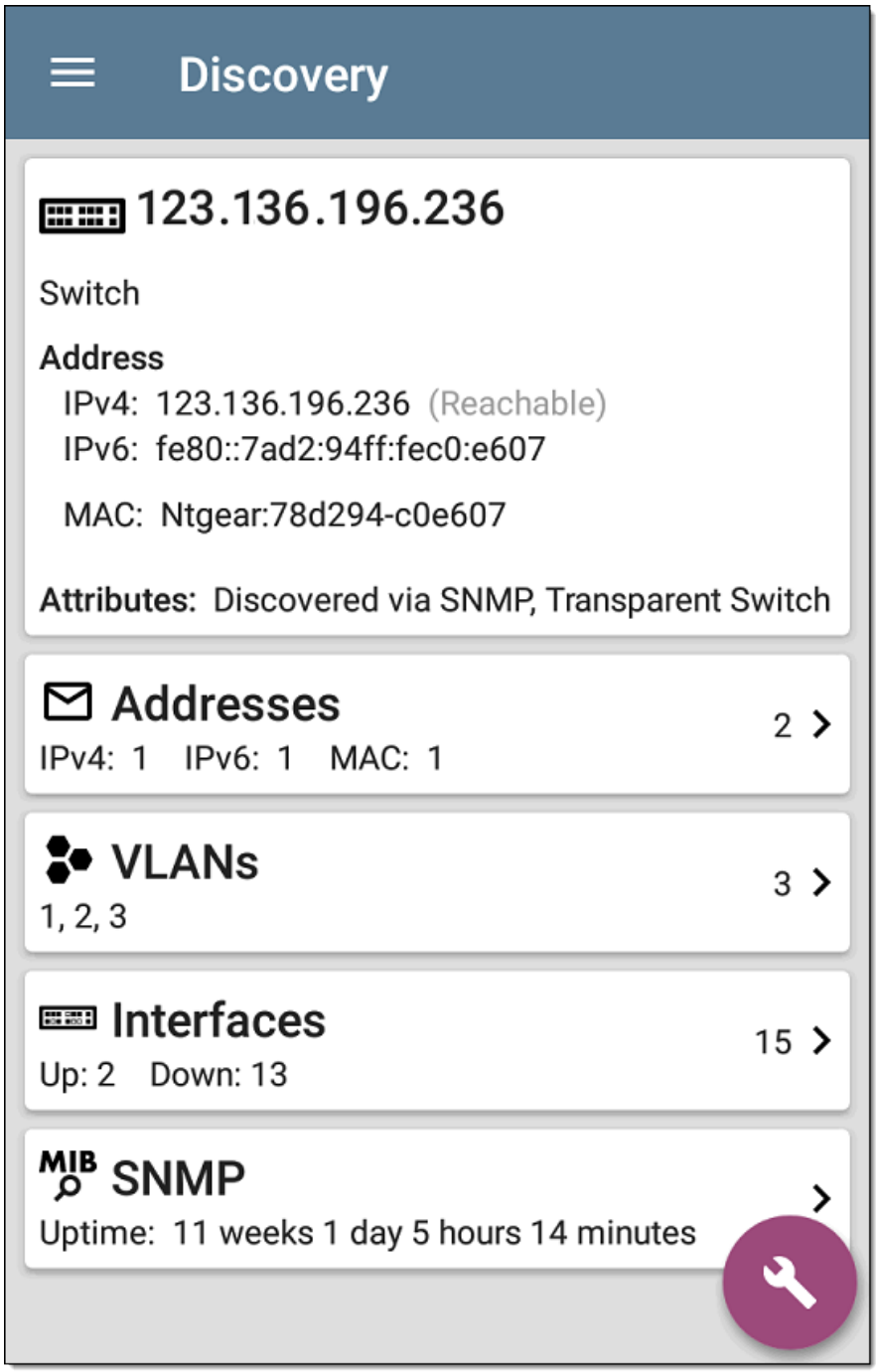
Discovery Details Screens

Tap any of the device cards on the main Discovery list screen to view Device Details.

The example below calls out a Router card and its Details screen.



The available data and actions on the Details screens vary significantly depending on the device type, connections, and data the LRAT was able to discover. In other words, only the discoverable information for each device is shown on the Details screen.



For the Switch screen shown above, Discovery was able to find an IP address but not a name for the switch.

Each Details screen shows additional information about the selected device, any Problems detected by the LRAT, and counts for other connected or corresponding network elements.

Each Details screen also has a FAB button that lets you take additional actions or run other applications on the device. The available actions and applications depend on the device type and connection available. See Discovery App Floating Action Menu for more information.

See Device Types for specifics about the different devices the LRAT can discover.

Top Details Card

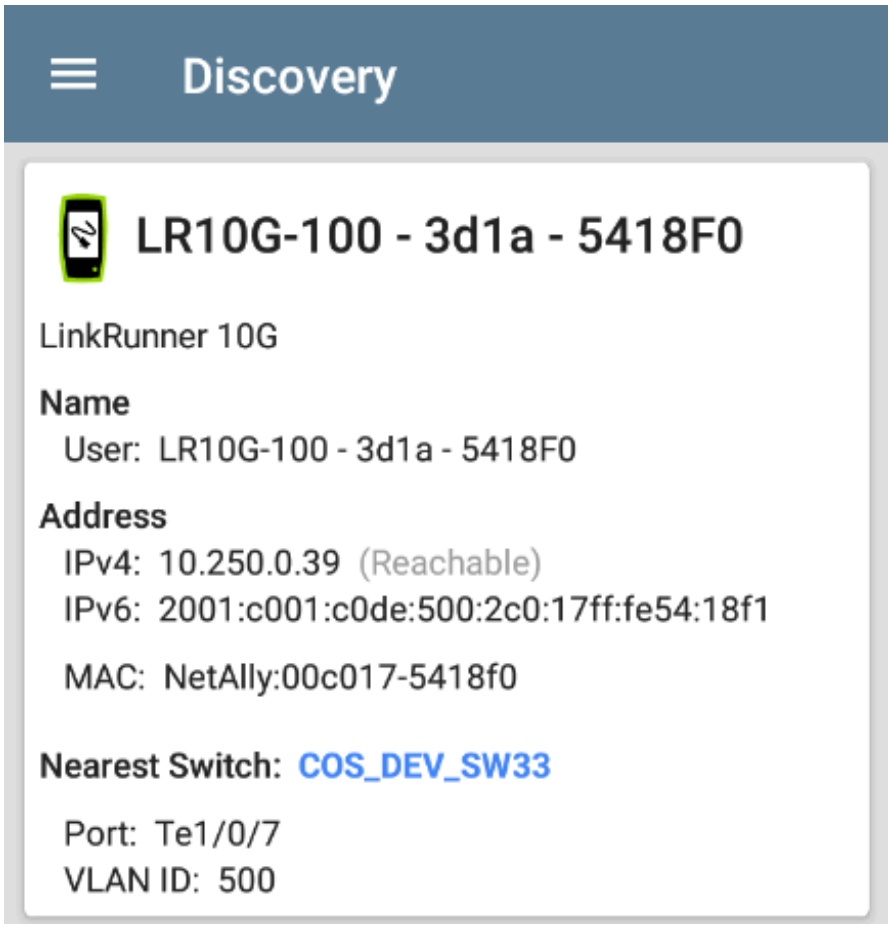
The top card on the Details screen summarizes the discovered data for the selected device.

The top of the card shows the device type(s) and icon (a Switch with a **Warning** status in the example image above).

The rest of the fields that appear on the top Details screen card depend on the device type and what the LRAT can discover about the device.

On the Discovery Details screens, you can tap any **blue linked name or address** to open a Discovery screen for the linked device.

> NOTE: Non-underlined links open in the same app (in this case Discovery), and **underlined links** open in a different app .



The Nearest Switch link opens a Discovery app Details screen for that device.

Data Fields on the Top Details Card

These fields may appear on the top card of a Device Details screen, depending on the device type and the information LRAT discovered:

Name: Discovered hostname(s) of the device. This section can display user-defined, DNS, mDNS, SNMP, NetBIOS, AP, and Virtual Machine names as discovered.

Address: Discovered IPv4, IPv6, and/or MAC addresses of the device. This section displays the default (first discovered) addresses of each type. For more addresses, select the Addresses card when available.

> **Authorization**: This field shows the user-assigned Authorization status of the device. See Assigning a Name and Authorization to a Device.

Nearest Switch: Name or address of the switch identified as closest to the device

> **Port**: Physical port where the device is connected
>
> **VLAN ID**: ID of the VLAN the device is on

Protocols: Routing protocols, discovered via packet analysis, operating on the device or network

Services: Network services provided by this device, such as DHCP or DNS

Attributes: Other discovered attributes about the device

Hypervisor: Name of the hypervisor on which a virtual machine is operating

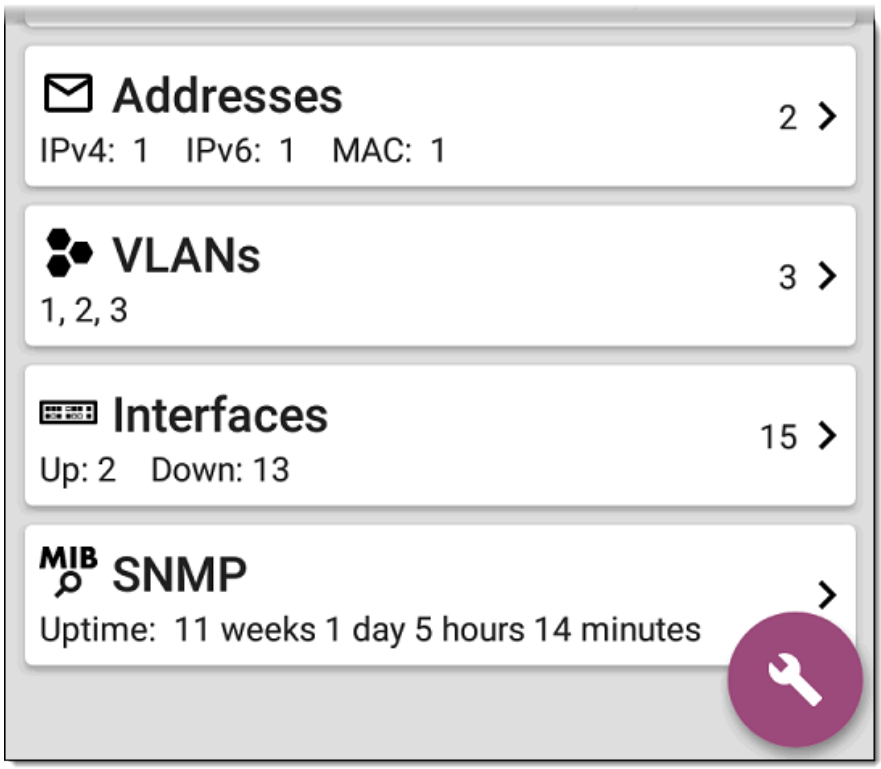
Virtual Machine: Name of the virtual machine

- **Guest OS**: Operating system running on the virtual machine
- **Memory Reservation**: Amount of memory reserved for the virtual machine

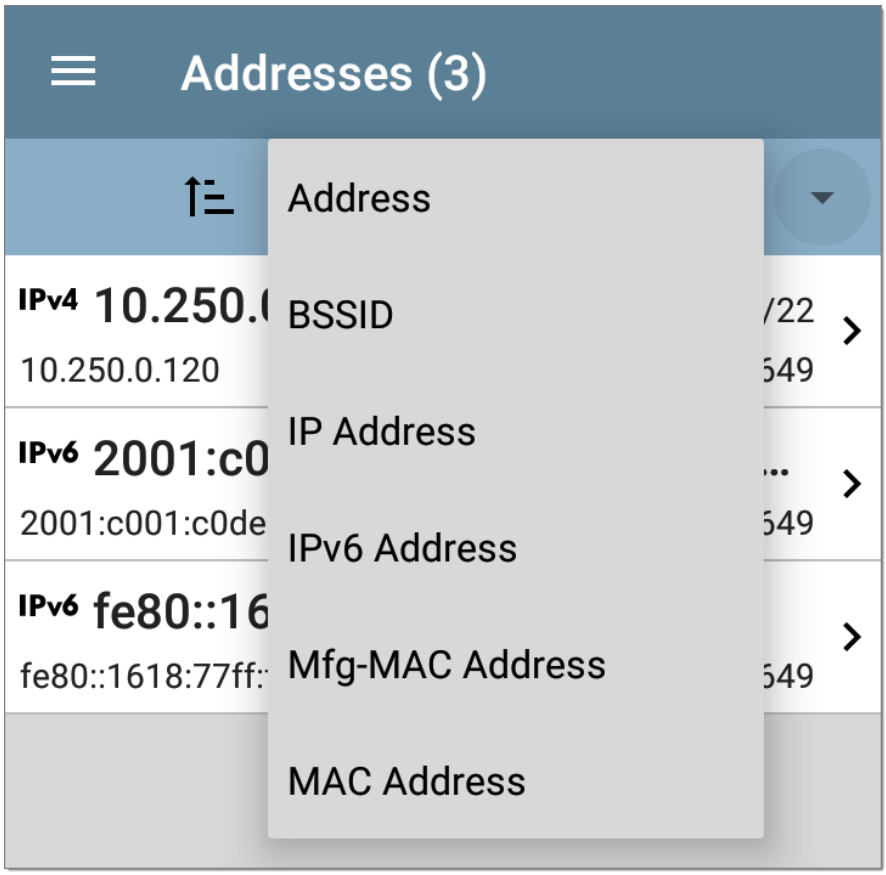
Last Seen: Time at which LRAT most recently detected the device

Lower Cards in Device Details

Tap any of the lower cards on a Device Details screen to view more discovered characteristics and "drill down" to specific Problems, Addresses, Interfaces, etc. for the selected device.



Screens with a list, such as Addresses shown below, also offer Sort options.



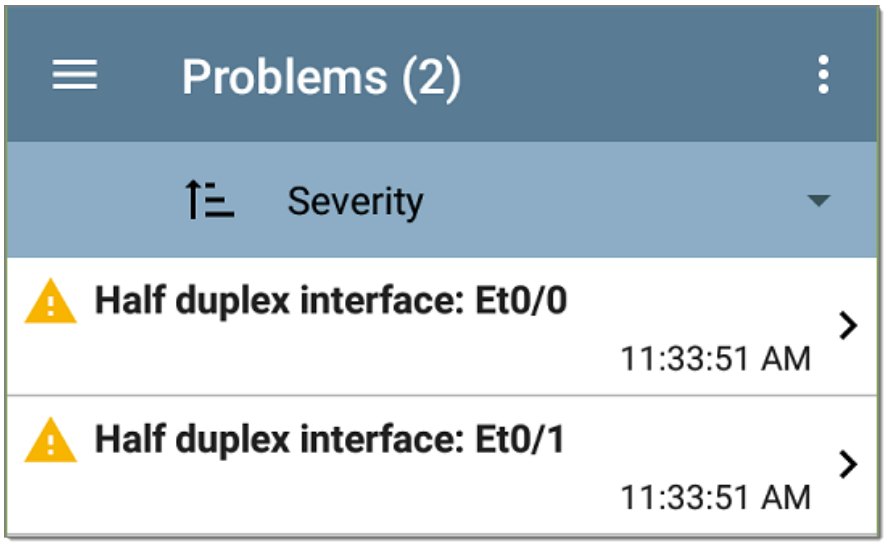
The rest of this topic provides examples of each type of Details screen and options for additional analysis.

Remember, you can tap any card with a right pointing arrow › to open a new screen with more information about the device or characteristic.

Problems

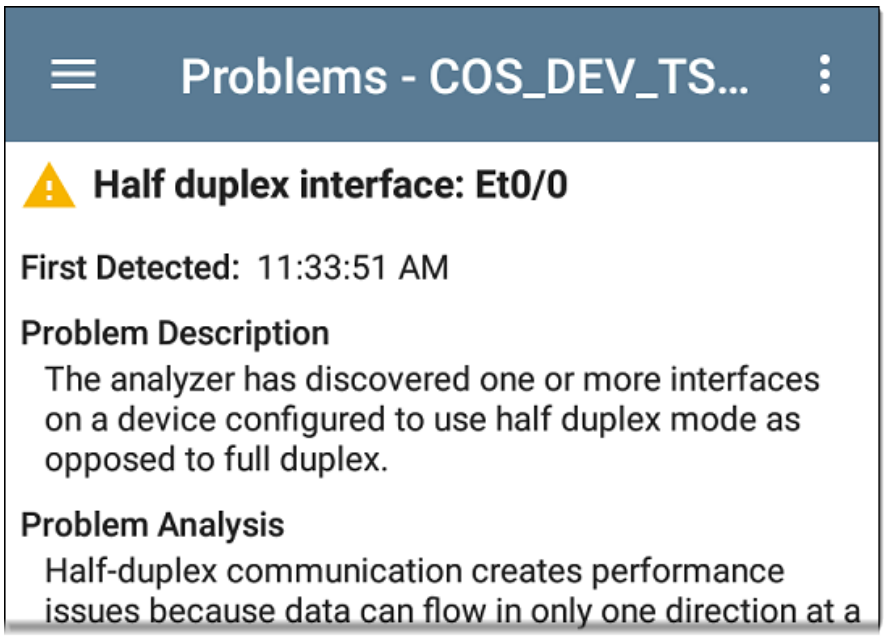
The Problems card shows the icon color of the highest severity problem, and the number of detected **Warning**, **Failure or Error**, **Information**, and **Resolved** conditions for the device or network component.

Tap the Problems card to view the Problems list screen (unless only 1 Problem is detected, in which case, the detailed Problem description opens, skipping the list screen).



Tap the sort field to sort the list by **Severity** or by the time when the problem was **First Detected**.

On the Problems list screen, tap a Problem's row to read a detailed description.

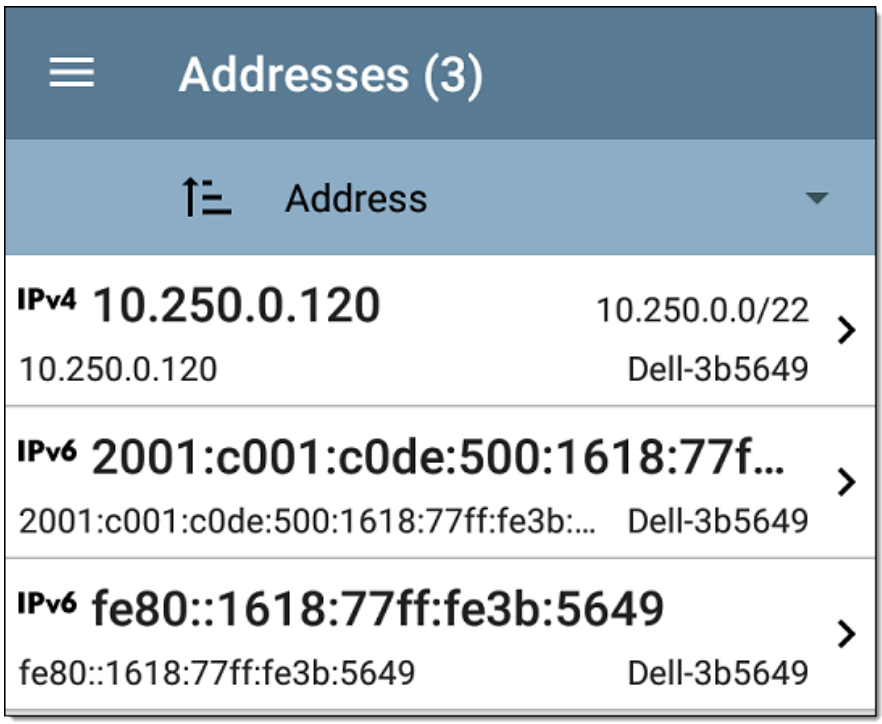


To clear a problem, tap the action overflow button ⋮ at the top right of the Problem list or description screen, and then tap **Clear Problem**.

See Problem Settings to select which problems are detected and displayed by your unit.

Addresses

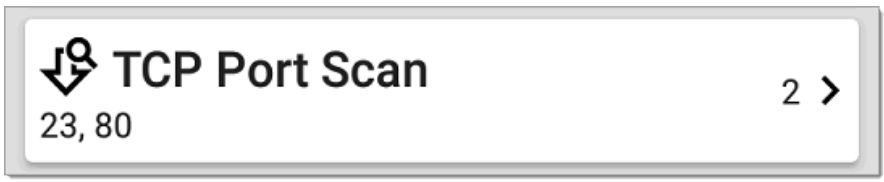
The Addresses card displays the number of each type of address discovered: IPv4, IPv6, MAC. Tap to view the addresses and related information.



From the Addresses list screen, you can sort the list order and tap any of the discovered addresses to investigate the address further.

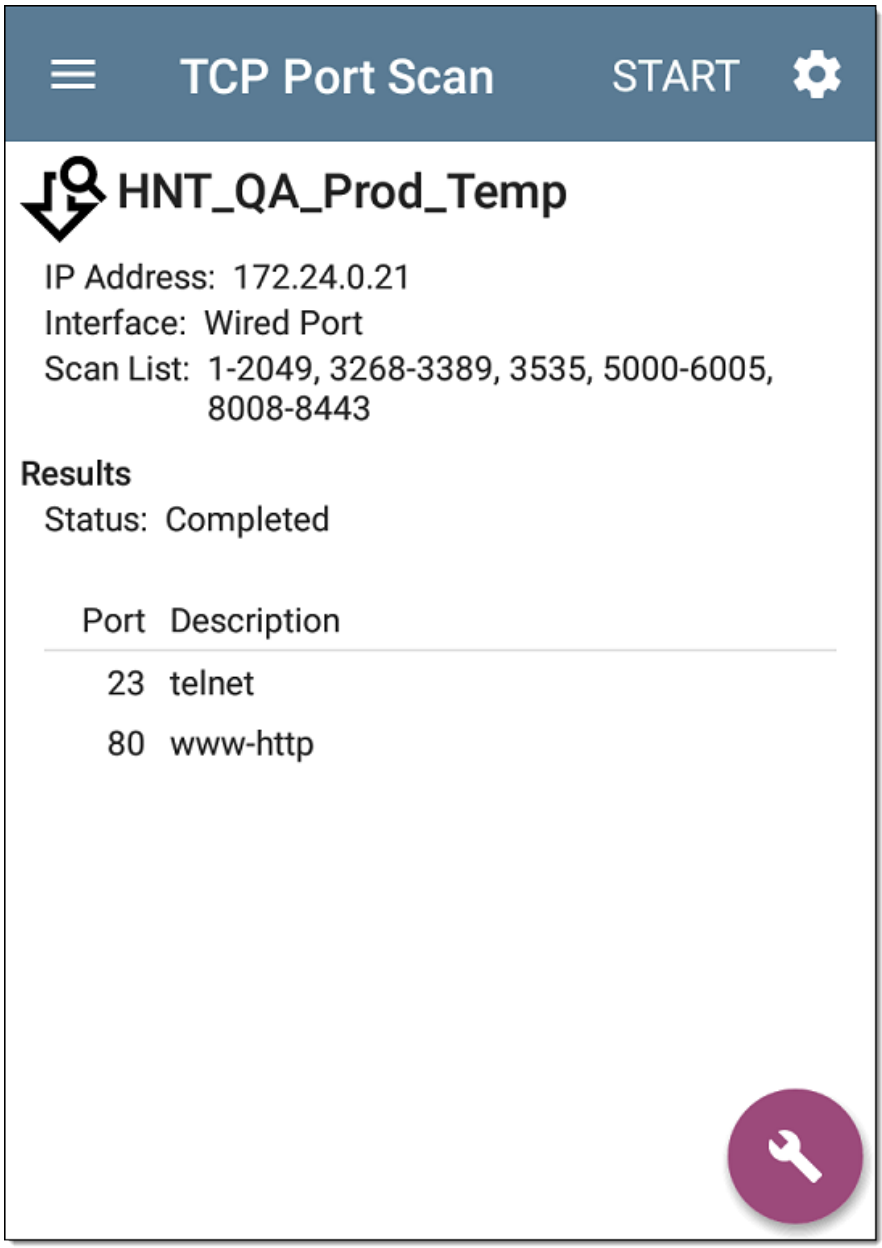
TCP Port Scan

If you have run a TCP Port Scan (from the Discovery FAB) on a device or IP address, a TCP Port Scan card appears on the device's Details screen.



This card lists open port numbers and shows the total quantity of open ports. Tap the card to open the TCP Port Scan screen.

You can also open this screen from the Discovery floating action menu.



The top of the TCP Port Scan results screen shows the name or IP address of the tested device and the following fields:

IP address: IP address of the device that was scanned

Interface: Test or management port from which the test ran, set in the TCP Port Scan settings

Scan List: List of port numbers tested

Results

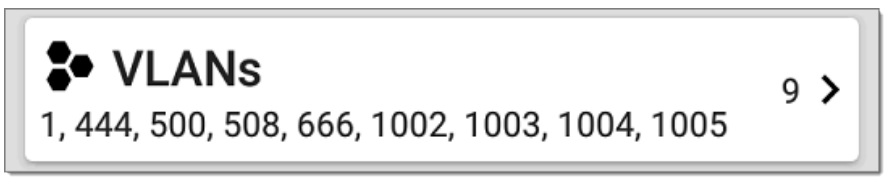
Status: Current status of the port scan

Port/Description: List of all the detected open ports with their descriptions

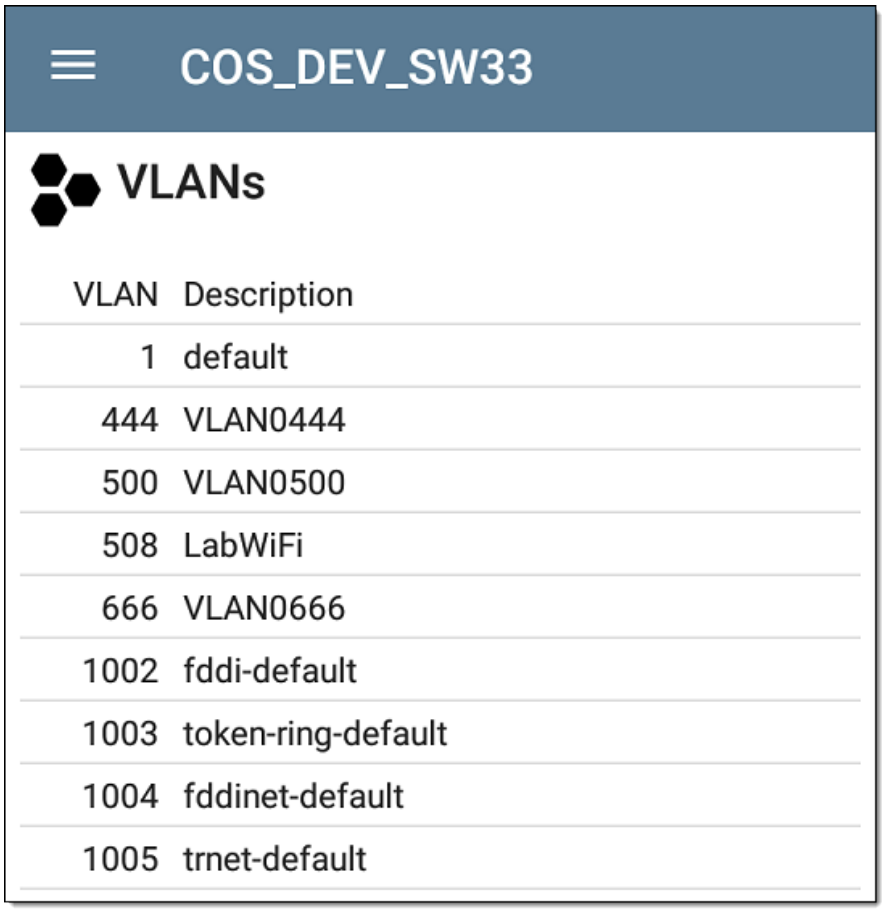
See also TCP Port Scan Settings.

VLANs

The VLANs card displays the VLAN IDs this device is using or for which it is configured.



This card does not appear if no VLANs are detected or configured. Tap the card to open the VLANs screen.



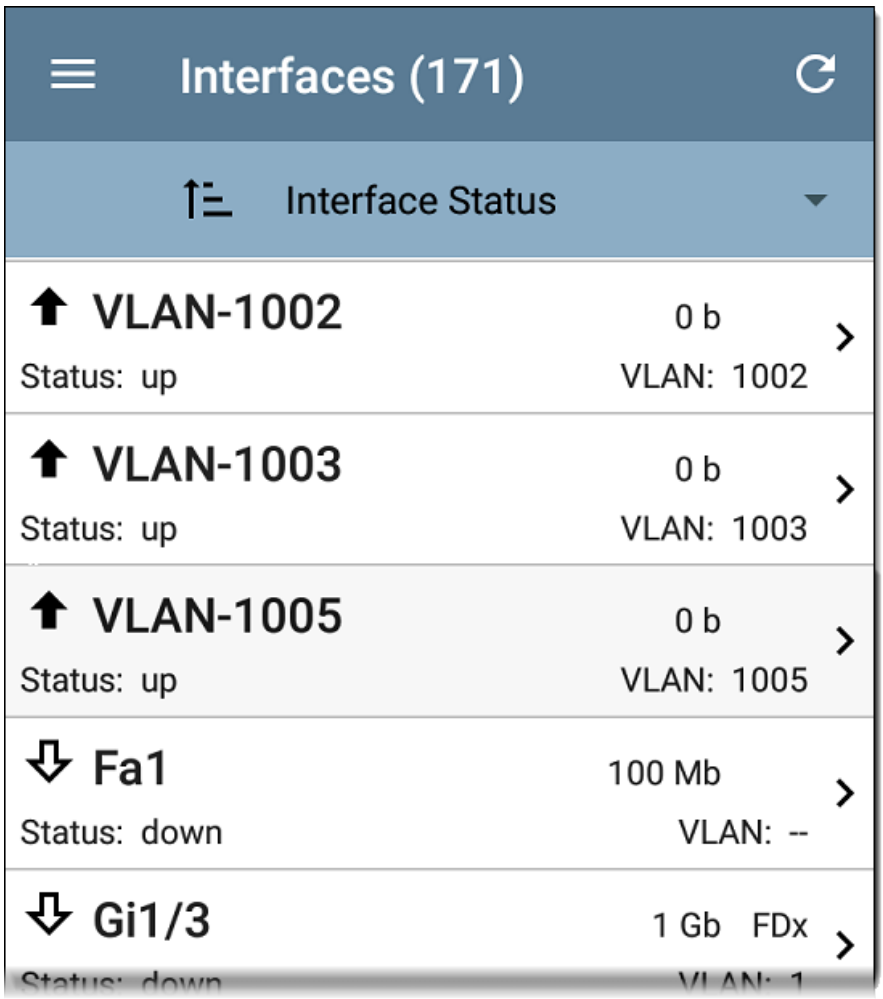
The VLANs Details screen also shows the description with each VLAN ID.

Interfaces

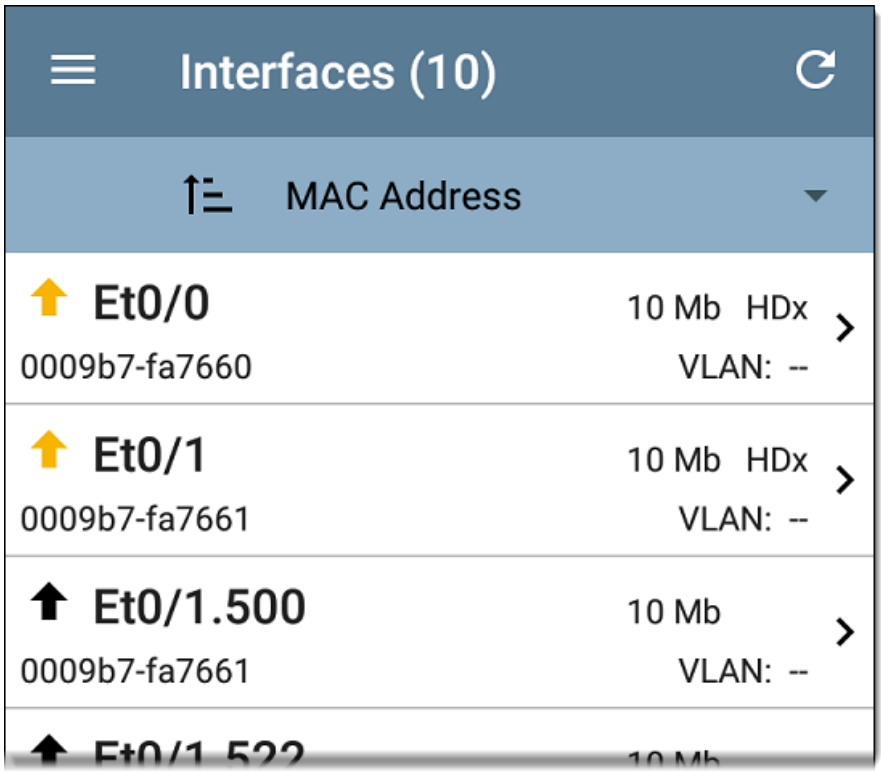
Interface are discovered using SNMP.

The Interfaces card shows the number of Up and Down interfaces and the total number of Interfaces to the right.

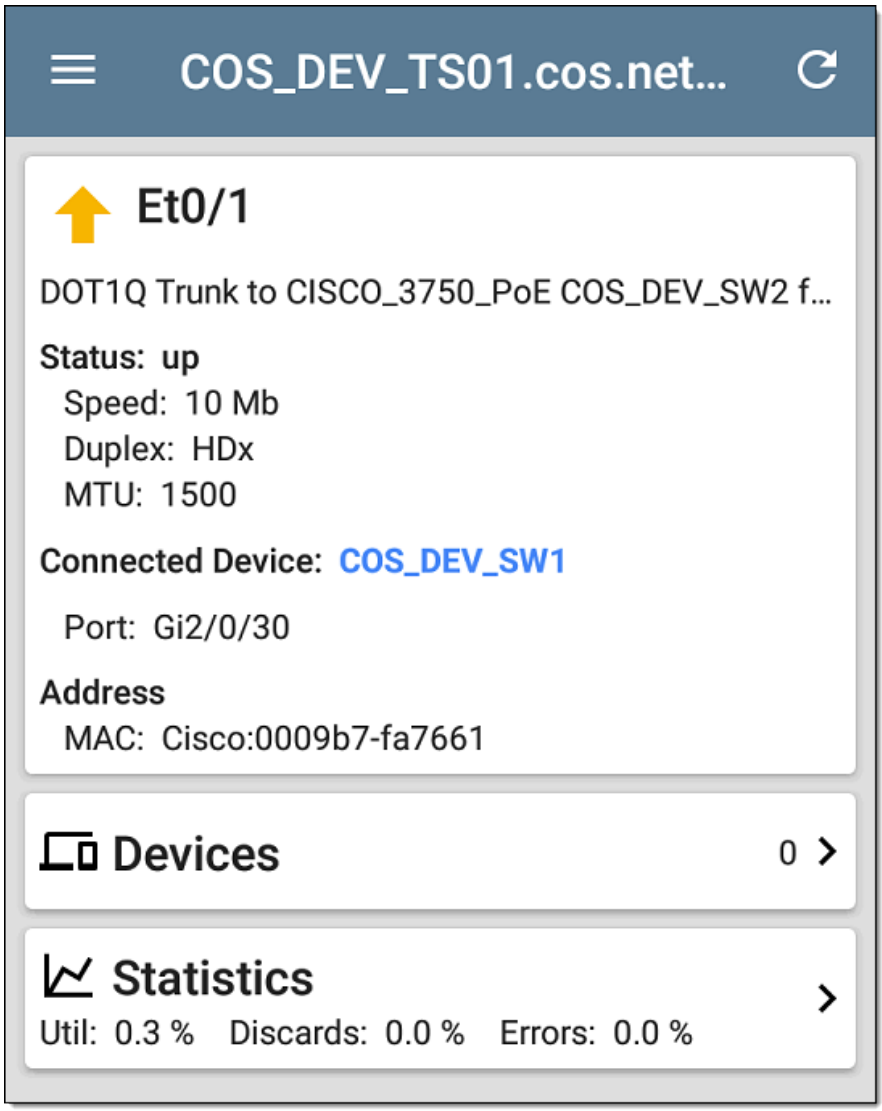
Tap the card to view the list of Interfaces.



Like other Discovery list screens, the Interfaces list provides a number of Sort options, and the selected sort option affects the type of information displayed. The image above shows Interfaces sorted by Status (up or down). The image below shows Interfaces sorted by MAC Address, so each Interface's MAC address is displayed.



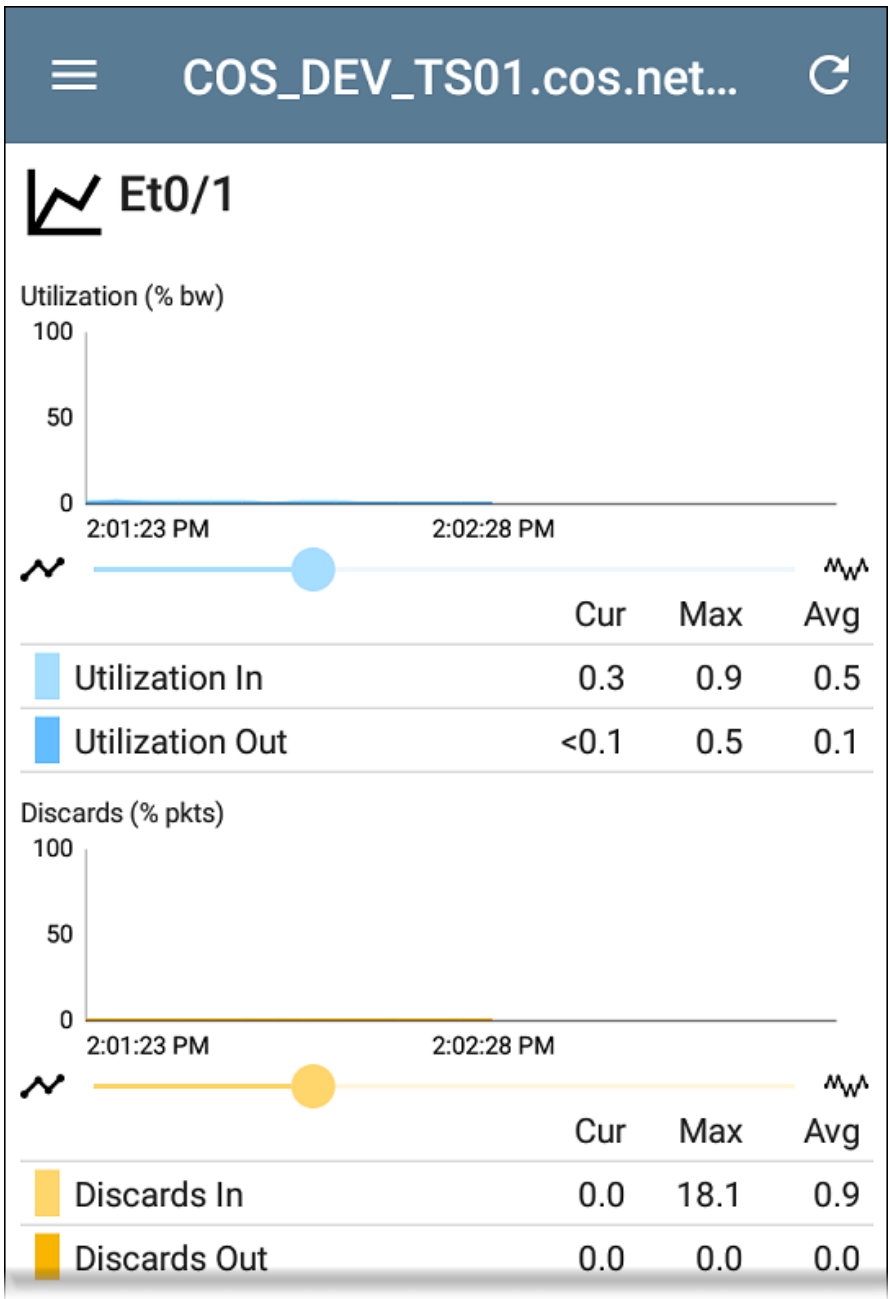
Tap an Interface row to open a new Discovery Details screen for that Interface.



The Interface Details screen contains a description of the interface and information about its Status, Connected Device and Port, and Address.

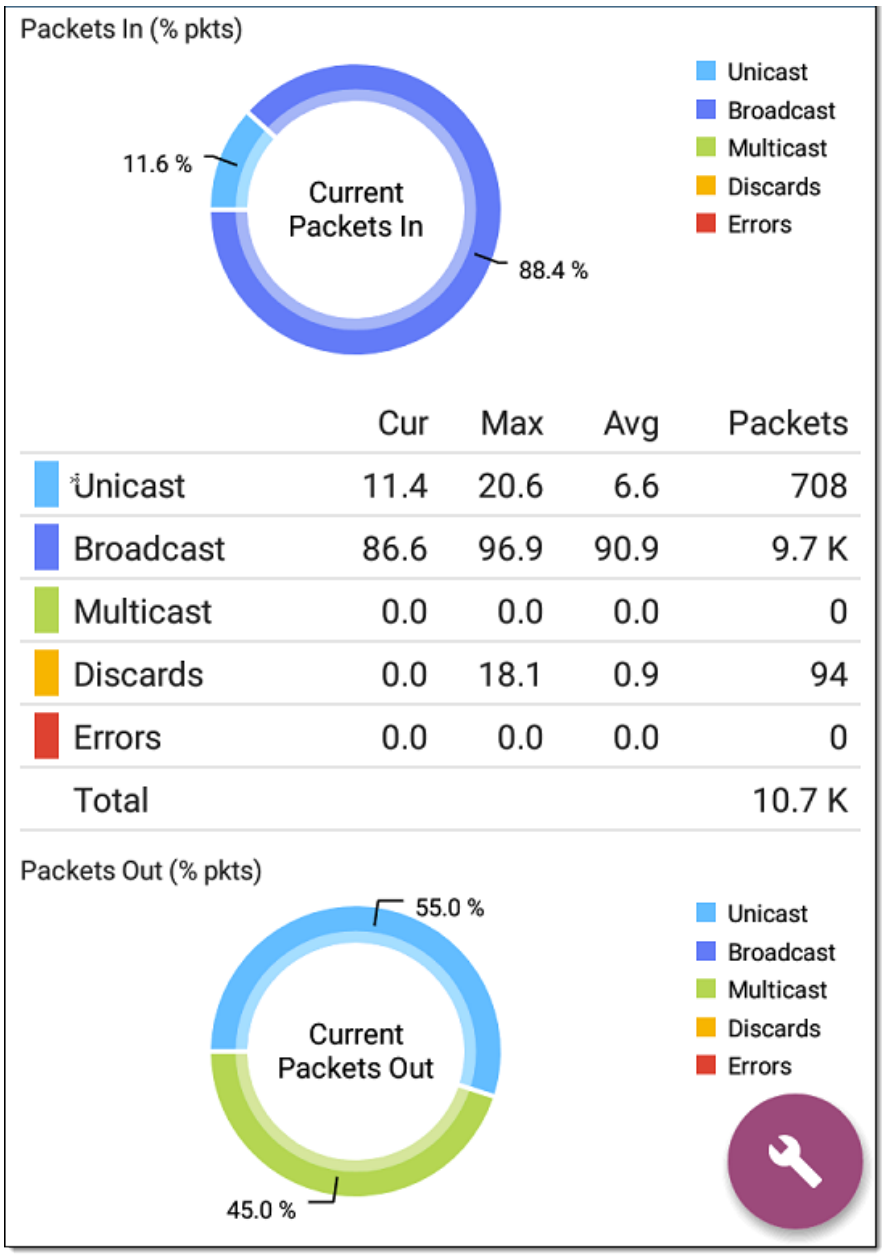
MTU: Maximum Transmission Unit, the maximum packet frame size configured on the interface port

From this screen, you can tap the lower cards to review any discovery **VLANs** and **Devices** for the Interface as well as graphs of the Interface **Statistics**.

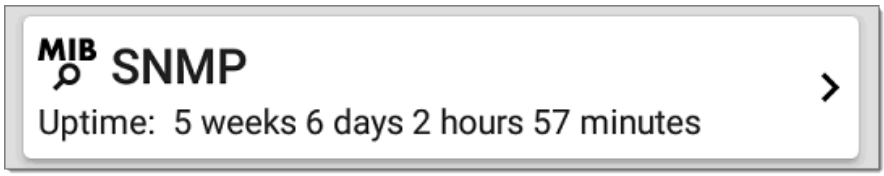


The Statistics screen displays real-time trending graphs of Utilization, Packet Discards, Packet Errors. See the Trending Graphs topic for an overview of the graphs' pan and zoom controls.

Below the trending graphs are pie charts of Packet transfers to and from the Interface.



SNMP



This card shows SNMP Uptime. Tap the card for additional details.

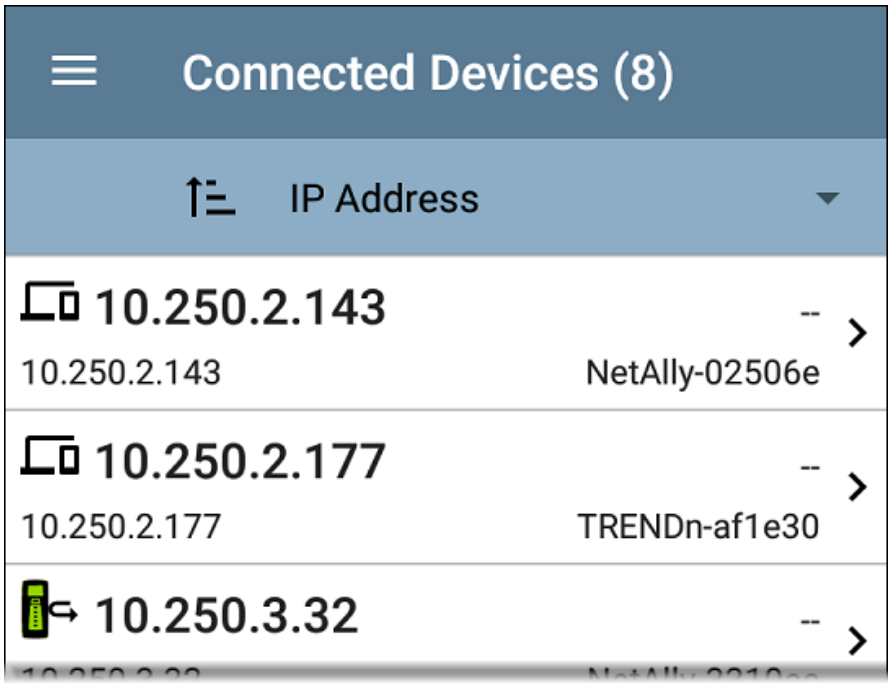
SNMP System Group: These data fields are gathered from the system group and other key device version information.

SNMP: SNMP versions the device supports, Engine ID (for v3), and how the LRAT is currently communicating with the device, along with credentials, including the Community String in use

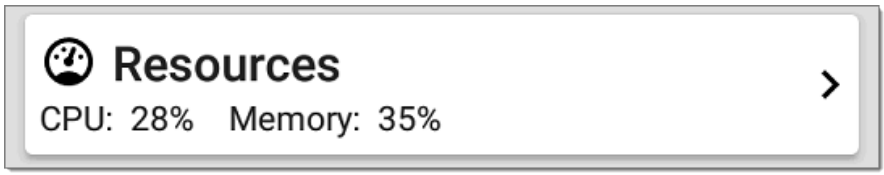
Connected Devices

The Connected Devices card appears on the Details screen for Unknown Switches. While the LRAT may be unable to directly identify the connected switch, the devices connected to it provide clues about where the switch is operating.

The Connected Devices card shows the number of discovered devices that are connected to the Unknown Switch. Tapping the card opens a Discovery list screen with the connected devices.

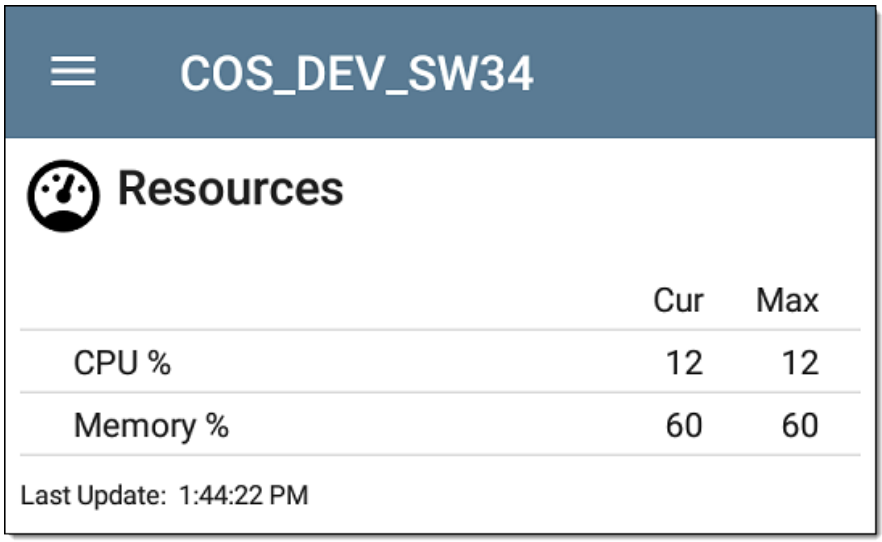


Resources



The Resources card shows the percentages of CPU, memory, and storage usage on the device. This information is gathered via SNMP.

Tap the card to view current and maximum resource utilization measurements.



By default, LRAT displays a **Warning** condition if CPU, Memory, or Storage utilization is above 90%. You can adjust problem detection and thresholds in the Problem Settings accessed from the Discovery navigation drawer.

Discovery App Floating Action Menu

The floating action button (FAB) on Details screens offers additional actions depending on the device type and connection available.

Opening other NetAlly apps, such as from a Details screen auto-populates the new app with the device's name and/or address. In this way, the Discovery app provides a helpful shortcut

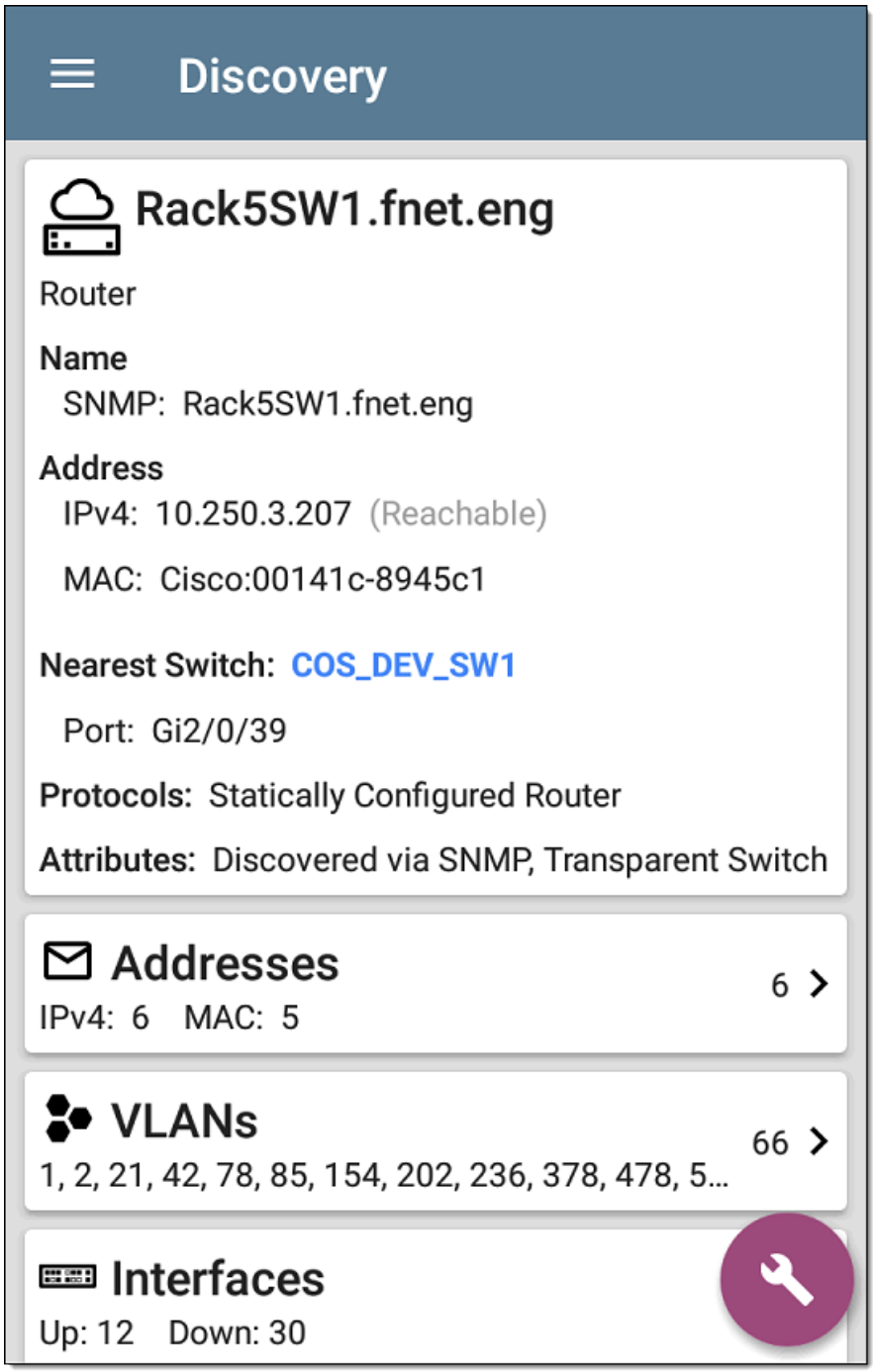
and avoids making you retype the target addresses or hostnames in other testing apps.

- Tap **TCP Port Scan** to open the TCP Port Scan screen in the Discovery app.
- Tap **Add Test Target** to create a new AutoTest target matching the currently selected device. A dialog first displays to select the test type, then the AutoTest app opens, displaying the newly added target's settings. You can then further customize the target.
- For devices with a MAC address, tap **Name** and **Authorization** to open a dialog that lets you assign a custom user name and Authorization status.
- Tap **More** to open a secondary list of floating action buttons:
  - Tap **Telnet** or **SSH** to open the JuiceSSH app.
  - Tap **Back** to return to the primary FAB list.

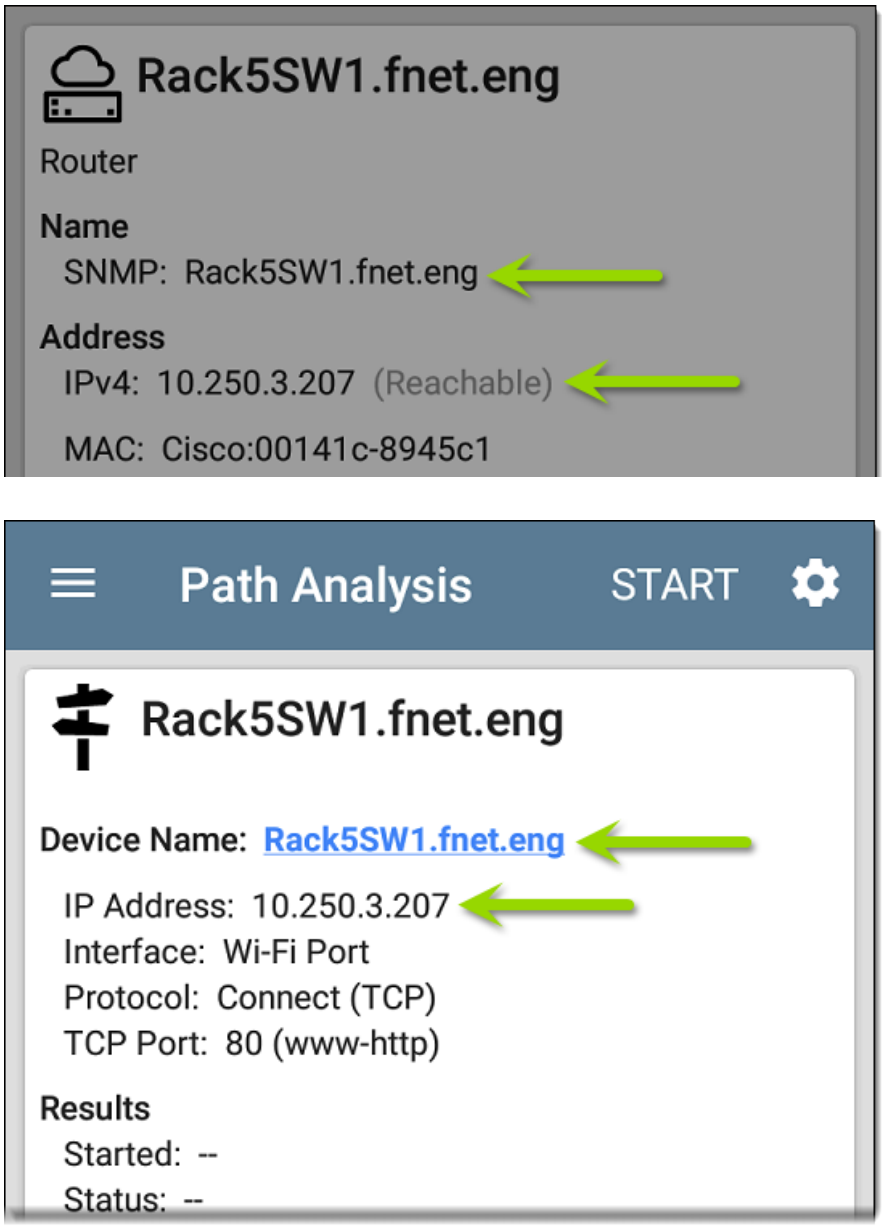
Auto-Populating Device Addresses

When another app is opened from the FAB, the default address and name shown on the Top Details Card are the targets populated.

For example, the Router shown in the Details screen below has multiple IPv4 and MAC addresses (which can be viewed by tapping the Addresses card).



When you open the FAB and select a different app, such as Path Analysis, only the address and name listed at the top of the Details screen are populated in the Path Analysis app.



To open another screen or app with a different address, open the Addresses card, and select another address to view its Details screen.

Back to Title and Contents

Device Types

The Discovery app lists and analyzes the types of devices explained in this section. Different data may be available to the LRAT depending on the device type, how it was discovered, and your configured settings.

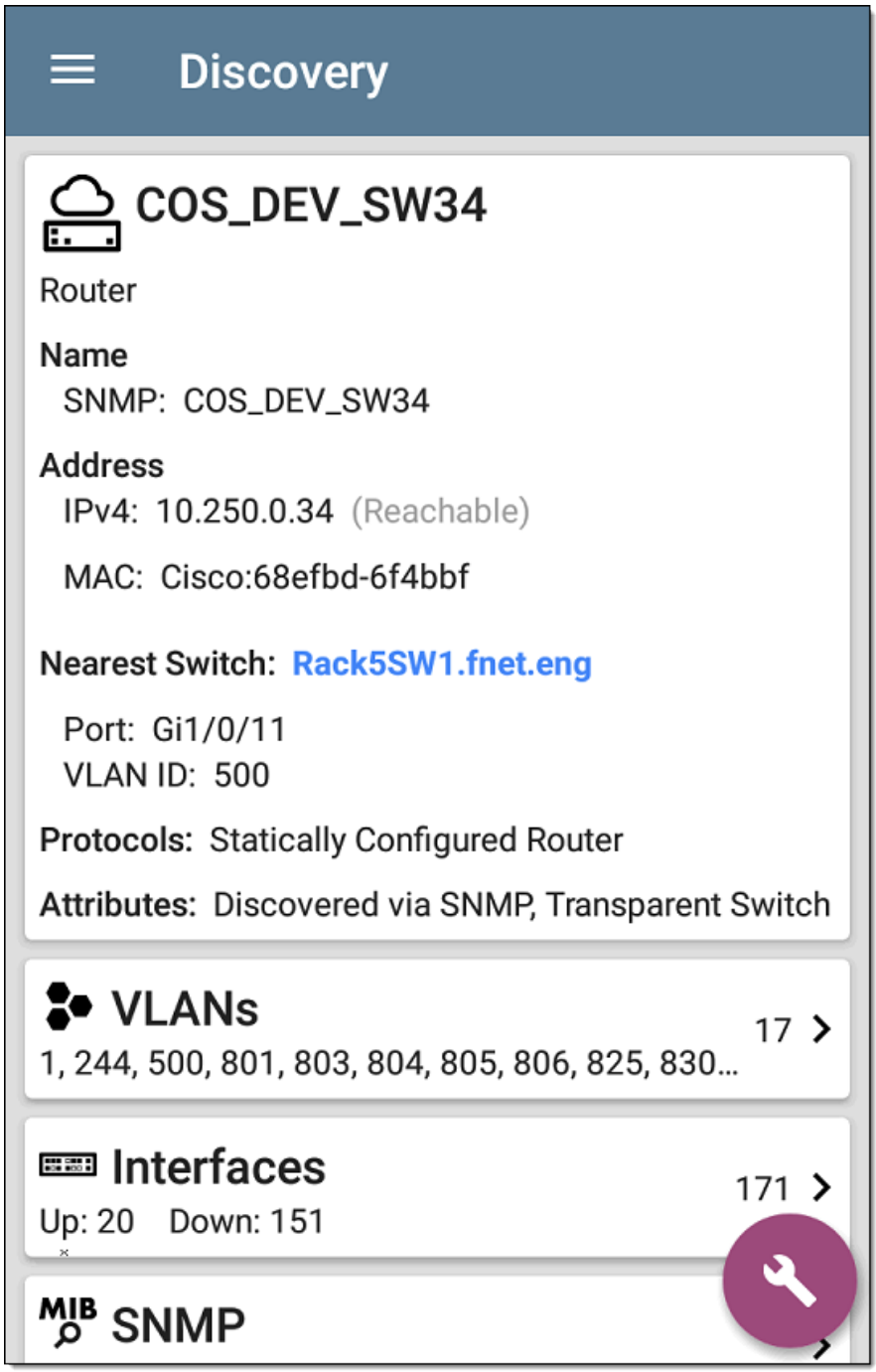
See Discovery Settings for SNMP Configuration and Devices Discovered Through Other Devices options.

For descriptions of the different Details cards and screens, see Discovery Details.

The images in the rest of this section show examples of data that Discovery may display for each device type.

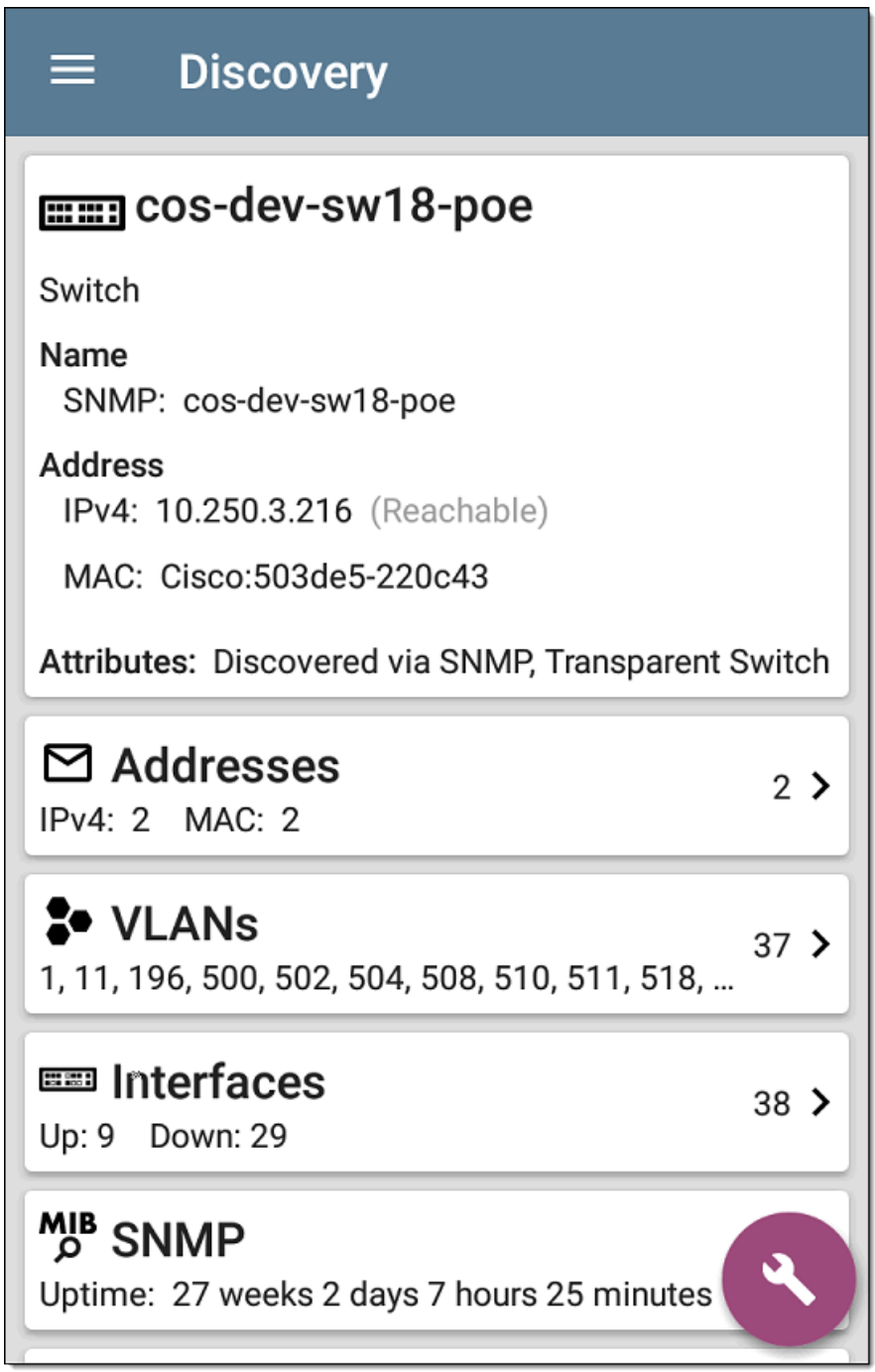
Routers

LRAT discovers IP routers by monitoring traffic and querying hosts.



Switches

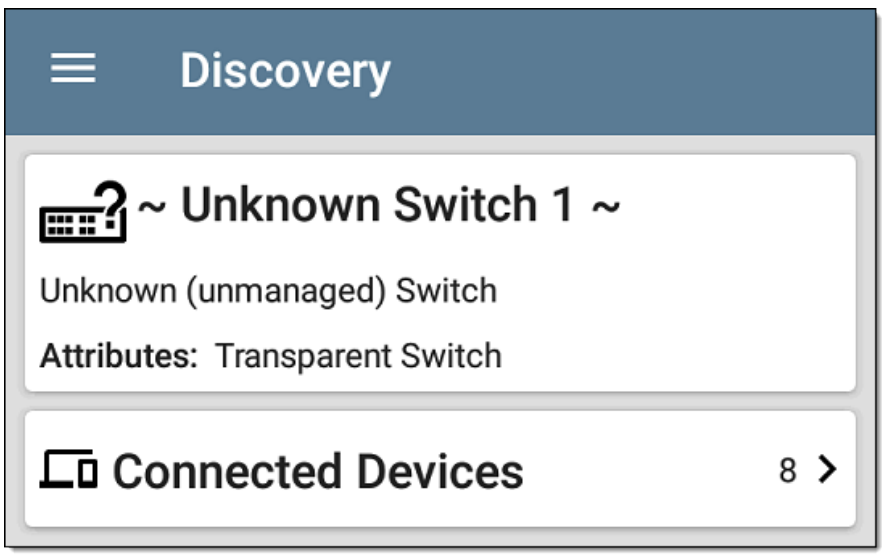
Switches are also discovered by monitoring traffic and querying hosts.



Unknown Switches

Unknown switches are detected indirectly by analyzing traffic going through surrounding switches. The LRAT cannot identify the switch, but it can sense where a switch is active on the network via the device MAC addresses in that space.

The LRAT numbers the switches as they are discovered. (These numbers may change each time the discovery process runs.)



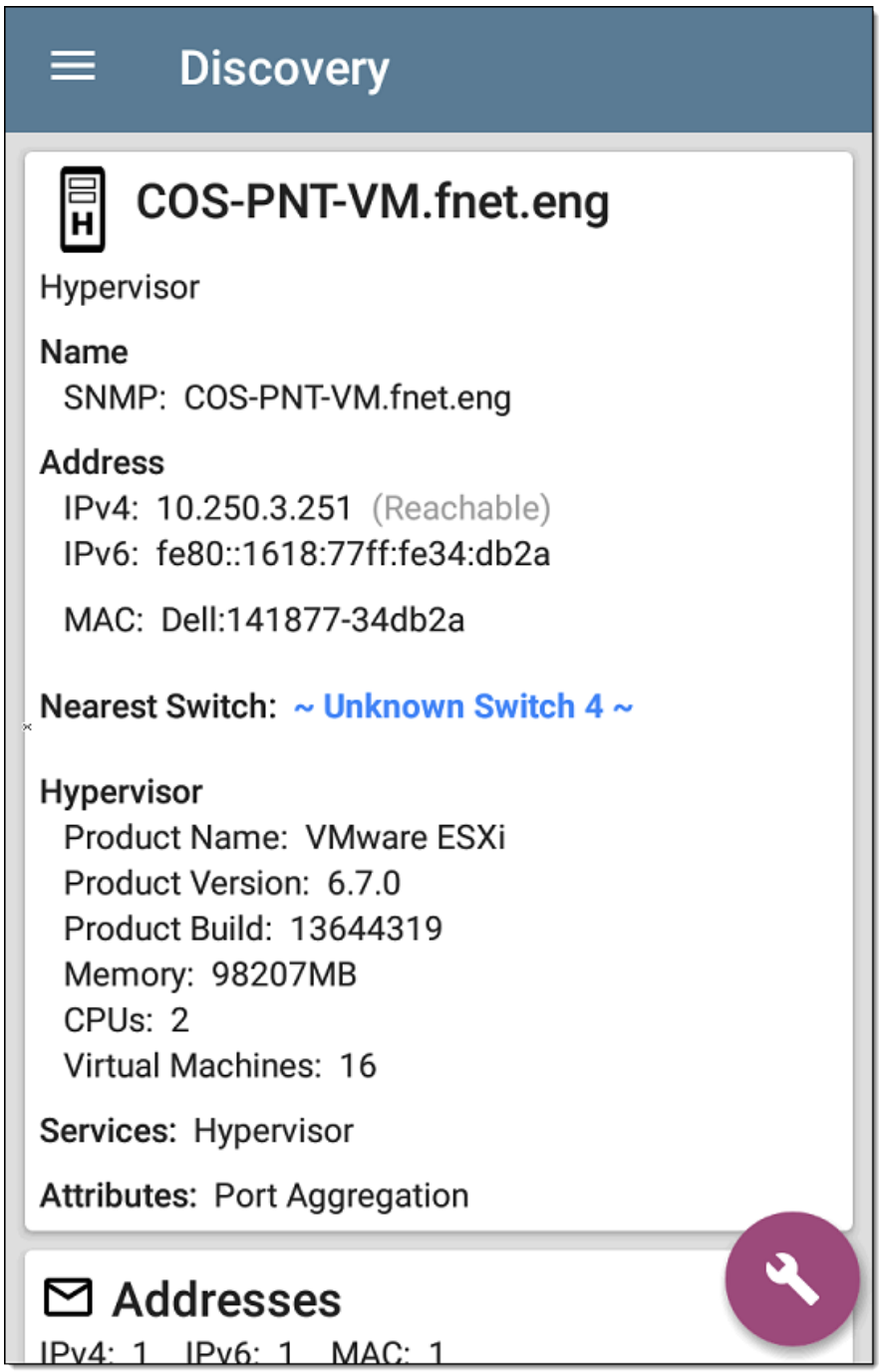
The Unknown Switches Details screen shows the number of devices connected to the switch. Tap the Connected Devices card to view the connected devices, which may provide clues about the location of the unknown switch.

Network Servers

Network servers include NetBIOS, DHCP, and DNS servers.

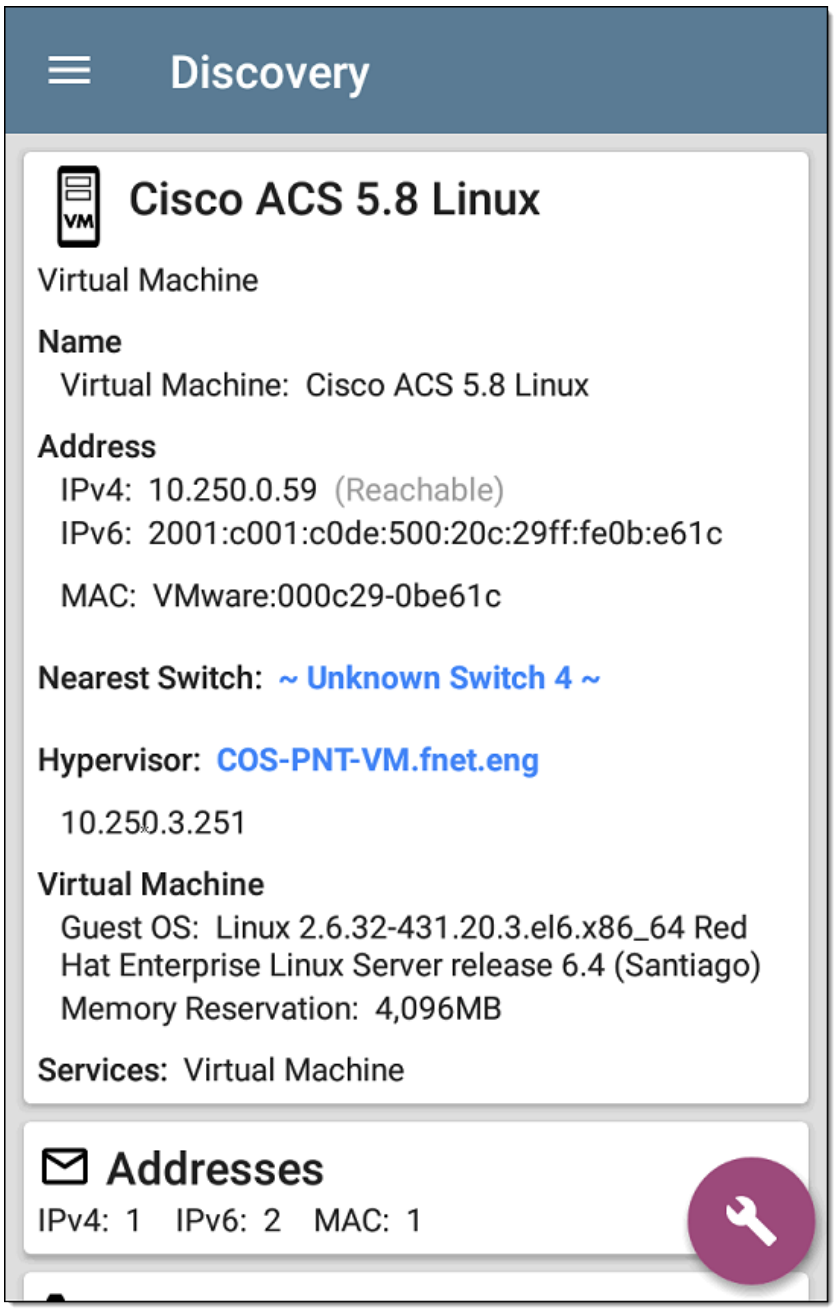
Hypervisors

VMware hypervisors are discovered via SNMP. The hypervisor's SNMP agent must be enabled for the LRAT to discover it and classify it as a hypervisor.



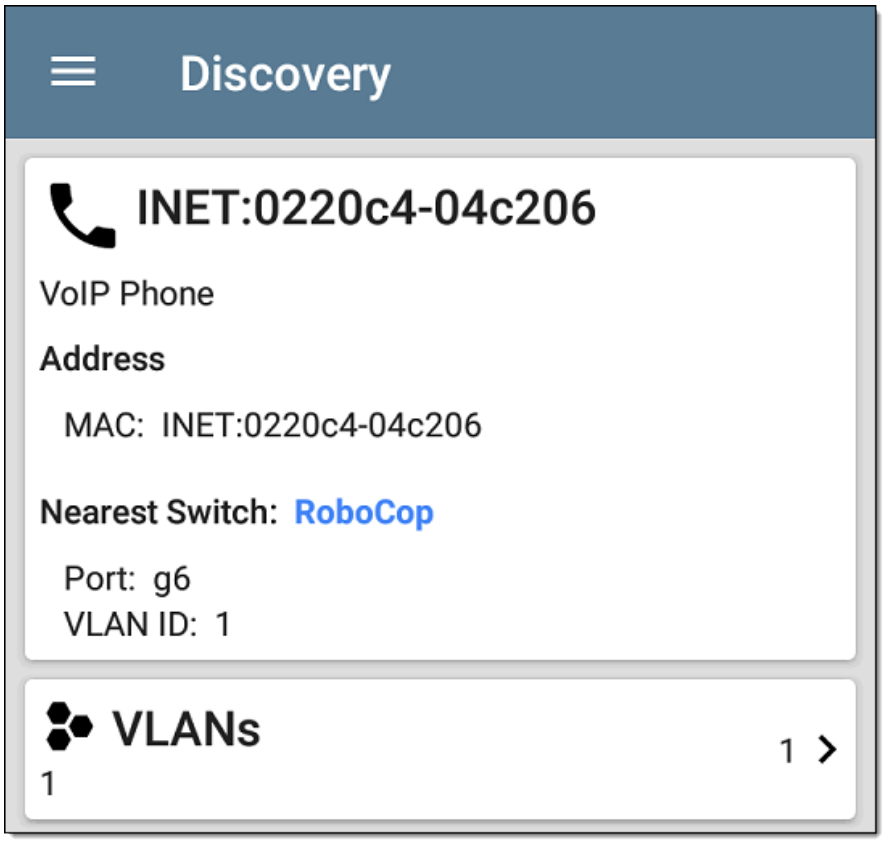
Virtual Machines

VMware virtual machines are discovered from VMware client table in SNMP-enabled VMware hypervisors. Devices are also classified as Virtual Machines if they have a VMware MAC.



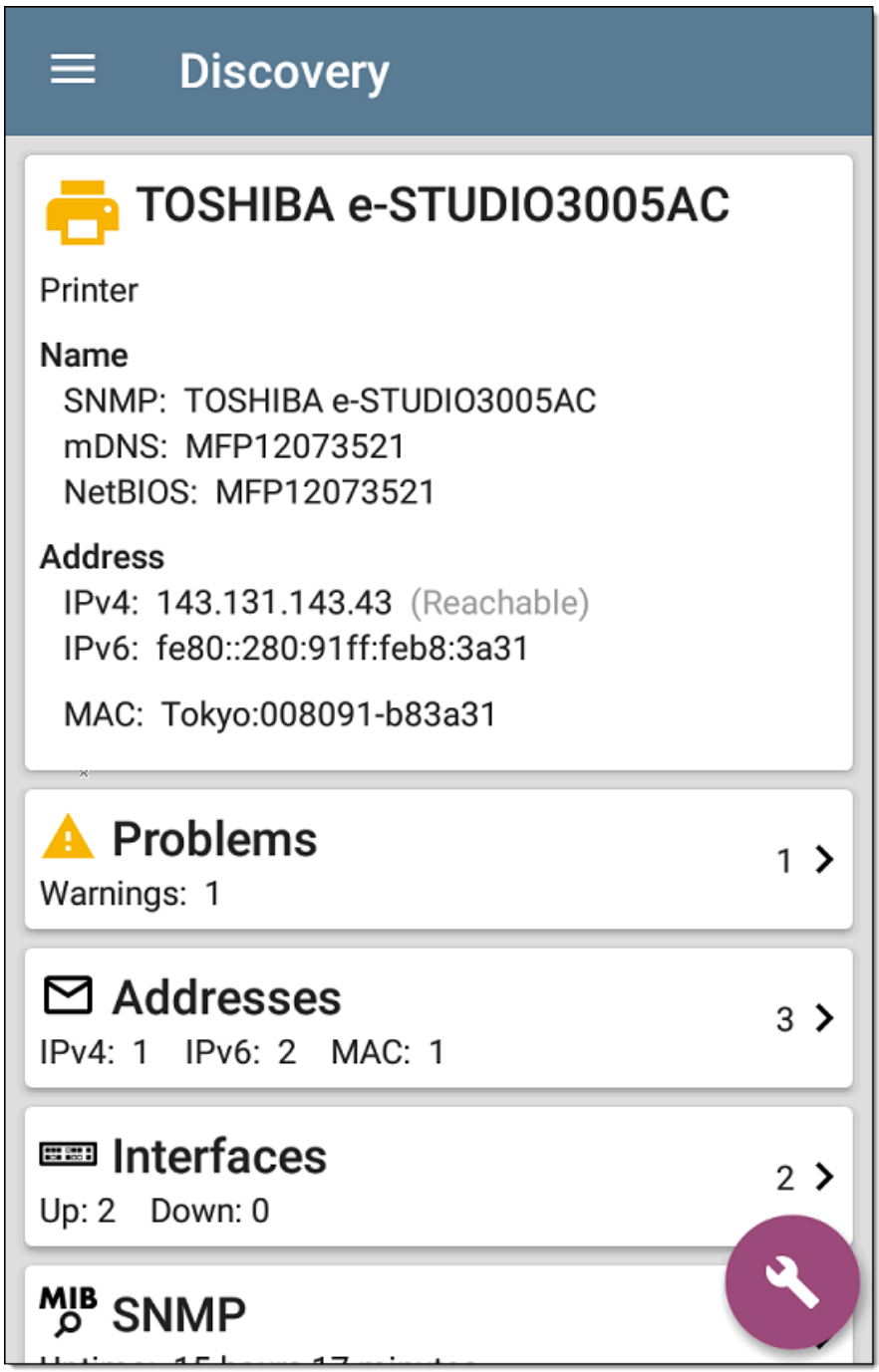
VoIP Phones

VoIP discovery provides visibility into the VoIP and layer 2/3 configuration of the network.



Printers

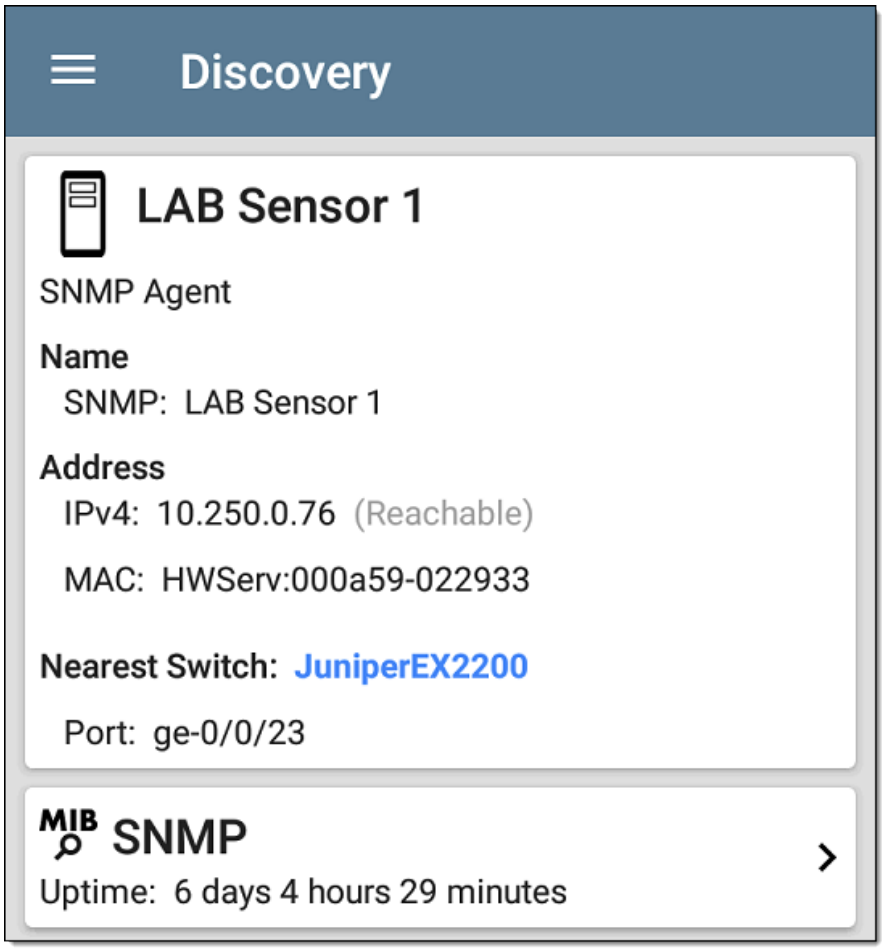
The LRAT identifies IP printers via the SNMP Printer MIB and IPX printers via diagnostic requests and queries.



SNMP Agents

SNMP agents are discovered using SNMP queries. See SNMP Configuration.

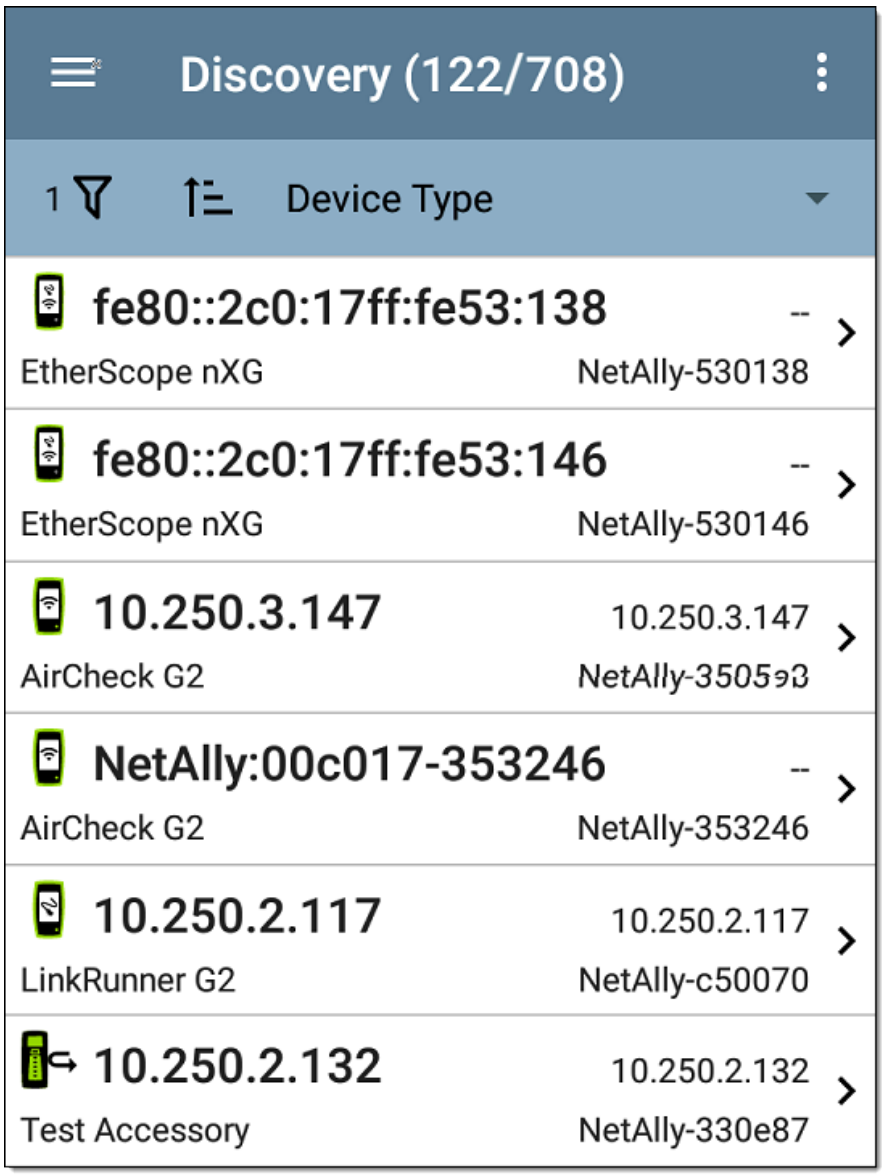
> NOTE: If LRAT cannot discover the SNMP agents on your devices, they may be connected to another subnet, like a management subnet. Solve this issue by adding the subnet to Extended Ranges.



See also SNMP Details.

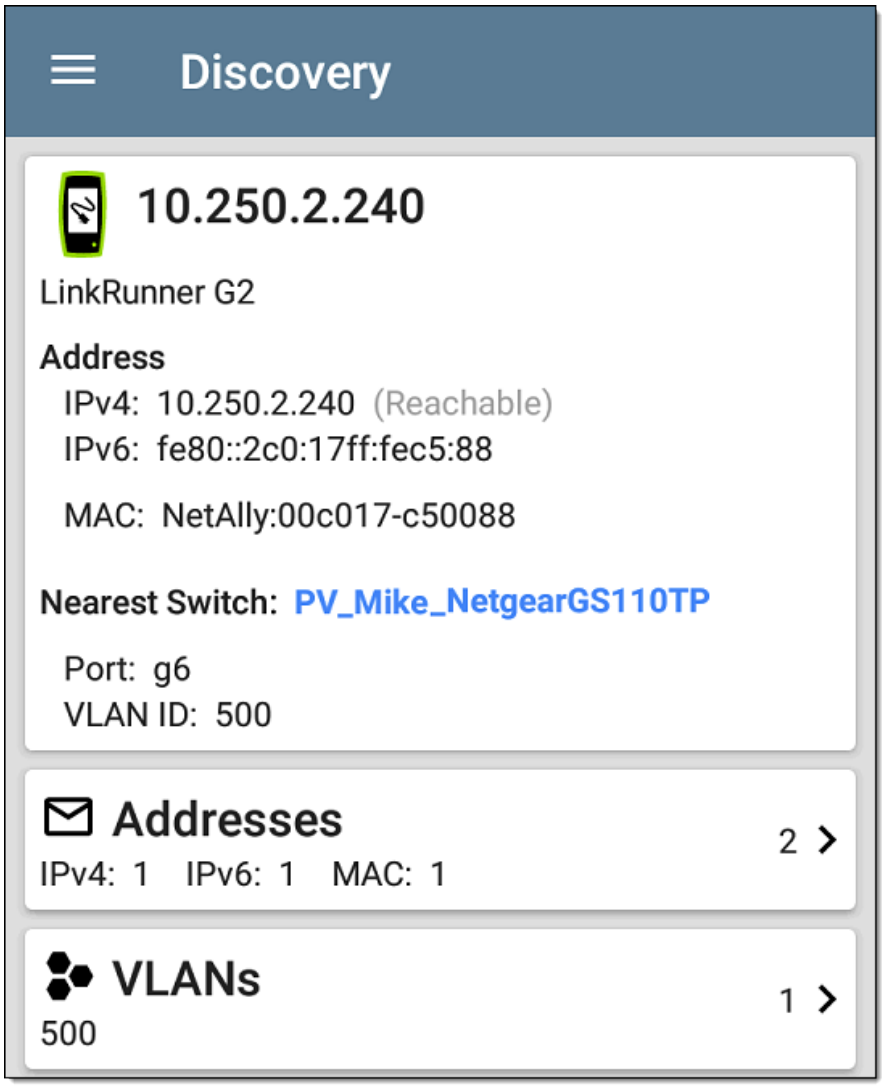
Network Tools

The LRAT can also identify other NetAlly network testers (LRAT, AirCheck G2, OneTouch AT, LinkRunner (AT and G2), and Test Accessory).



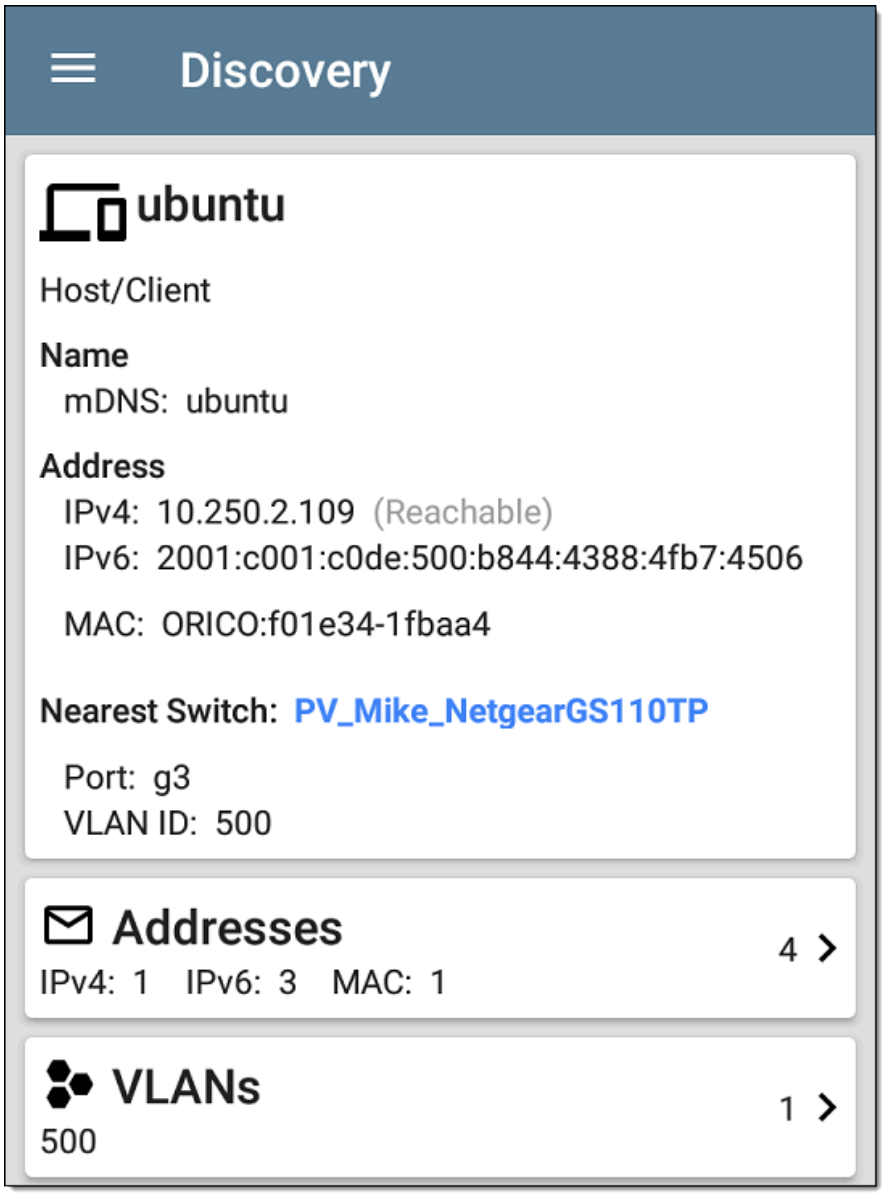
The image above shows several NetAlly tools as they appear in the main Discovery list.

LRAT displays all the information it can gather about each tool on the Details screen.

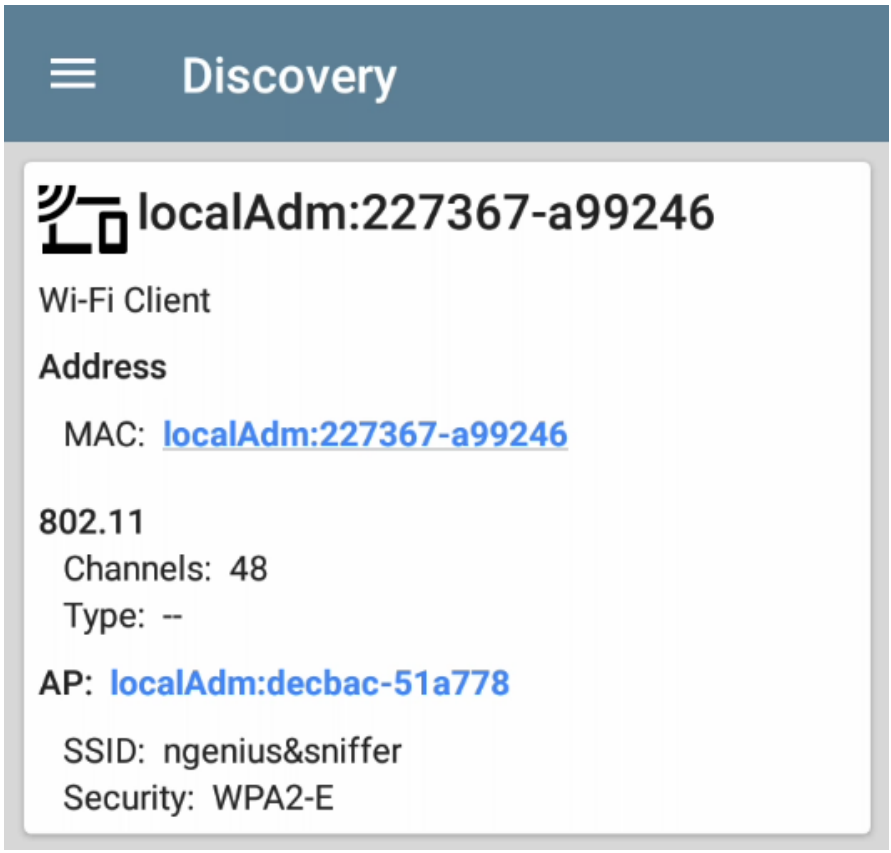


Hosts/Clients

Other hosts and clients are discovered by traffic monitoring and querying. If a host cannot be identified as belonging to one of the other categories (Switch, Router, VoIP device, etc.) then it is categorized as Host/Client.



NOTE: A MAC address that begins with LocalAdm indicates that the address has been locally randomized to prevent unauthorized tracking.



Back to Title and Contents

Device Names and Authorization

Assigning a Name and Authorization to a Device

The Discovery app provide the option to assign a **Name and Authorization** to any discovered device with a MAC Address.

Assigning a User Name and/or Authorization status does not change any of the information on the actual device, only how the device's information displays on the LRAT on which the Name and Authorization are assigned.

You only need to assign a Name and/or Authorization to one MAC address for a device with multiple addresses. Names and Authorizations are saved in the internal authname.txt file and remain set as the unit powers off and on.

This feature allows you to quickly identify your known devices and categorize them with the following statuses:

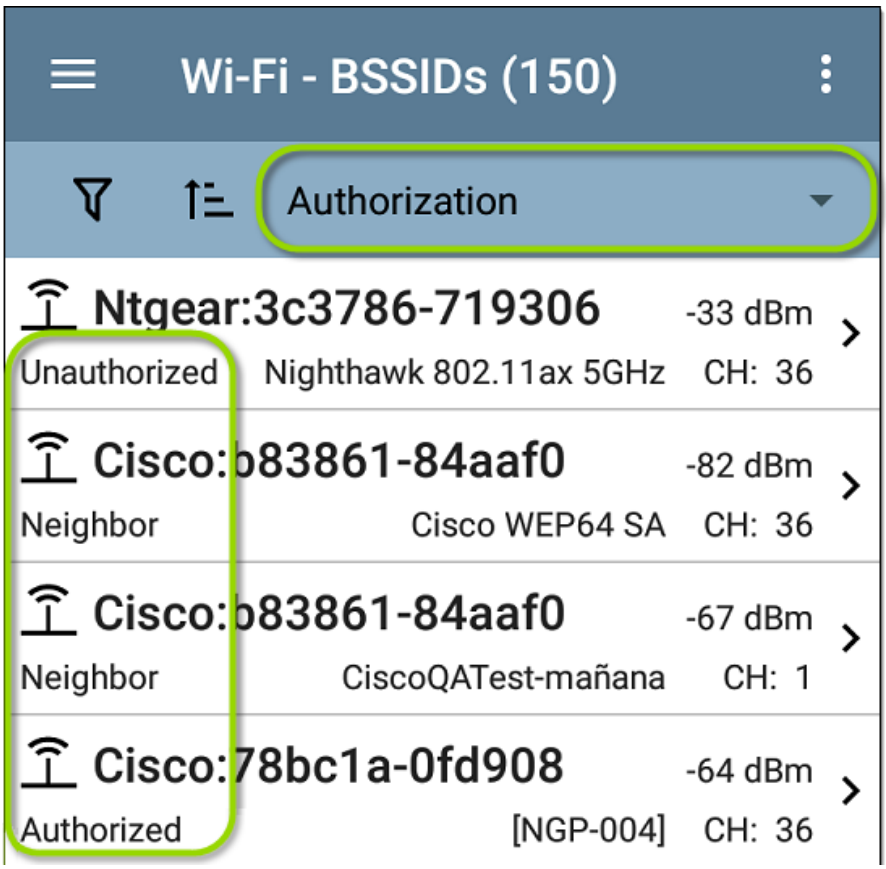
- **Authorized**: For devices approved for use on your network
- **Neighbor**: For devices owned and controlled by neighboring organizations
- **Flagged**: To give visibility to a specific device
- **Unknown**: For devices that have not been identified or classified
- **Unauthorized**: For devices that should not be on the network and may present a security risk
- **Unspecified**: Default unassigned Authorization status

While the Authorization statuses are designed with these intended meanings, you can use them however you like for your purposes.

Once set, the custom User Name is shown in other NetAlly apps wherever device information is displayed. The Authorization is displayed in the Discovery app.

You can sort and filter by the assigned Authorization in the Discovery app. When a list is sorted by Authorization (in normal sort order), the

devices with Authorizations of highest concern appear at the top. The image below shows a list screen sorted this way:



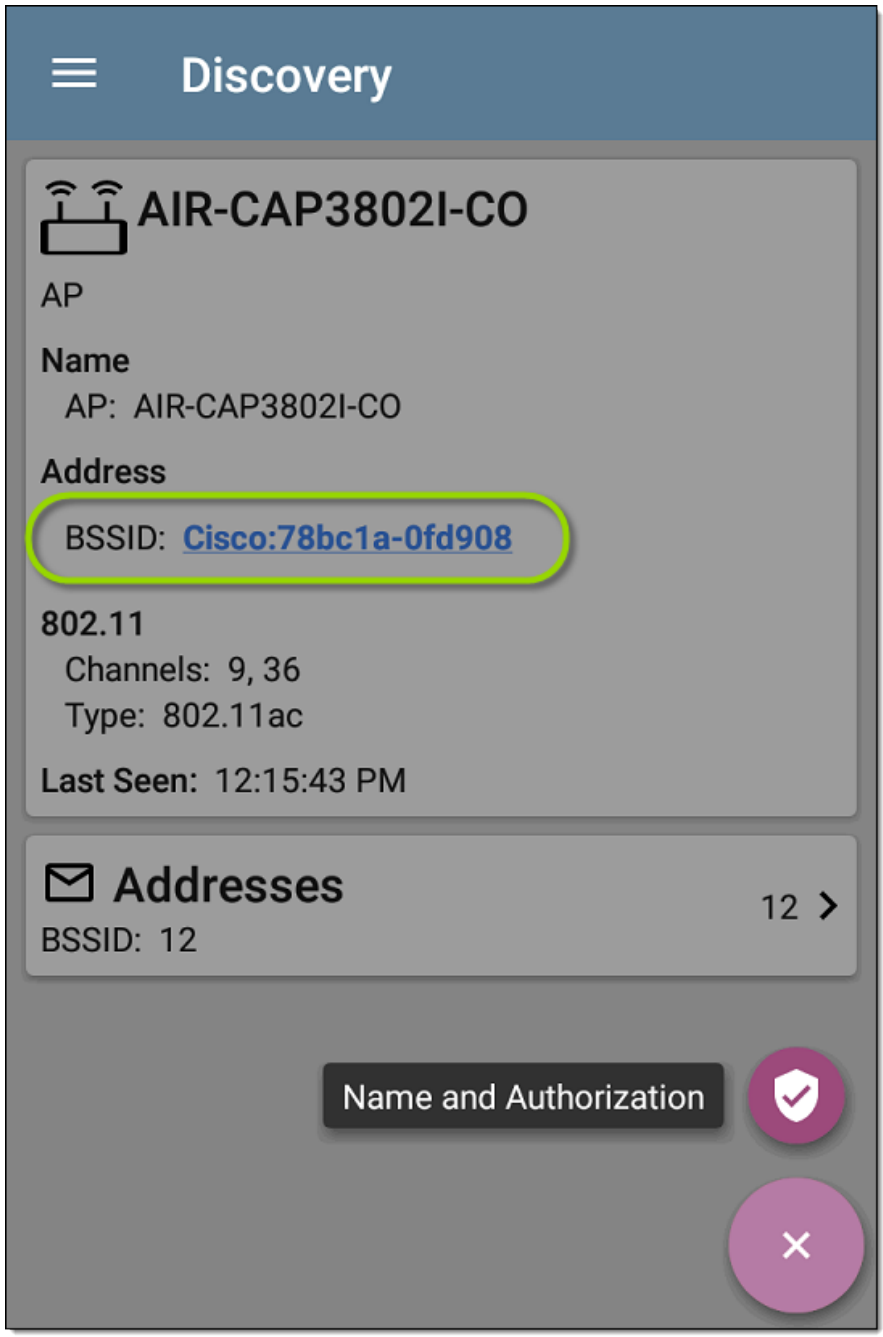
Applying a Name and/or Authorization

Access the **Name and Authorization** function from the floating action menu on a Discovery Details screen.

> NOTE: When applying an Authorization to a device with multiple MAC addresses, the Authorization status is only applied to the

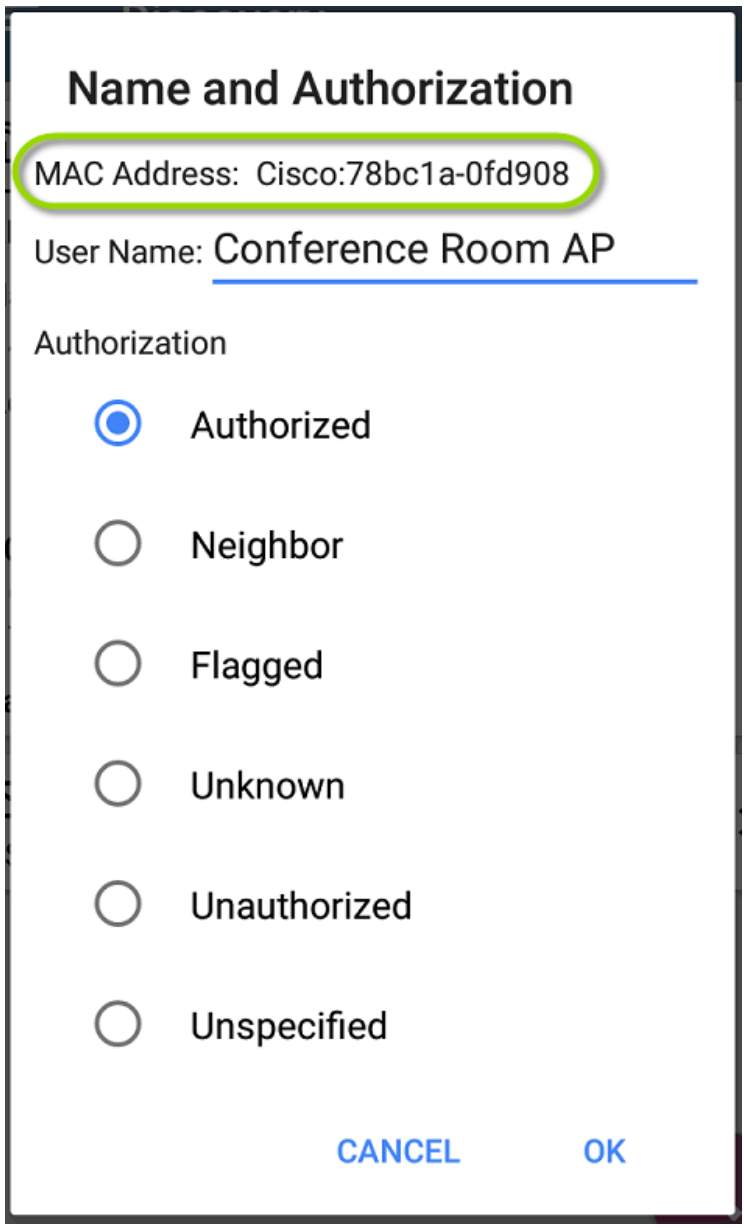
MAC address displayed on the Details screen, as shown in this section.

1. Tap the FAB on a Discovery screen for a device with a discovered MAC.



The example above shows an AP's Details screen in the Discovery app.

2. Select **Name and Authorization** to open the dialog.



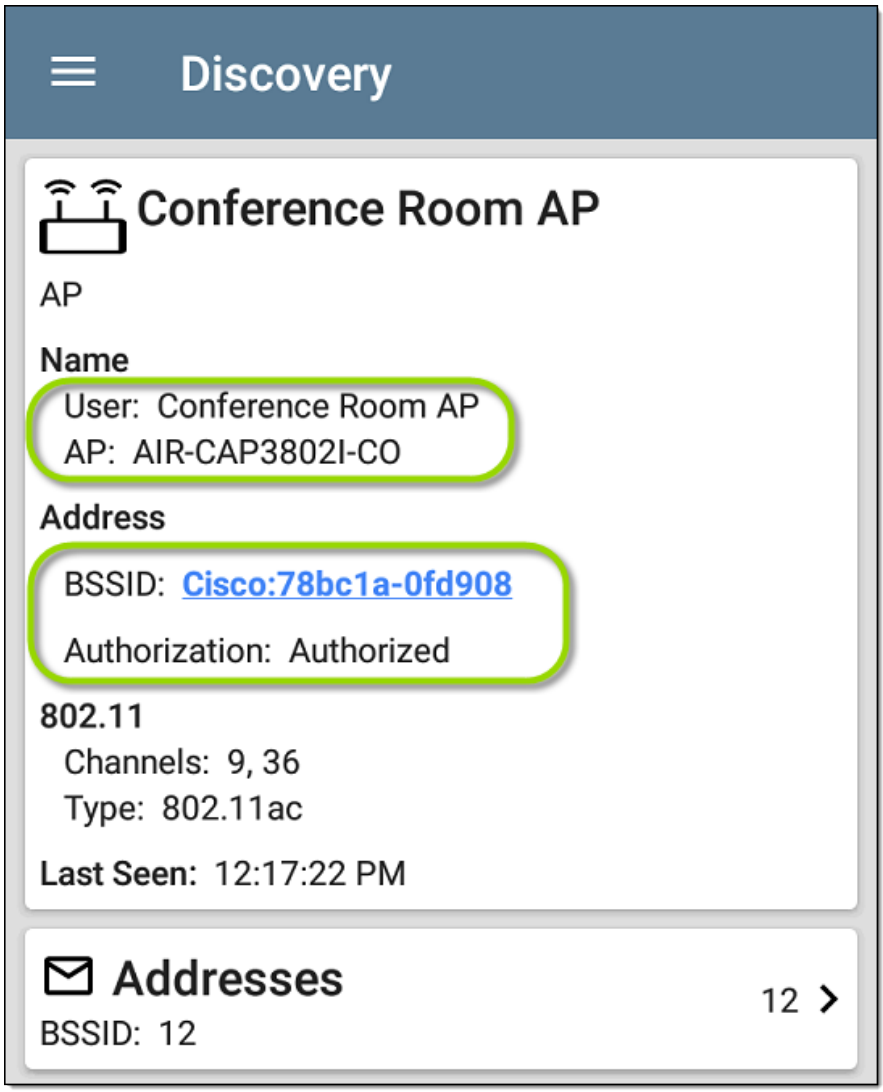
3. In the Name and Authorization dialog, tap the **User Name** field to enter a customized

name, if desired. In the image above, the user has entered the name "Conference Room AP."

NOTE: It is possible to *either* enter a user name or select an Authorization. You do not have to do both.

4. Select the radio button to assign an **Authorization** status as needed.
5. Tap **OK** to apply.

Once applied, the User Name and Authorization are displayed on the Discovery Details screen.

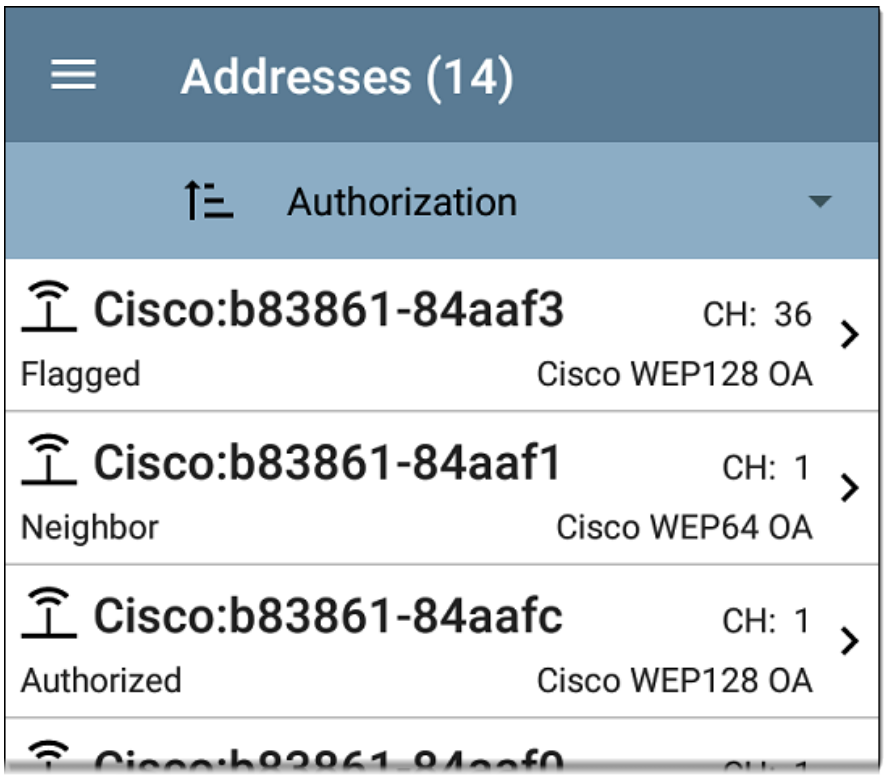


NOTE: If different Authorization statuses are assigned for different MAC addresses on the same device, the Authorization of highest concern appears on the device's Details screens.

Changing or Clearing a User Name or Authorization

Open the Name and Authorization dialog again *for the same MAC address* on a device to reassign or clear the assigned User Name or Authorization. If the Name or Authorization do not update as expected after a few minutes, you may have assigned them to multiple addresses for the same device.

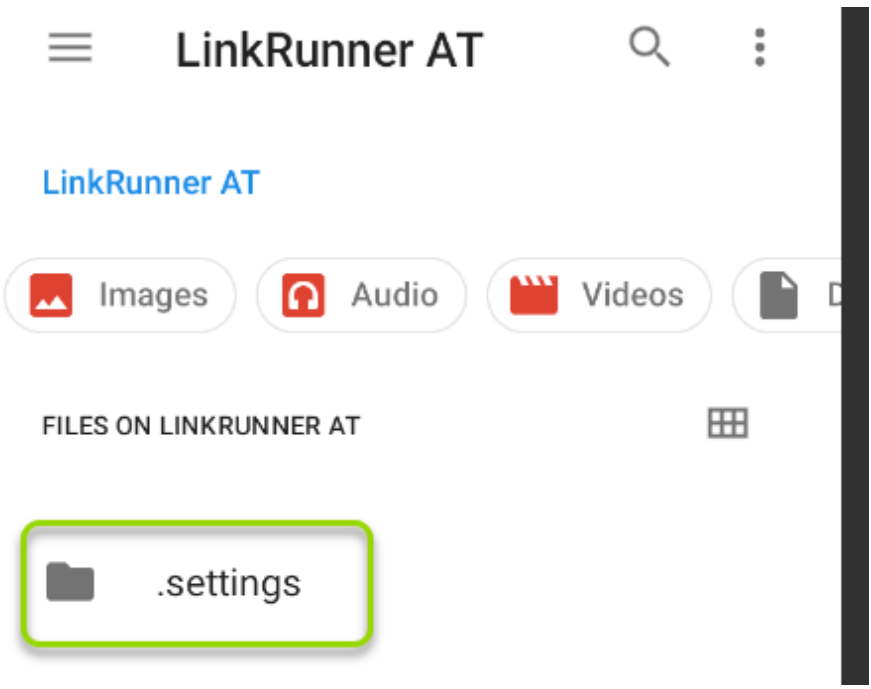
To view all assigned Authorizations for a device, open the Discovery screen for the device and view the Addresses screen. Then, sort by Authorization.



To reset a device's User Name and/or Authorization to the unassigned defaults, open the Name and Authorization dialog, clear the User Name field and leave it blank, and select the **Unspecified** Authorization. Then, tap **OK**.

Revising or Importing authname.txt

Custom Names and Authorizations are stored in the **authname.txt** file in the LRAT's internal storage **.settings** folder, accessible from the Files app.



If desired, you can manually edit this file on the LRAT unit, or you can create a new authname.txt file on a PC and import it onto your unit in the

same file location. (You can also push auth-name.txt files from Link-Live to your test unit.)

> NOTE: Your LRAT 3000-4000 can parse ? wildcard characters in the authname.txt file (although * wildcard characters are not allowed).

The default authname.txt file on your unit contains instructions on how to format your Name and Authorization entries:

- Each line defines one MAC in the format:
  `MAC, [Authorization][, Customized Name]`
- Authorization is case insensitive and can be one of these strings:
  - Authorized
  - Neighbor
  - Flagged
  - Unauthorized
  - Unknown
  - Unspecified (or blank)
- You can substitute a question mark **?** for a MAC digit to match any value for that digit.

A sample authname file could look like this:

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

To edit the authname.txt file on the LRAT, third-party apps, such QuickEdit Text Editor, are available from the NetAllyApp Store ▶️ .

For help importing a file, see the Managing Files topic.

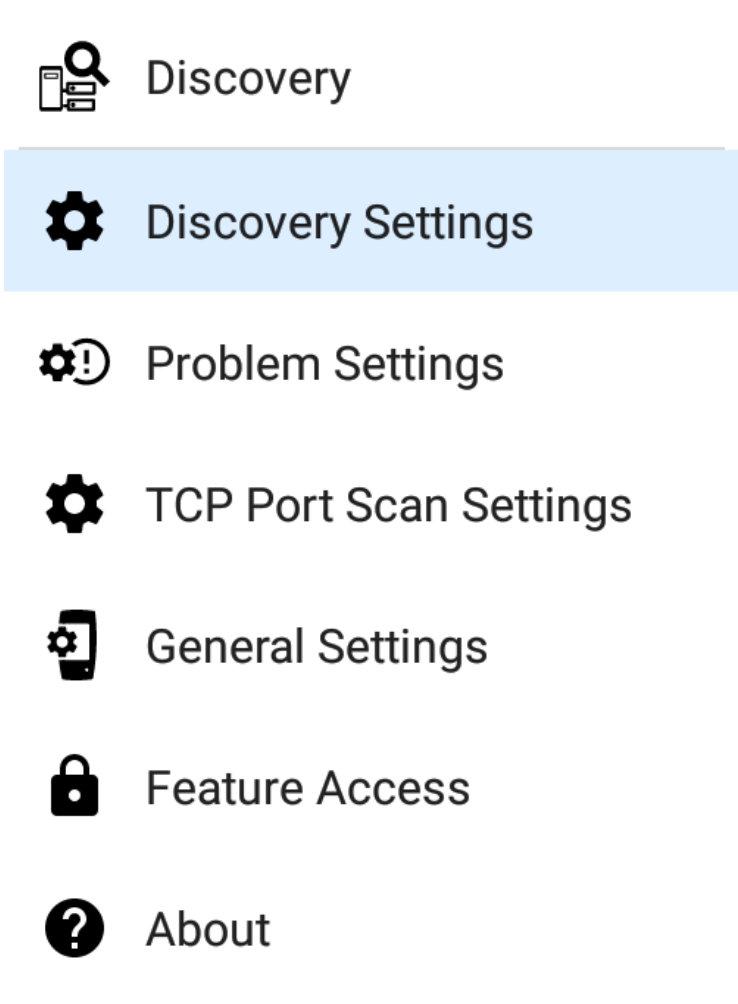
> NOTE: After importing and overriding the authname.txt file, NetAlly recommends Refreshing Discovery in the Discovery app or restarting your unit.

Back to Title and Contents

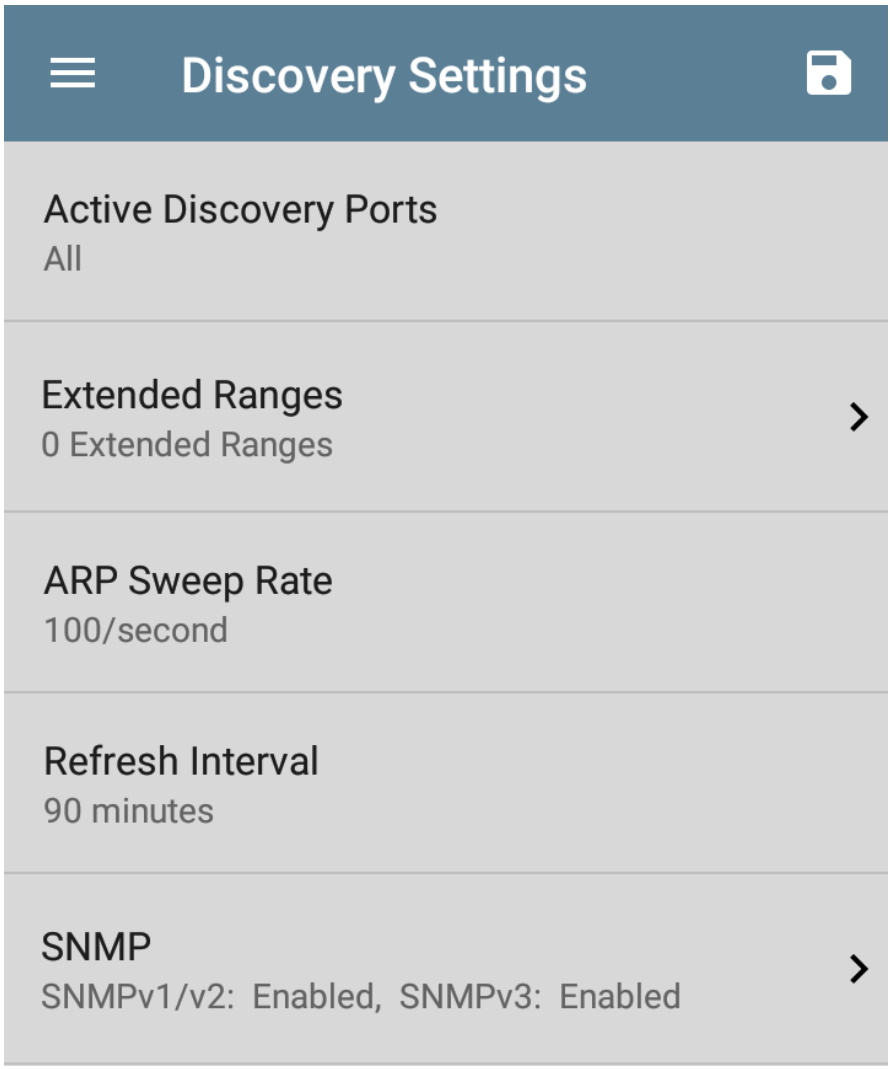
Discovery Settings

Discovery configurations include SNMP settings, Community Strings and the order in which they are used, Credential Sets, Ports, Extended Ranges, and process intervals.

Access the Discovery settings screen by sliding out the left-side navigation drawer or tapping the menu icon, and selecting **Discovery Settings**.



(Tap here to skip to Problem Settings, TCP Port Scan, or back to General Settings.)



To adjust Discovery Settings:

1. On the **Discovery Settings** screen, tap each field described in this topic, as needed, to select or enter your required configuration elements.

2. When you finish configuring, tap the back button  to return to the main Discovery List screen.
3. Then, Refresh Discovery from the action overflow menu  to apply the new configuration.

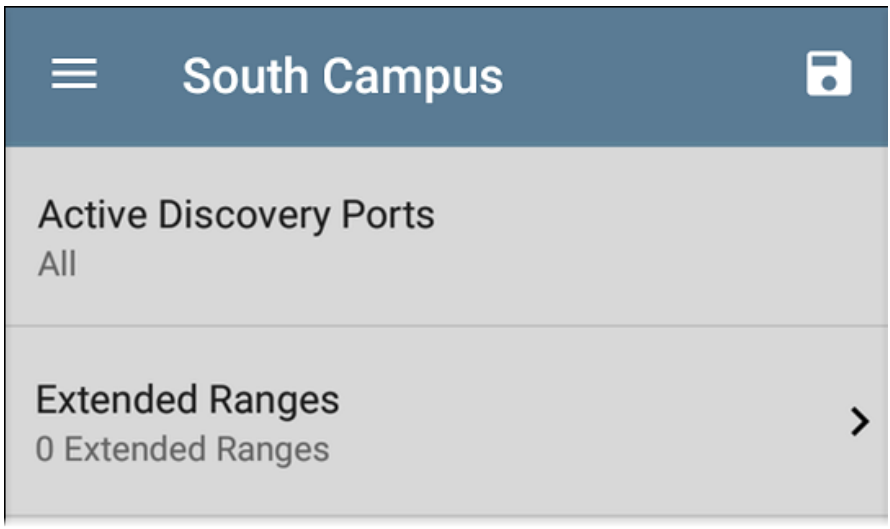
You can load, save, import, and export configured Discovery settings by tapping the save button  on this screen.

- **Load** opens a previously saved Discovery configuration.
- **Save As** saves the current configuration with an existing name or a new custom name.
- **Import**: Import a previously exported settings file.
- **Export Selected** or **Export All**: Create an export file of current settings, and save it to internal or connected external storage.

See Managing Testing App Settings for more instructions.

After you have saved a configuration, the custom name you entered appears in the title of the

Discovery Settings screen. In the image below, a user has saved a custom configuration named "South Campus," which replaces the "Discovery Settings" screen title.



Active Discovery Ports

Tap **Active Discovery Ports** to select which port Discovery uses to gather data. (Discovery uses all of the ports by default. Uncheck them to limit which ports are used.) Discovery runs through the enabled ports only if an active network link is available. See Selecting Ports for explanations of the different ports.

Extended Ranges

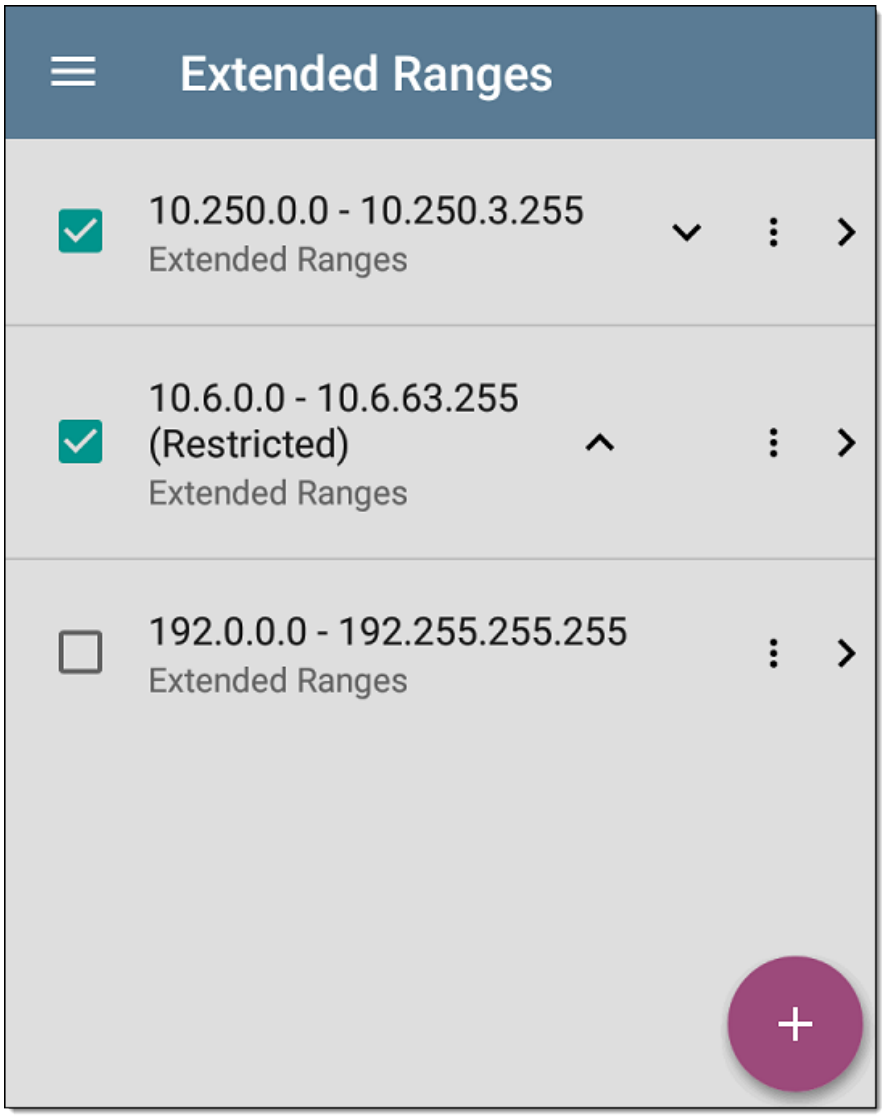
The Extended Ranges screen allows you to enter addresses of non-local subnets on which you want the Discovery process to run. Discovery sweeps all of the enabled Extended Ranges for devices, whether directly connected or off-net. The LRAT performs Ping sweeps on subnets that are not directly connected and ARP sweeps on connected subnets.

When the SNMP agents are on a subnet that is separate from the hosts (PC's and servers) subnet, additional networks must be configured for discovery:

- The network address of the remote subnet you want to discover, meaning the host (PC and server) network.
- The network address of the switch and router SNMP agents in the remote subnet, e.g. a management subnet.

Configure both SNMP **Credential Sets** and **Extended Ranges** to ensure that the LRAT always discovers management subnets, regardless of your network port connections.

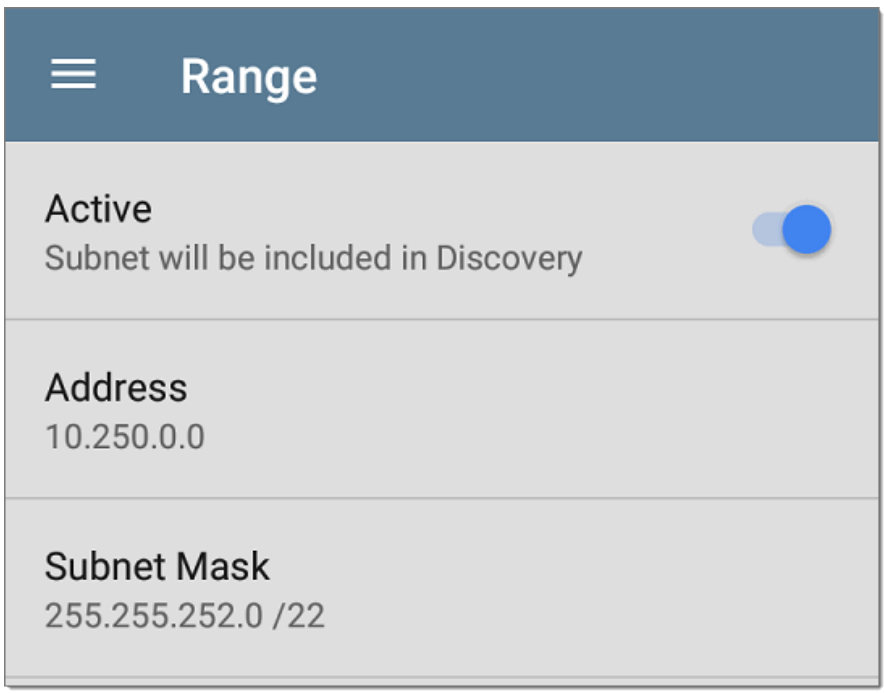
Tap the field to open the Extended Ranges list screen.



- Check or uncheck the boxes to include or exclude an extended range from the current Discovery configuration. Unchecked Extended Ranges do not affect the default Discovery behavior in the current

configuration, but they may be used in other Discovery configurations (like Community Strings and Credentials).

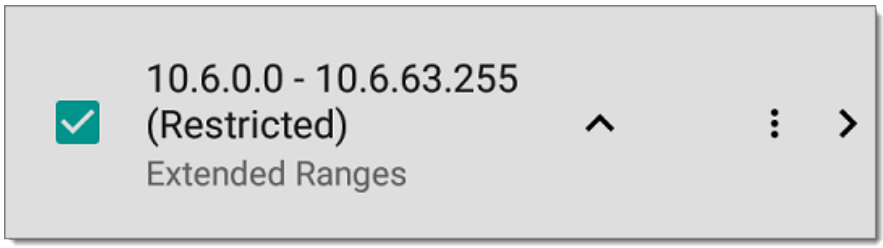
- Tap any Extended Range's row to edit its address and subnet.
- Tap the FAB + to add new extended ranges.



Active vs. Restricted Subnets

For each configured Extended Range, you can tap the toggle button to switch from **Active** to **Restricted**. Discovery is performed on Active Ranges. Setting a Range to **Restricted** disables the discovery process on that network or subnet,

meaning the LRAT will *not* communicate with devices within the restricted range.



- Restricted Ranges take precedence regardless of the order in which they are listed on the Extended Ranges screen.
- You can Restrict a part of a configured Active Extended Range.
- You can also restrict a single device, whether it is part of an Active Range or not. To enter a single device that you do not want discovered, enter its IP address in the Address field, and set the Subnet Mask field to 255.255.255.255.

Address

Tap the **Address** field to enter or select an IP address range.

Tap the drop-down menu to select a previously Discovered Subnet. The Address field is automatically populated with your selection.

Subnet Mask

Tap this field to select a subnet mask. If you select an already Discovered Subnet, the Subnet Mask is also pre-populated.

ARP Sweep Rate

Tap the ARP Sweep Rate field to select a rate between 5 and 100 ARP requests per second.

This setting can prevent the LRAT from shutting down ports that sense too many ARPs being sent.

Refresh Interval

This setting controls the time between runs of the Discovery process. By default, Discovery runs every 90 minutes. Tap the **Refresh Interval** field to select a different interval, up to 8 hours.

The **Manual** option turns off regular automatic Discovery, and the process refreshes only if you

select **Refresh Discovery** from the main Discovery list screen.

SNMP Configuration

The MIB (Management Information Base) of SNMP managed devices contains information such as device configuration, interface configuration and statistics, SNMP tables (like host resource and route tables) and VLAN details. Through the Discovery process, the LRAT interrogates MIBs to determine the device type, ports, connected subnets, and other data.

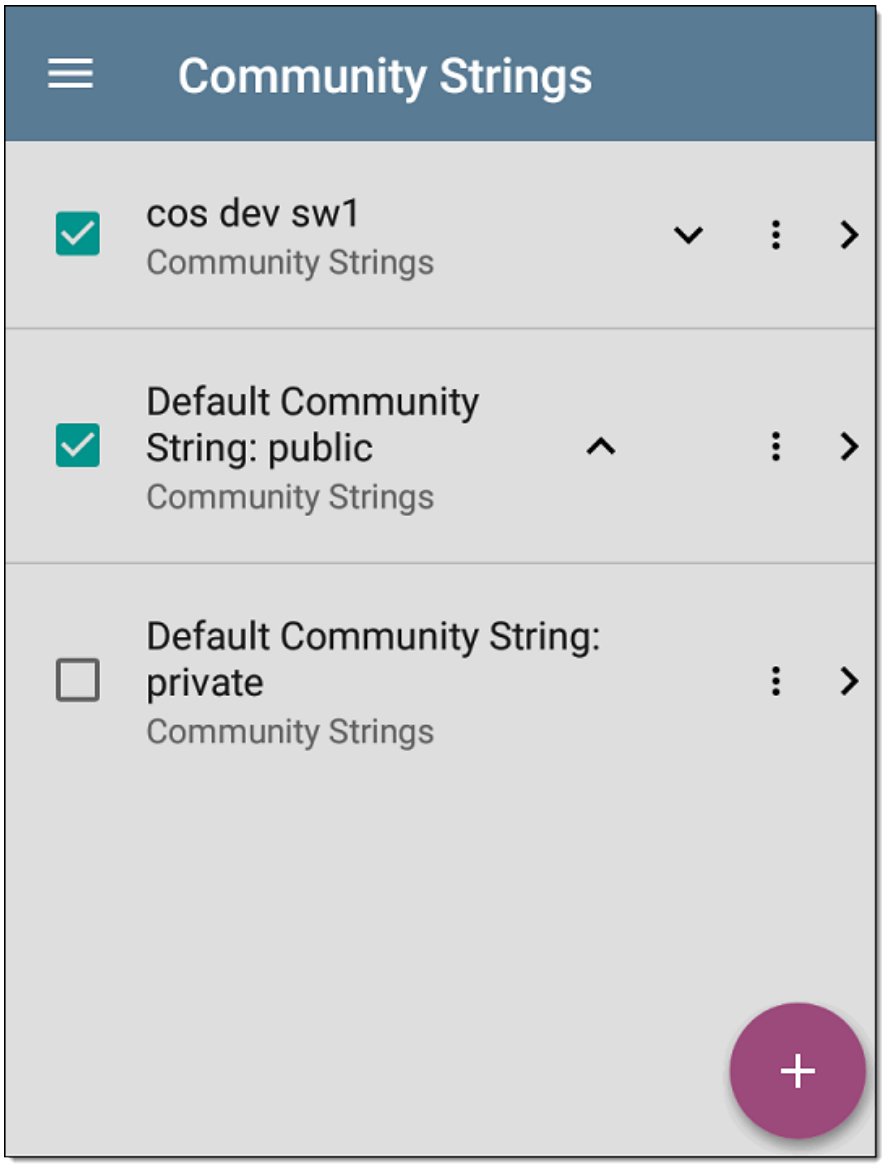
SNMP credentials are required to communicate with the SNMP agents on your interconnect devices, such as switches and routers. The Discovery Settings allow you to enter the SNMP community strings and credential sets the LRAT uses to communicate with those devices.

SNMPv1/v2

Tap the toggle button to enable or disable SNMPv1 and v2 queries. This setting is enabled by default and uses the Community Strings configured in the next setting.

Community Strings

Tap this field to open the Community Strings list screen and add, edit, or remove community strings.



The LRAT uses the checked strings in the order shown on this screen. If it does not receive a

response from the queried device using one string, it sends the next string.

> NOTE: This screen and others in the Discovery settings operate much like the AutoTest Profile Group screen.

On the Community Strings screen, you can perform these actions:

- Check or uncheck the boxes to include or exclude a string from use in the current Discovery configuration.
- Tap the up and down arrows  to change the order in which the LRAT uses the strings to query a device.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a Community String.
  CAUTION: Deleting a string removes it from all saved Discovery configurations. To remove a string from the current Discovery configuration only, simply uncheck it.
- Tap the FAB  to add new Community Strings.

- Tap any Community String's row to edit the string and its description.

  TIP: To minimize discovery time, uncheck or delete all unused community strings, as every failed query extends the discovery time. You can also arrange the community strings in the order they are used most.

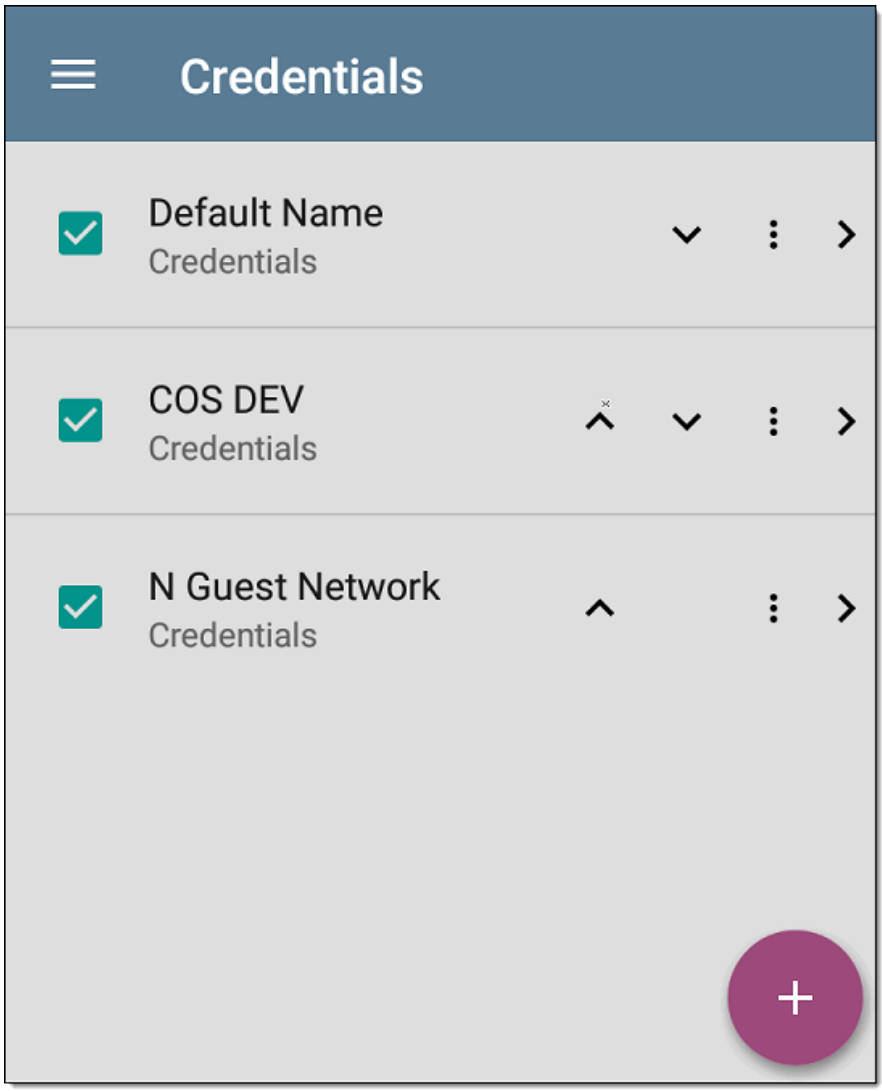
SNMPv3

Tap the toggle button to enable or disable SNMPv3 queries. This setting is enabled by default and uses the Credentials configured in the next setting.

NOTE: If this setting is enabled, but no SNMPv3 credentials are configured, the LRAT discovers the engine IDs of all SNMPv3 agents. This is a good way to discover if a device supports SNMPv3.

Credentials

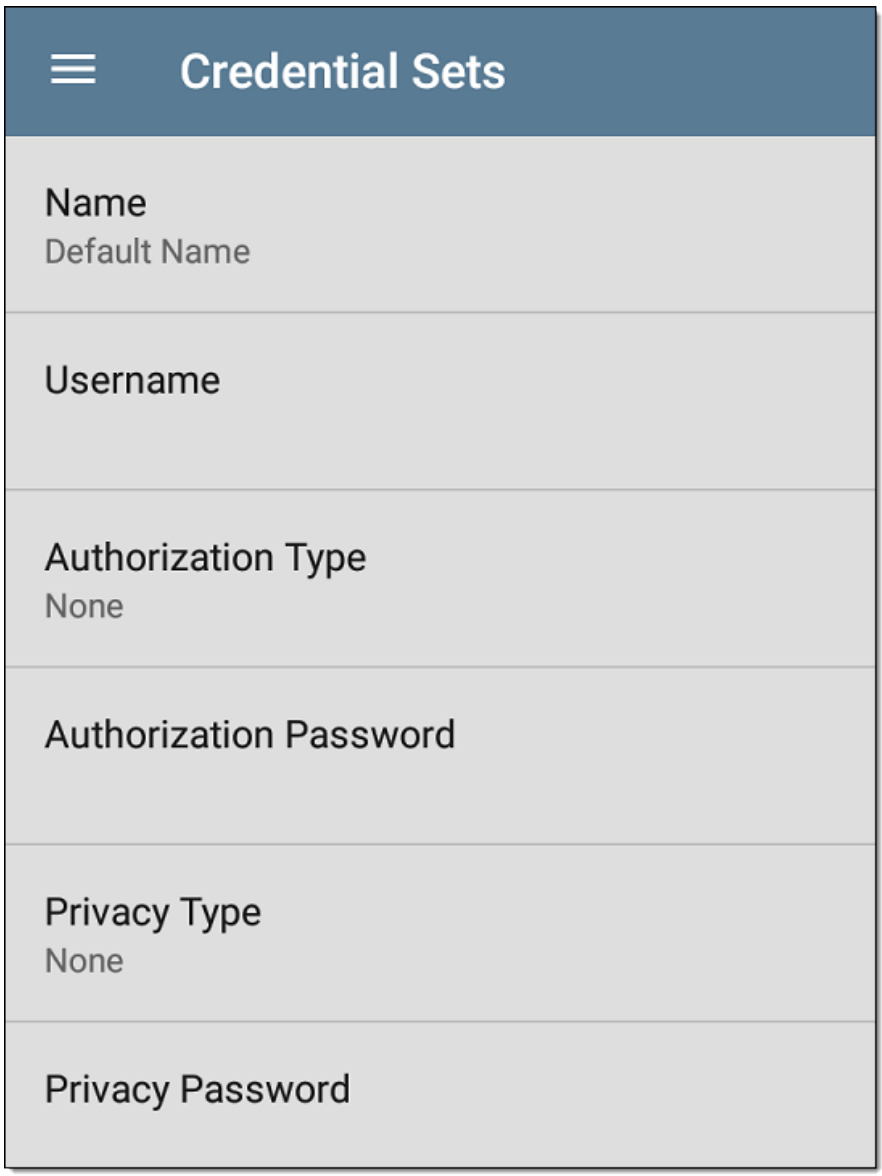
Tap this field to open the Credentials list screen.



This screen interface works like the Community Strings screen above. LRAT uses the Credentials in the order shown.

- Check or uncheck the boxes to include or exclude a set of Credentials from use in the current Discovery configuration.
- Tap a row to edit its credentials.

- Tap the FAB + to add new credentials.



On the Credentials Sets screen, tap each field to select or enter the credentials required.

Name

Tap the **Name** field to enter a custom name for the Credential Set.

Username

Tap to enter the SNMPv3 username.

Authorization Type and Password

LRAT Discovery supports two SNMPv3 Authorization types: HMAC-SHA and HMAC-MD5. If Authorization is required, enter the appropriate password.

Privacy Type and Password

LRAT Discovery supports four Privacy Types: CBC-DES, AES-128, AES-192, AND AES-256. If needed, enter the appropriate Privacy Password.

SNMP Query Delay

This function controls how long your LRAT waits between SNMP queries to key tables that can cause CPU spikes in the SNMP agents, including the ARP cache, IP address table, routing tables, and FDB tables.

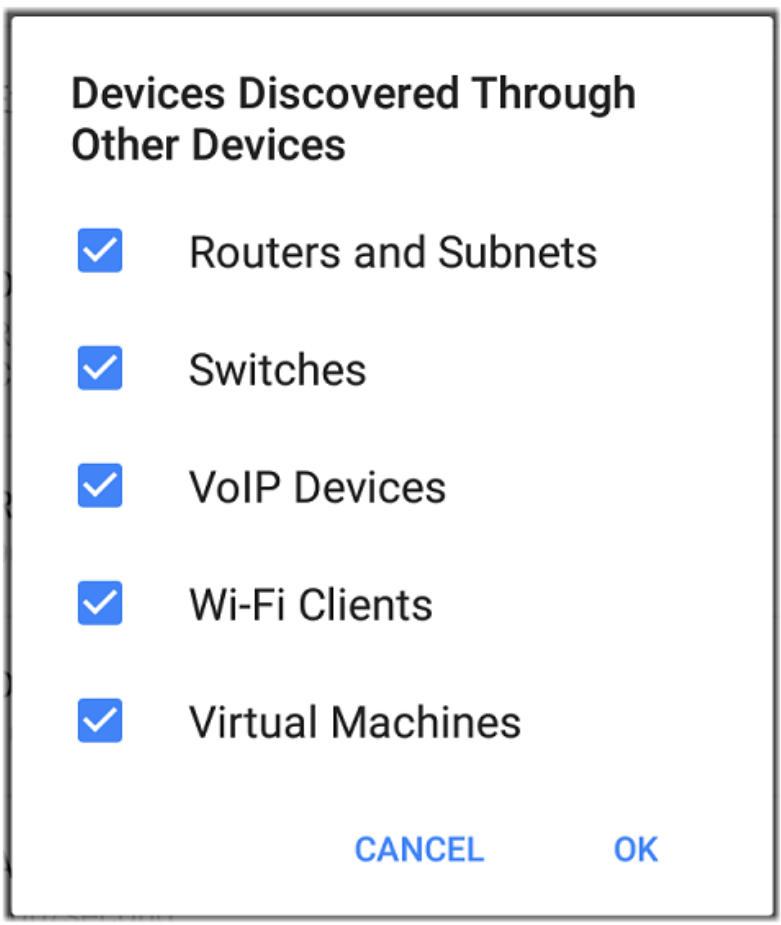
The default SNMP Query delay is No Delay. When querying the key large tables, the LRAT asks for more data as soon as a response has been

Back to Title and Contents

received. You can select a 1 or 5 second delay if needed.

Devices Discovered Through Other Devices

By default, LRAT discovers devices from SNMP tables of other devices. If you do not want Discovery to automatically find devices from SNMP tables of the device types listed here, you can uncheck their boxes.



Routers and Subnets

When the Routers and Subnets checkbox is enabled, any discovered routers are included in discovery results. In addition, if Discovery has SNMP access to a discovered router, its routing tables are read, and the next hop routers are added to the Discovery list. If any local subnets are available in the routing tables, these are also added to the Subnets list. This process continues until all the available SNMP credentials are tried for the added routers.

> NOTES: Discovery does not sweep every discovered subnet; discovered subnets are only added to the subnets list. To perform discovery in a specific subnet, see **Extended Ranges** above.
>
> If another site has routers you want to discover using this process but there isn't a local next hop link from this site, you can add one of the routers of that site to discovery. The process then runs from that router and finds the routers on that site as well. Add the subnet of the router or just the

router’s IP address with a mask of /32 to Extended Ranges.

Switches

When the Switches checkbox is enabled, discovery adds any switches that it finds in SNMP neighbor tables of other devices to the Discovery list.

For example, when LRAT is reading the CDP and LLDP caches of one switch, it contains other switches. If this option is enabled, the LRAT adds those other switches, even if they are not in discovery ranges.

> NOTE: To Discover switches at another site, add one of the switches of that site to Discovery Extended Ranges.

VoIP Devices

When the VoIP Devices checkbox is enabled, discovery adds any VoIP devices that it finds in SNMP tables of other devices regardless of the subnet. These are usually found in the LLDP-MED tables of the switches. Enabling the Switches option provides the best chance of finding all your VoIP devices.

Virtual Machines

When the Virtual Machines checkbox is enabled, discovery adds any virtual machines that it finds in SNMP tables of other devices. These are usually found in the ESX host > SNMP tables. Adding the subnets of your ESX hosts to Extended Ranges helps with finding your virtual machines.

Device Health Interval

Discovery automatically runs a set of network health tests to search for network Problems, such as high utilization, discards, or errors on all discovered interfaces and device resources.

The selected time Refresh Interval is the minimum time between each run of the Device Health tests. Tap the field to disable Device Health testing or to change the interval from the default of 10 minutes to 30 or 60 minutes.

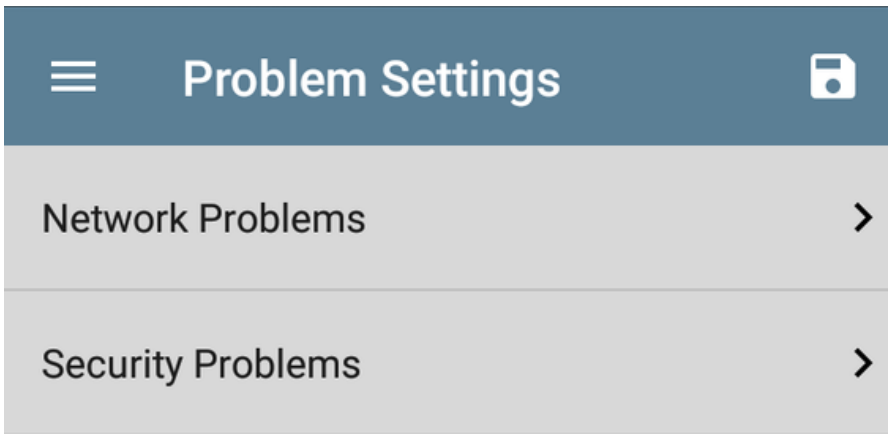
Disabling the Device Health testing affects the types of Problems that Discovery can detect.

See also Problem Settings.

Problem Settings

The Problem settings determine which issues are detected and displayed by the Discovery app as well as the thresholds for enabled problems, such as Packet Discards and Utilization.

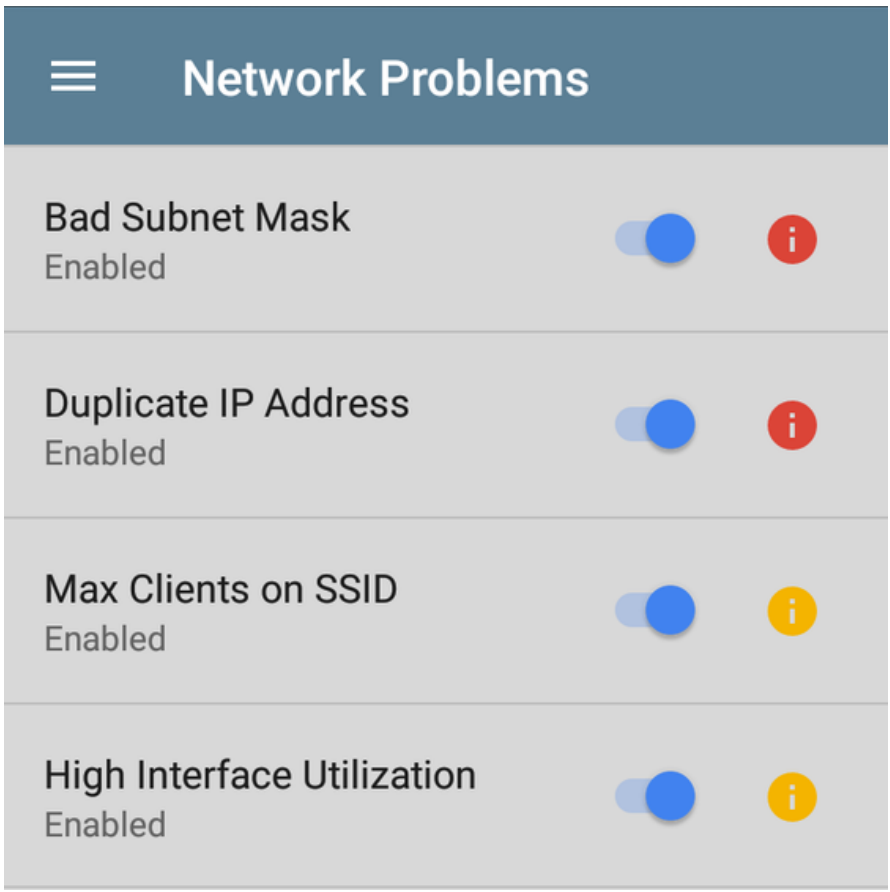
Access the Problem Settings screen by sliding out the left-side navigation drawer or tapping the menu icon in the Discovery app, and selecting **Problem Settings**.



Problems are categorized as Network or Security.

As with Discovery Settings, you can save, load, import, and export configured Problem Settings by tapping the save button on this screen. See Managing Testing App Settings for more instructions.

Tap the row for each to enable or disable the problem types and set thresholds where applicable.



All Problem types are enabled by default. Tap the toggle button to the right to disable each one.

- Tap the information icons to the right of each Problem to read a detailed description and recommended actions.
- **Red** icons indicate Failure conditions.

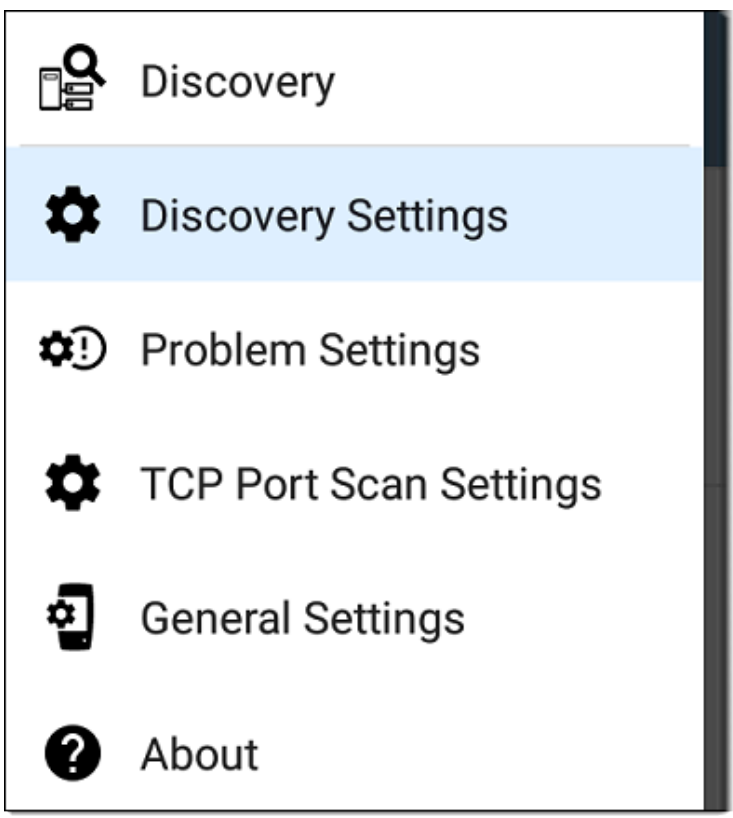
- **Yellow** icons indicate Warning conditions.

When you finish configuring, tap the back button  to return to the main Discovery screen.

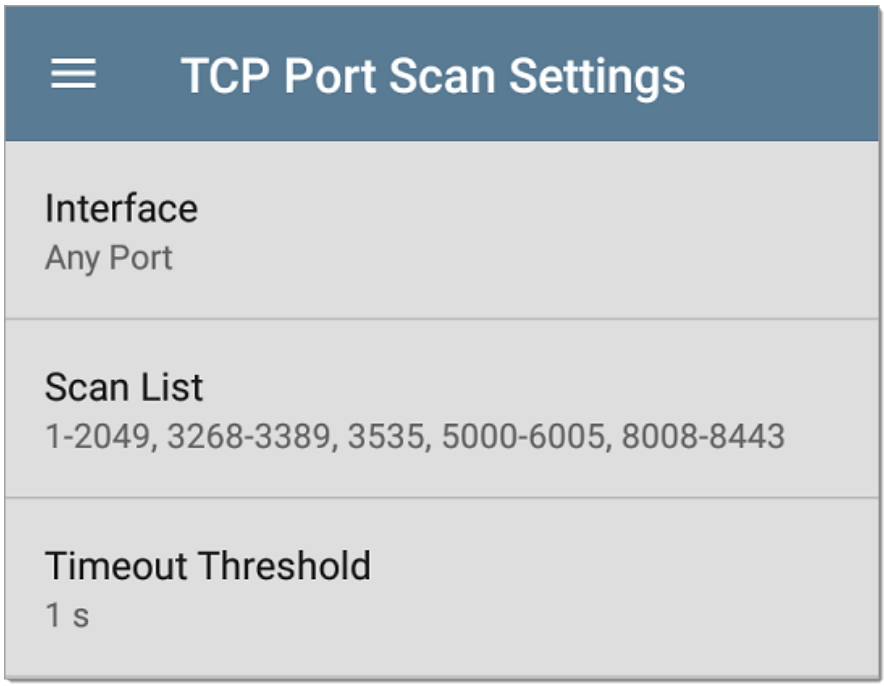
TCP Port Scan Settings

The TCP Port Scan feature checks for open ports on the current device. To run scan, tap the FAB on the Discovery Details screen, and then tap **TCP Port Scan**. The LRAT scans many ports simultaneously and reports the open port's numbers.

Access the TCP Port Scan Settings by sliding out the left-side navigation drawer or by tapping the navigation menu icon , and then selecting **TCP Port Scan Settings**.



This displays the TCP Port Scan Settings screen.



Interface: Tap the field to select the LRAT port from which the port scan runs. (See Selecting Ports for explanations of the different ports.)

Scan List: Tap this field to edit the list of port numbers that get tested during the port scan. You can enter port numbers or ranges, separated by commas.

Timeout Threshold: Tap this field to select a value for how long the LRAT waits for a response from each port or to enter a custom value. The scan ends after all the ports in the Scan List have had this amount of time to respond, and then the results screen lists the ports that responded within the threshold.

See also the TCP Port Scan results card and screen.

Path Analysis App

Path Analysis traces the connection points, including intermediate routers and switches, between the LRAT 3000-4000 and a destination URL or IP address. You can use Path Analysis to identify issues such as overloaded interfaces, overloaded device resources, and interface errors. It also shows how devices within your network (and off-net devices) are connected to each other along a path.

All switches are pre-discovered through SNMP queries. When the measurement is complete, LRAT shows the number of hops to the destination device. A maximum of 30 hops can be reported.

> NOTE: This application applies to the LinkRunner AT 4000 only.

Introduction to Path Analysis

Path Analysis combines Layer 3 and Layer 2 measurements.

The Layer 3 measurement combines the classic Layer 3 IP (UDP, ICMP, or TCP) traceroute measurement with a view of the path through the Layer 2 switches.

The Layer 2 measurement discovers switches between the router hops by looking for the routers' MAC addresses in the switch forwarding tables by sending SNMP queries to all discovered switches. The switches found in the path are displayed between the router hops when the measurement finishes.

Path Analysis is most effective when you have configured the Discovery app with SNMP credentials. See SNMP Configuration in the Discovery Settings topic to learn how.

Path Analysis Settings

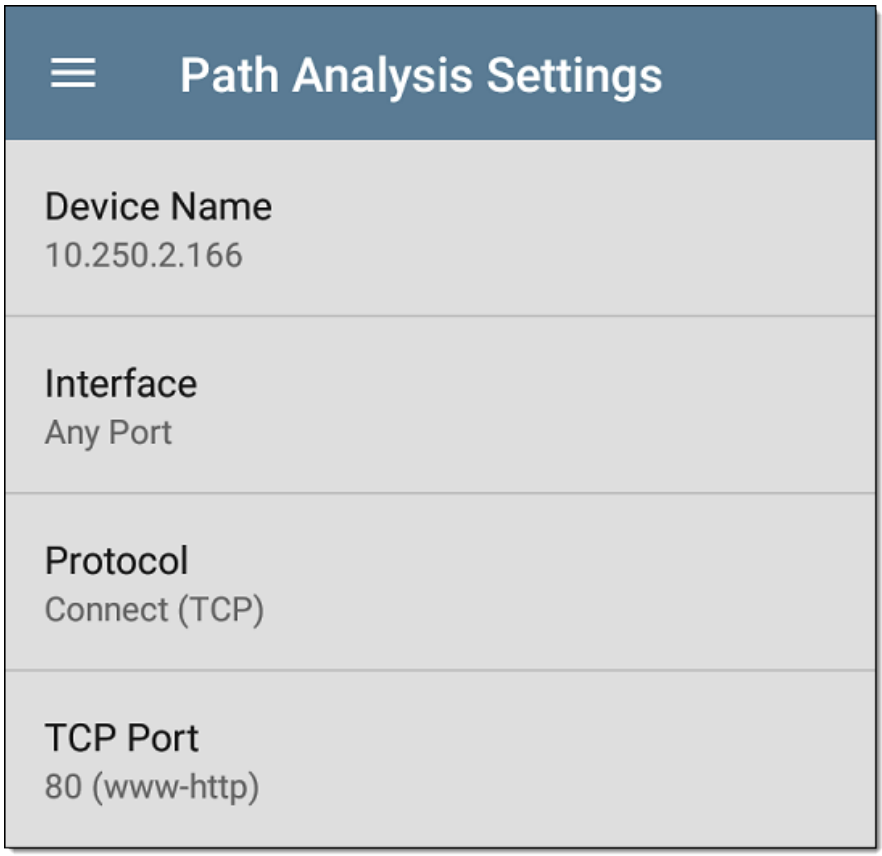
The Path Analysis source device is always your LinkRunner AT 4000. The default destination is www.google.com.

Populating Path Analysis from Another App

Like other LRAT testing apps, when you open Path Analysis from another app, like Discovery, the address of the network component you were viewing in the previous app is pre-populated as the Path Analysis Destination.

Configuring Path Analysis Manually

Open the app settings to configure a custom destination and select an Interface and Protocol. To open from the Path Analysis app screen, tap the settings  icon, or open the left-side navigation drawer and select **Path Analysis Settings**.



On the Path Analysis Settings screen, tap each field as needed to configure your target:

Device Name: Tap to enter the IP address or DNS name of the Path destination. The default is www.google.com.

Interface: This setting determines the device port to run the path analysis runs. Tap the field to select a port. (See Selecting Ports for explanations of the different ports.)

LRAT must have an active network link on the selected port to run a Path Analysis. If **Any Port**

is selected, available links are used in the order shown in the Interface selection dialog.

See Test and Management Ports for explanations of the different ports and how to link.

Protocol: Tap to select the Connect (TCP), Ping (ICMP), or Echo (UDP/7) protocol for your Path Analysis.

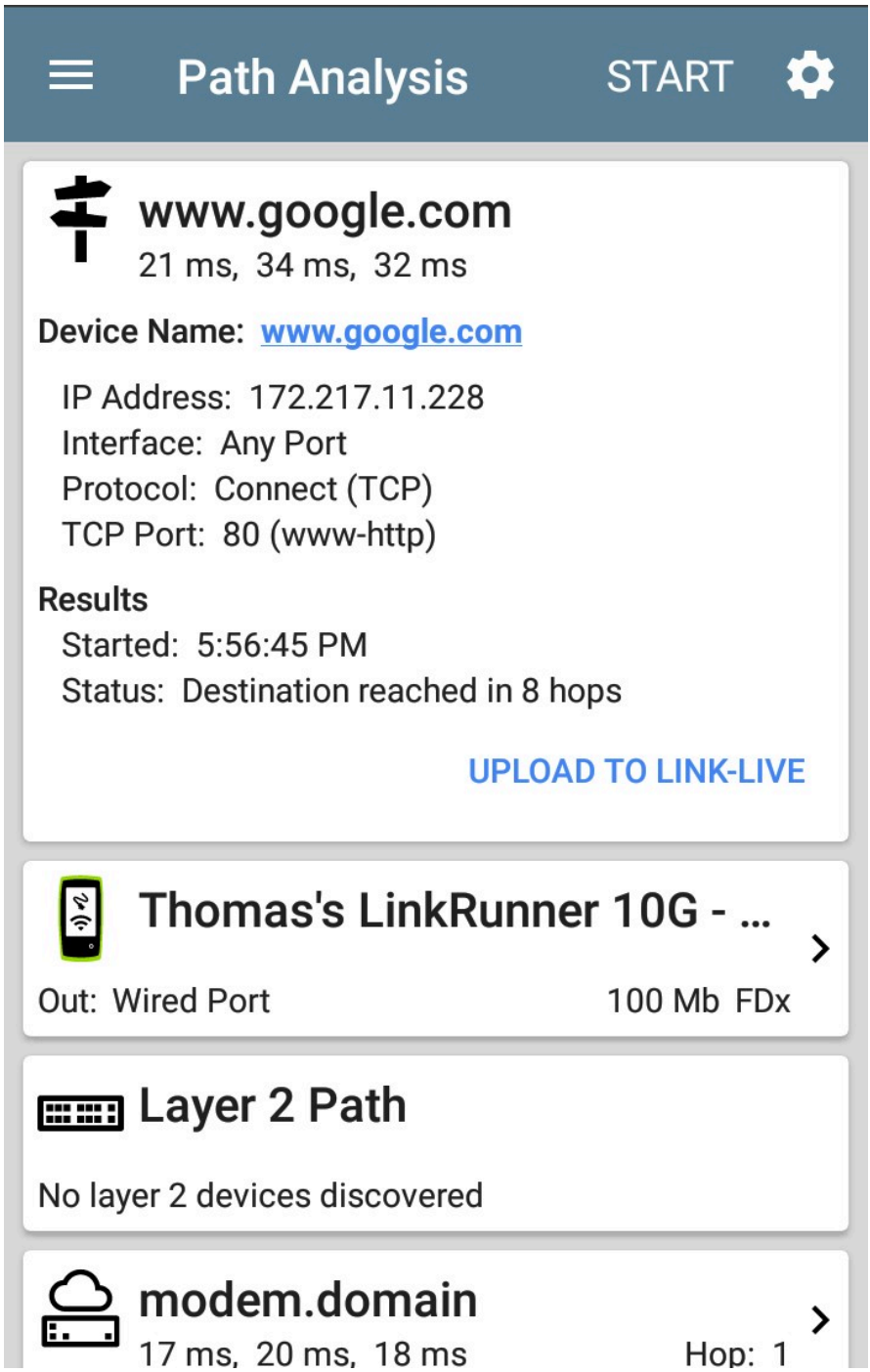
TCP Port: This field only appears if you have selected the Connect (TCP) Protocol. Tap to enter the port number over which you want to run Path Analysis. (You may need to enter a specific port number because routes can vary based on the port number and/or may be blocked by firewalls.)

Back to Title and Contents

Running Path Analysis

Tap the **START** button at the top of the app screen to begin a Path Analysis.

> NOTE: LRAT must be linked on the Interface (Port) selected in the app's settings. See Test and Management Ports for help.

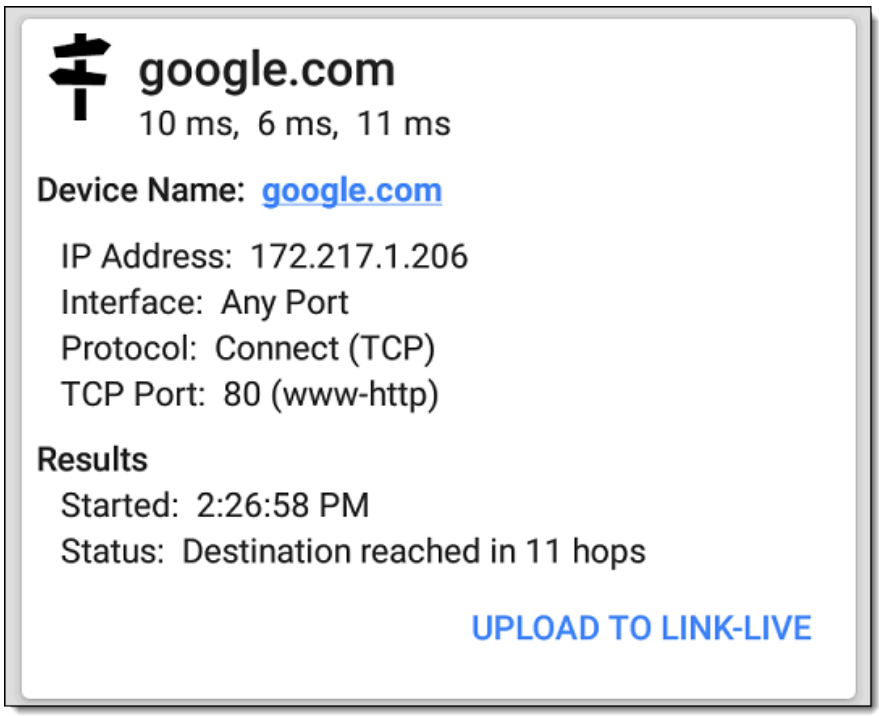


Like AutoTest, Path Analysis results are presented on cards. The top card shows the main test details, the second card shows information for the source device (your LRAT

3000-4000), and the following cards show the Layer 2 and Layer 3 Hops in the path, which are sequentially ordered.

Tap any **blue linked name or address** in the Path Analysis results screens to open the Discovery app and further examine the linked element.

Path Analysis Results and Source LRAT Cards



The top Path Analysis results card shows the path's Destination address at the top, followed

by the three response times from the TCP Connect, Ping, or Echo tests.

Device Name: Resolved DNS name or IP address of the destination entered in the settings

IP Address: IPv4 address of the target destination

Interface: The Interface option selected in the settings

Protocol: The Protocol selected in the settings (TCP, Ping, or Echo)

TCP Port: The port number used for a TCP Connect Protocol. (This field does not appear for Ping or Echo Protocol results.)

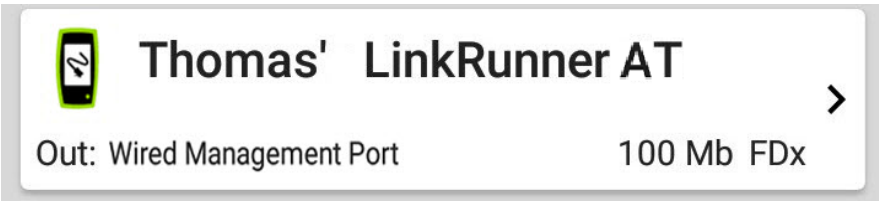
Results

Started: Time at which the Path Analysis began

Status: Current status of the Path Analysis test, including any error messages

UPLOAD TO LINK-LIVE: Tap this link to upload your results to a Link-Live account. See Uploading Results to Link-Live later in this topic.

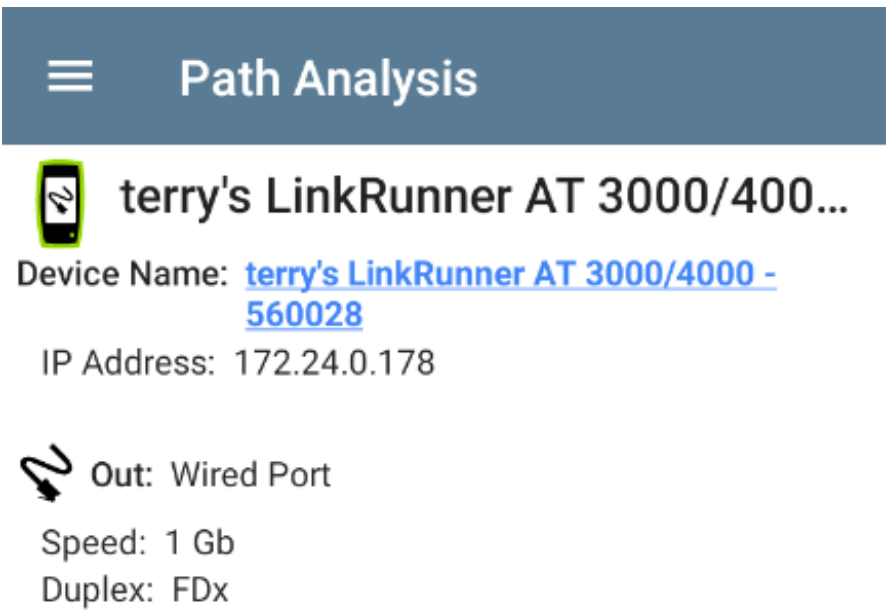
Source LRAT Card



This LRAT card displays the port from which the Path Analysis ran.

> NOTE: This card and screen only display a custom name for your LRAT if you have claimed it to Link-Live.

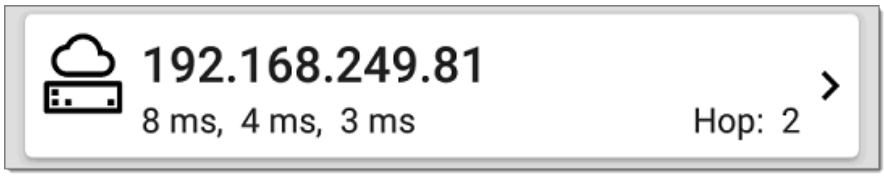
Tap the card to view more details. The image below shows the source LRAT card from a Wired Path Analysis, which displays the link speed and duplex.



(LinkRunner AT 4000 only) Under the LRAT source card, the Hop cards show Layer 2 and Layer 3 devices determined to be in the Path.

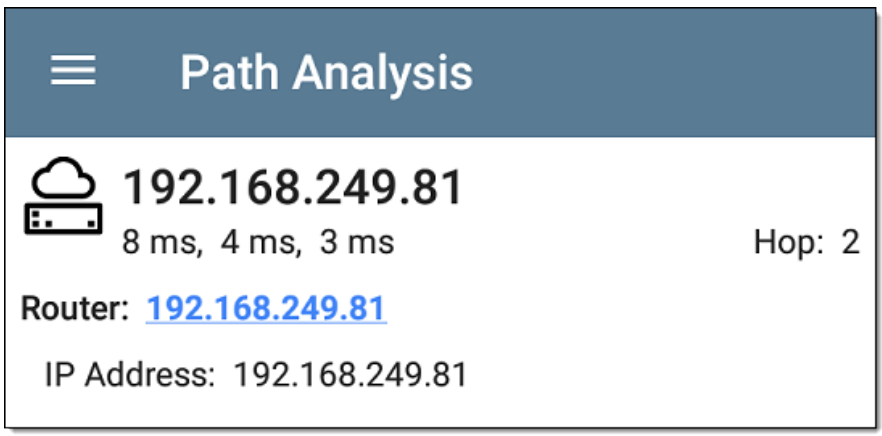
Layer 3 Hops

Each Layer 3 Hop card displays the device type icon, DNS name (if discovered), and IP address.



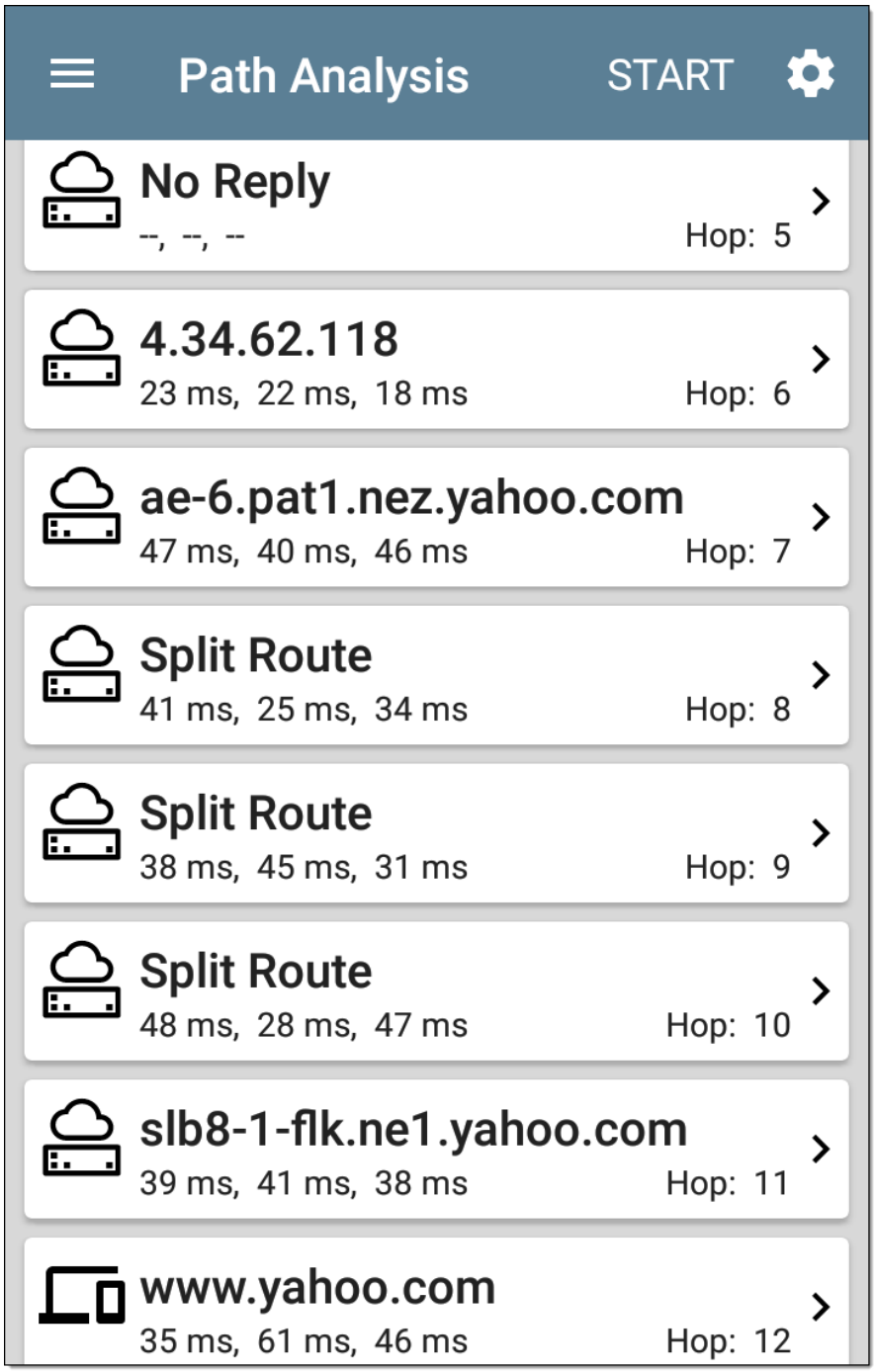
Beneath the name (or IP), the response times for each Connect (TCP), Ping (ICMP), or Echo (UDP/7) display in milliseconds. On the right side is the router Hop number of this device in the path.

Tap the card to view the hop Details screen.



No Reply

Sometimes Path Analysis displays Hop cards with "No Reply" (as shown below). This result means that the device in that portion of the path did not send an ICMP TTL timeout response.

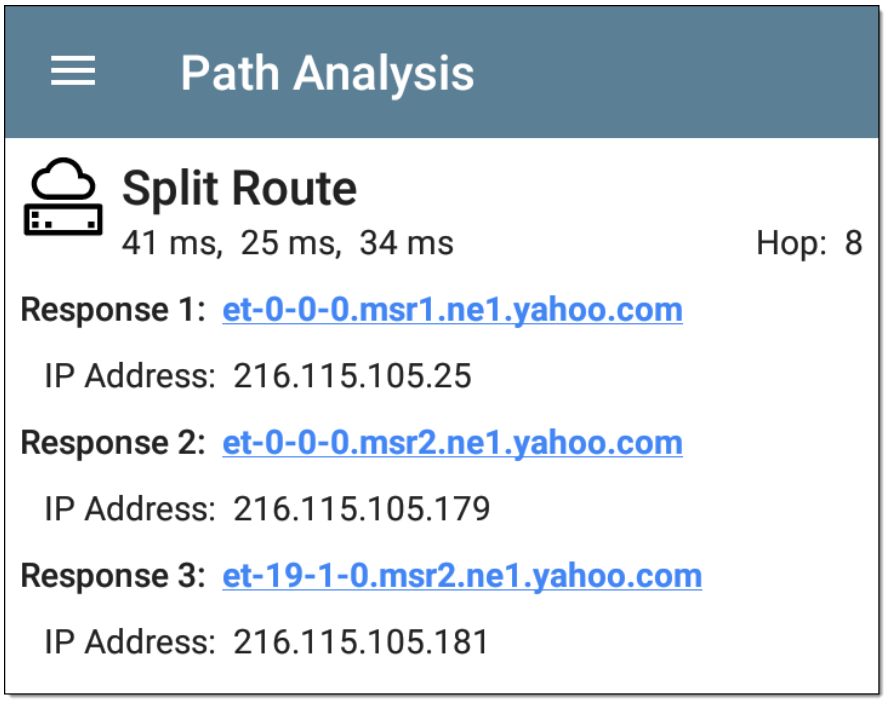


Split Route

Path Analyses may obtain a "Split Route" result (as shown above), meaning that two or three

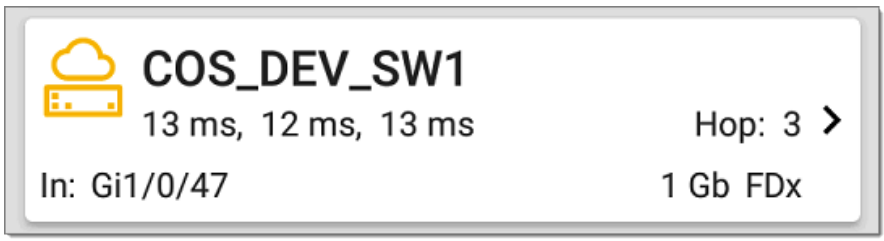
different routers within same hop responded to the three requests.

Tap a Split Route card to view the DNS names and IP addresses of the responding routers.



Layer 3 Interfaces and Statistics

Statistics for Interfaces on Layer 3 devices may be identified and measured if the LRAT has SNMP access.



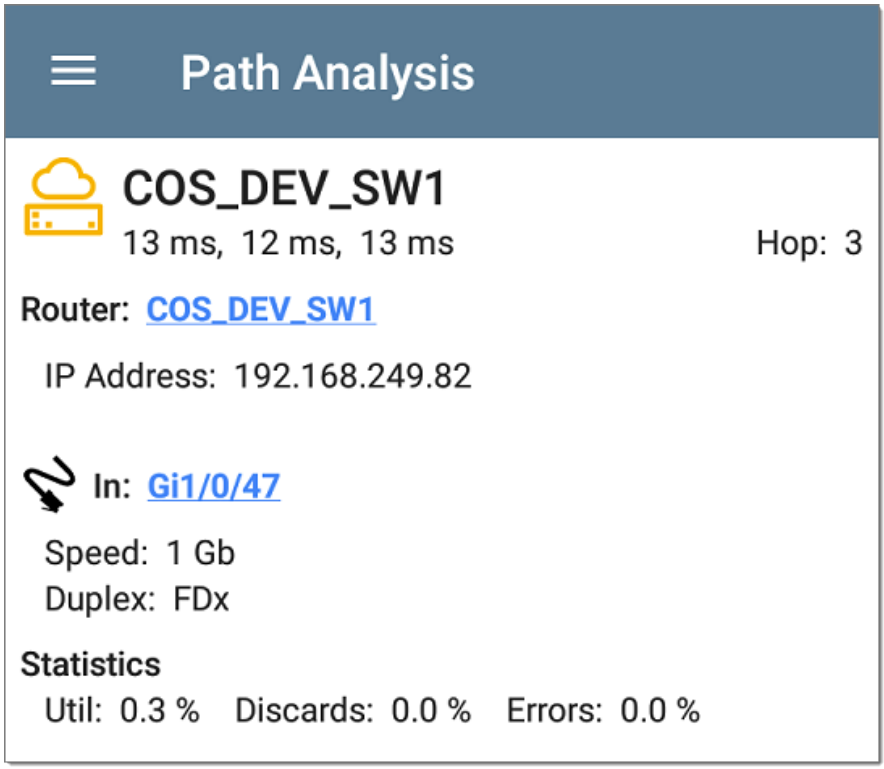
Tap a Hop card to see a summary of Interface Details and Statistics, if they are available.

See also Layer 2 Switch Interfaces and Statistics below.

Network Problems in Path Analysis

The Hop cards can also show detected Problems based on the Problem Settings in the Discovery app and display the device type icons in the corresponding colors.

The yellow switch icon in the image above indicates a **Warning** status.



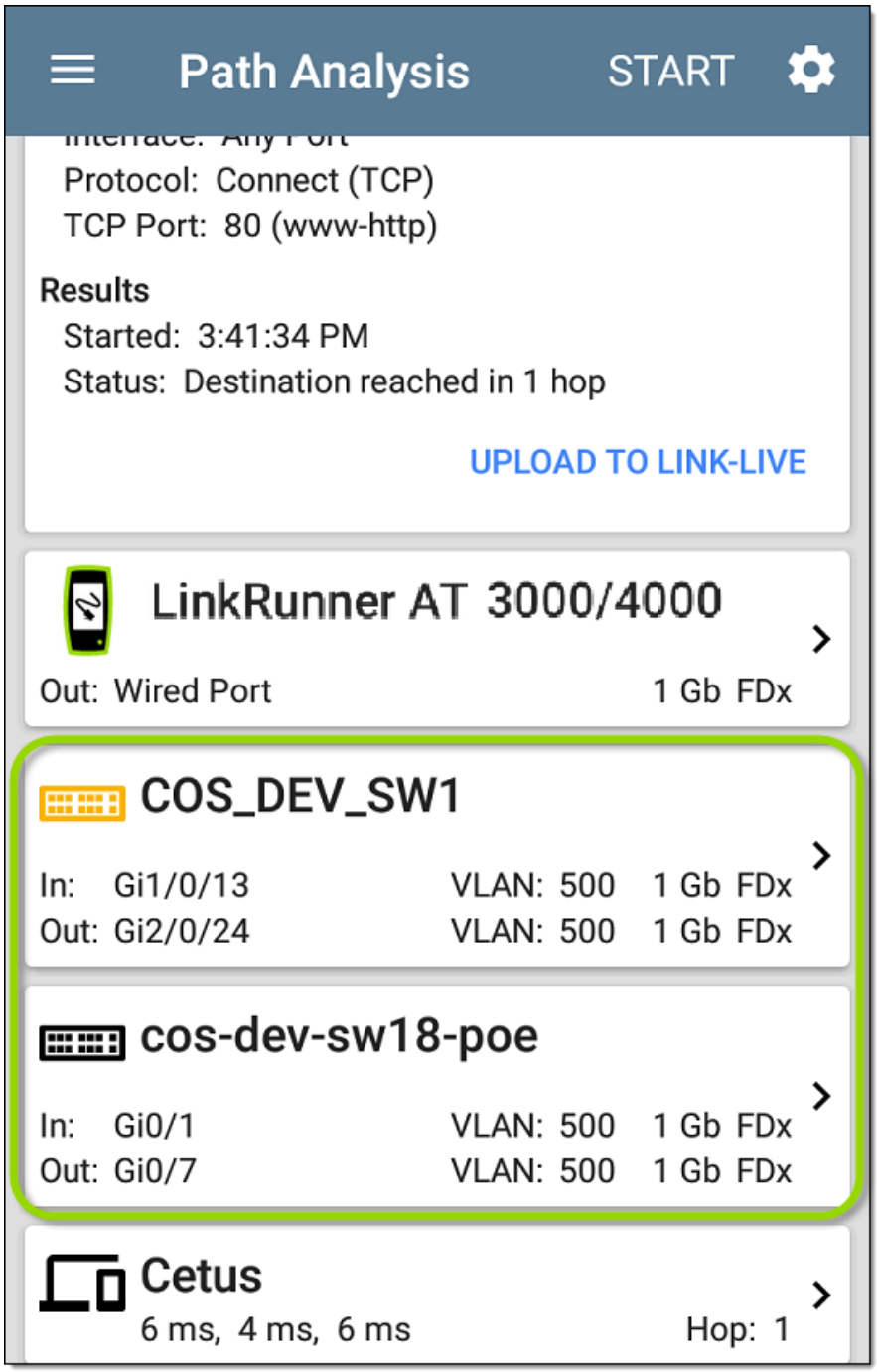
Tapping the blue linked switch name opens a Discovery Details screen for the switch, where the user can investigate the cause of the Warning.

Layer 2 Devices

Layer 2 devices can be switches or APs.

Layer 2 Switches

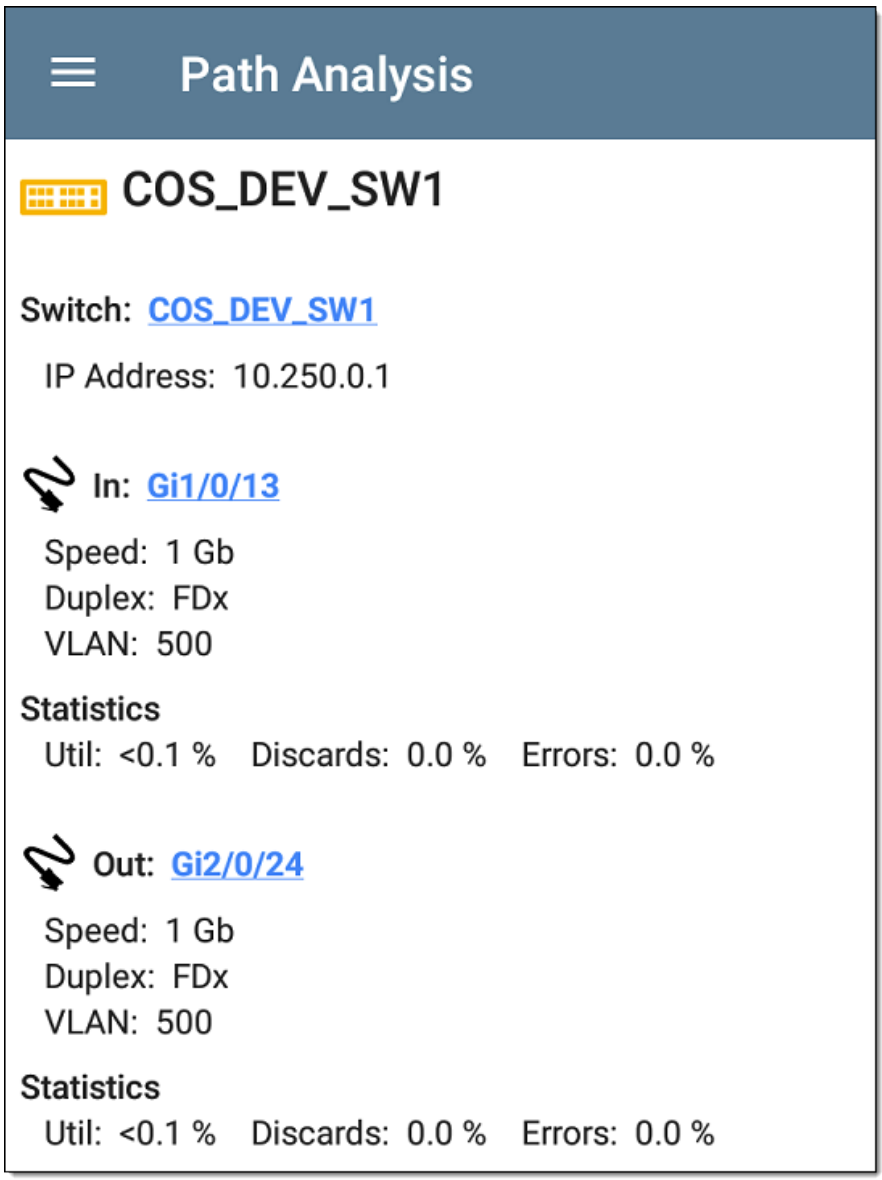
The image below displays an example of a Path Analysis to a device on the local broadcast domain with two switches in the Layer 2 portion of the path.



The LRAT is able to identify these Layer 2 switches and their interfaces because it has configured SNMP access to the switches.

The switch cards display the In and Out Interface IDs, VLAN ID, and the link speed and duplex (if detected) of the interfaces.

Tapping a Layer 2 card opens a Details screen for the device.



A Layer 2 Details screen displays the device name and IP address at the top.

NOTE: The yellow switch icon in the image above indicates a **Warning** status. See Network Problems in Path Analysis later in this topic.

Layer 2 Switch Interfaces and Statistics

Layer 2 Switch Details screens in Path Analysis display a summary of the Interface Statistics (described below). To view all available information for these interfaces, tap their blue links to open a Interface Details screen in the Discovery app.

Statistics for Interfaces on Layer 2 switches may be identified and measured if the LRAT has SNMP access.

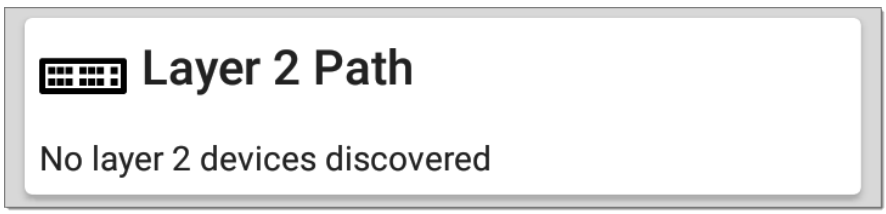
In/Out: Indicates the interface type and name. The interface name often contains the physical port number where the switch is connected to the network.

Util: Percentage of total interface capacity being used

Discards: Percentage of total packets that have been dropped

Errors: Percentage of packets containing errors

No layer 2 devices discovered

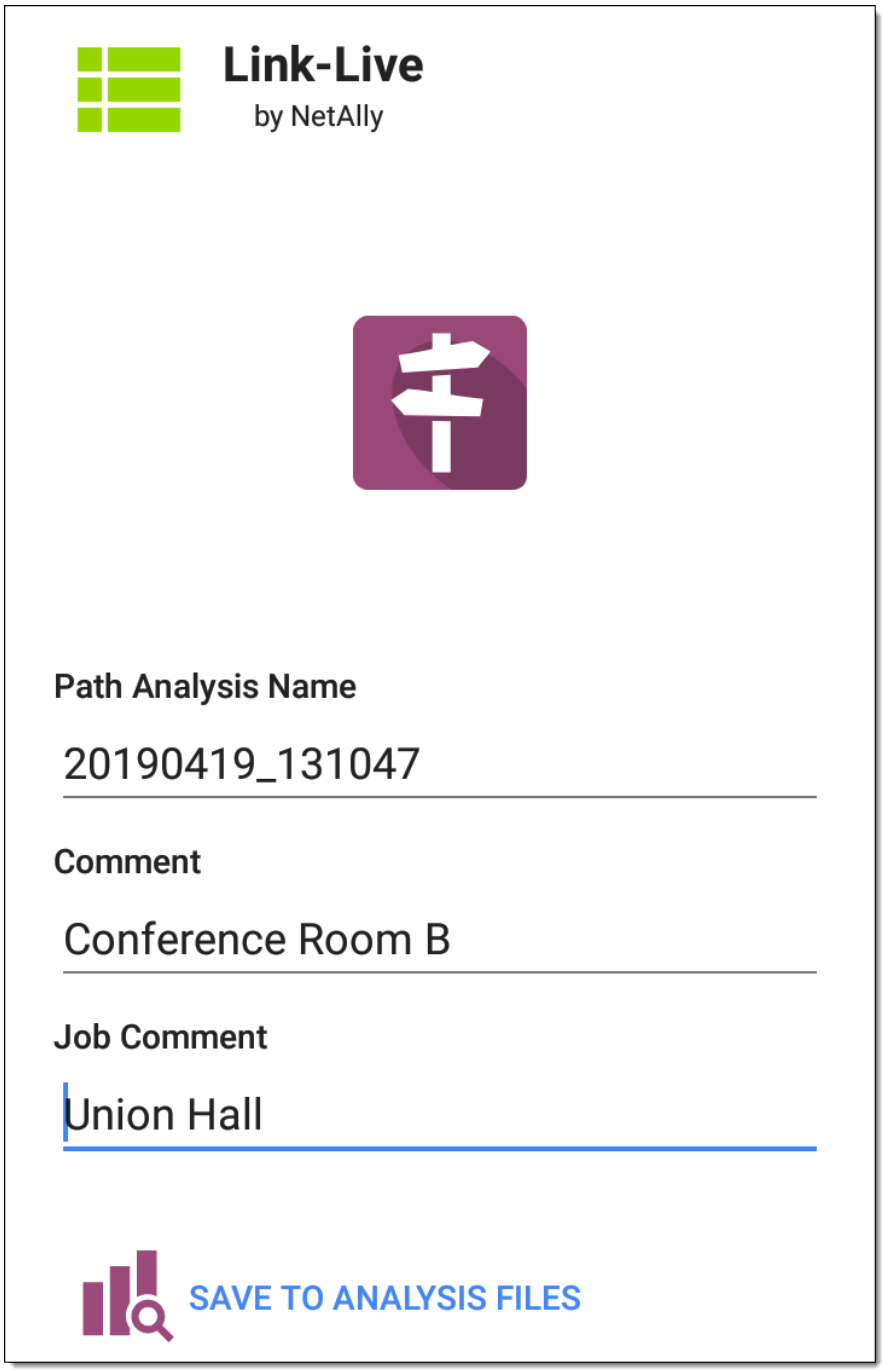


In some cases, the LRAT does not discover Layer 2 devices between Layer 3 devices. There may not be any Layer 2 devices, or LRAT might not have SNMP access to those switches.

The Layer 2 card may also display a result of "No switches found," which indicates that Discovery has not found any switches with SNMP access to determine if the switches are in the path. If this is an unexpected result, check and verify your SNMP Configuration and Extended Ranges in the Discovery app settings.

Uploading Results to Link-Live

Tapping the **UPLOAD TO LINK-LIVE** link on the top card opens the Link-Live sharing screen for path analysis results:



Path Analysis results are uploaded to the **Analysis** page on Link-Live.

Back to Title and Contents

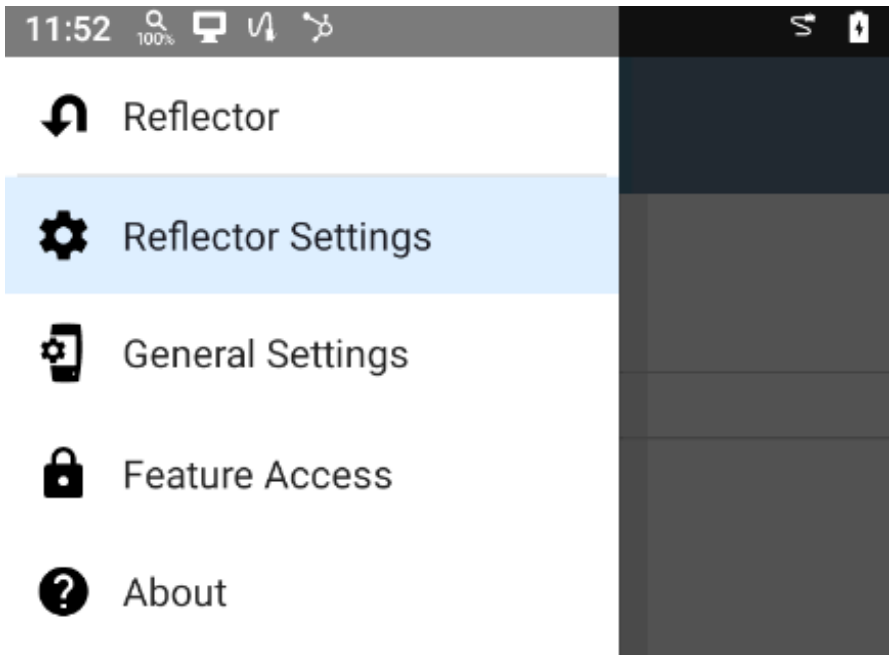
Reflector App

The Reflector app allows you to turn your LinkRunner AT 3000/4000 into a performance test reflector. You can use the Reflector app with other NetAlly testing devices that use the Performance or LANBERT apps. It can also be used as a general purpose packet reflector. Your unit takes packets received from the other device; flips the source and destination MAC and IP address; and then sends the packets back to the device. The sending device can then compare the number of packets sent to the number received from Reflector. This app can be useful for pre-deployment testing of network endpoints and ensuring that network performance can support specific applications.

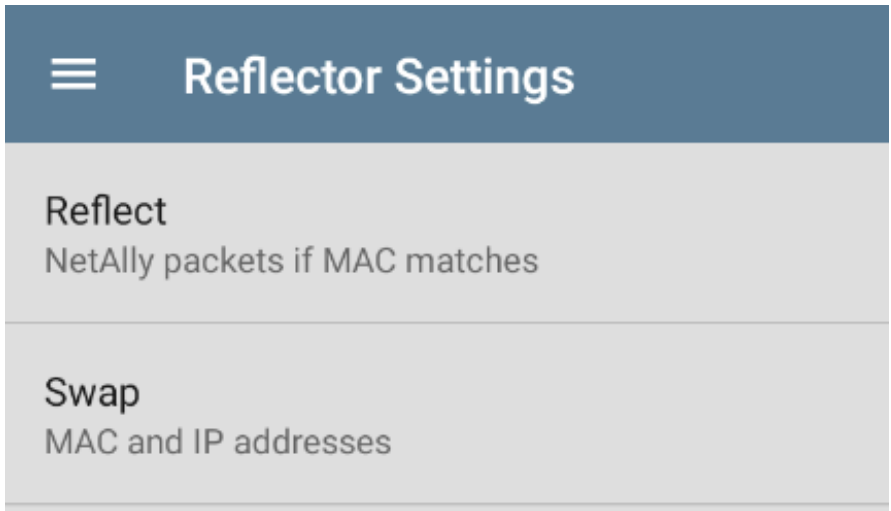
Reflector Settings

To choose basic Reflector settings:

1. From the main Reflector screen, tap the navigation menu icon or swipe from the left-side drawer to display the navigation menu.



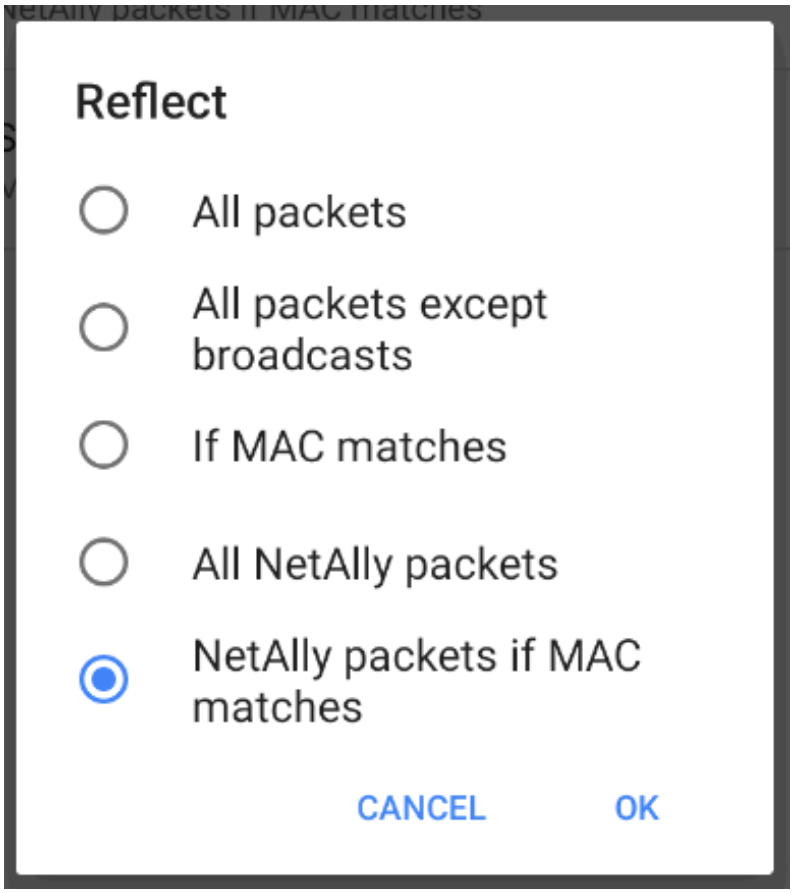
2. Tap **Reflector Settings** to display the settings options.



3. Tap each field described below as needed to configure the reflector. Changed settings are automatically applied. When you finish configuring, tap the back button to return to the main Reflector screen.

Reflect

Tap this field to select the packets to reflect:

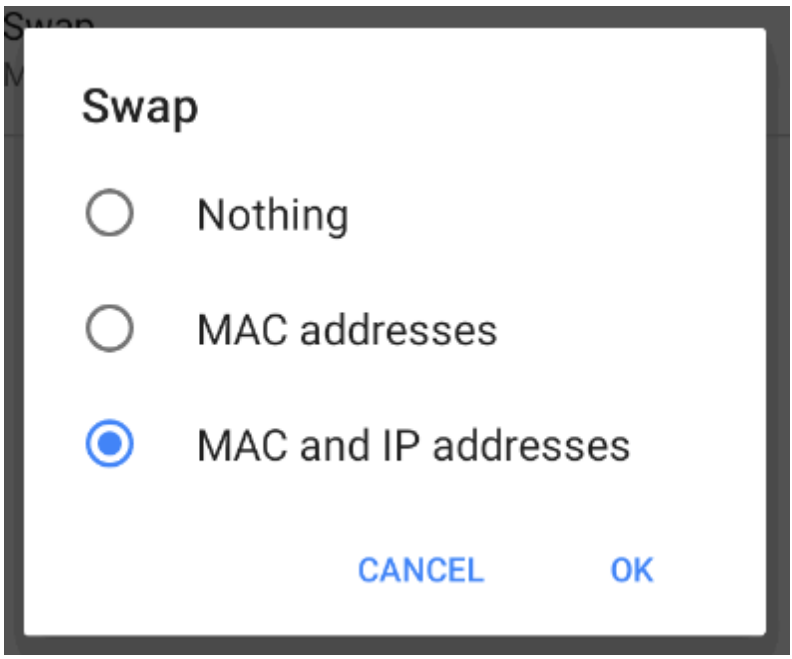


- In general, NetAlly recommends the default value of **NetAlly packets if MAC matches** to avoid any undesired traffic on your network.
- If you use Reflector with a NetAlly test unit running the Performance app, use the Reflect default value of **NetAlly packets if MAC matches** *and* set use Swap default value of **MAC and IP addresses**.
- If you use Reflector with a NetAlly test unit running the LANBERT app, set the Reflect

value to **All packets except broadcasts** *and* set the Swap value to **MAC addresses**.

Swap

Tap this field to select the swap options:



- In general, NetAlly recommends the default value to avoid any undesired traffic on your network.
- If you use Reflector with a NetAlly test unit running the Performance app, use the Swap default value of **MAC and IP addresses** *and* use the Reflect default value of **NetAlly packets if MAC matches**.

- If you use Reflector with another NetAlly test unit running the LANBERT app, set the Swap value to **MAC addresses** *and* set the Reflect value to **All packets except broadcasts**.

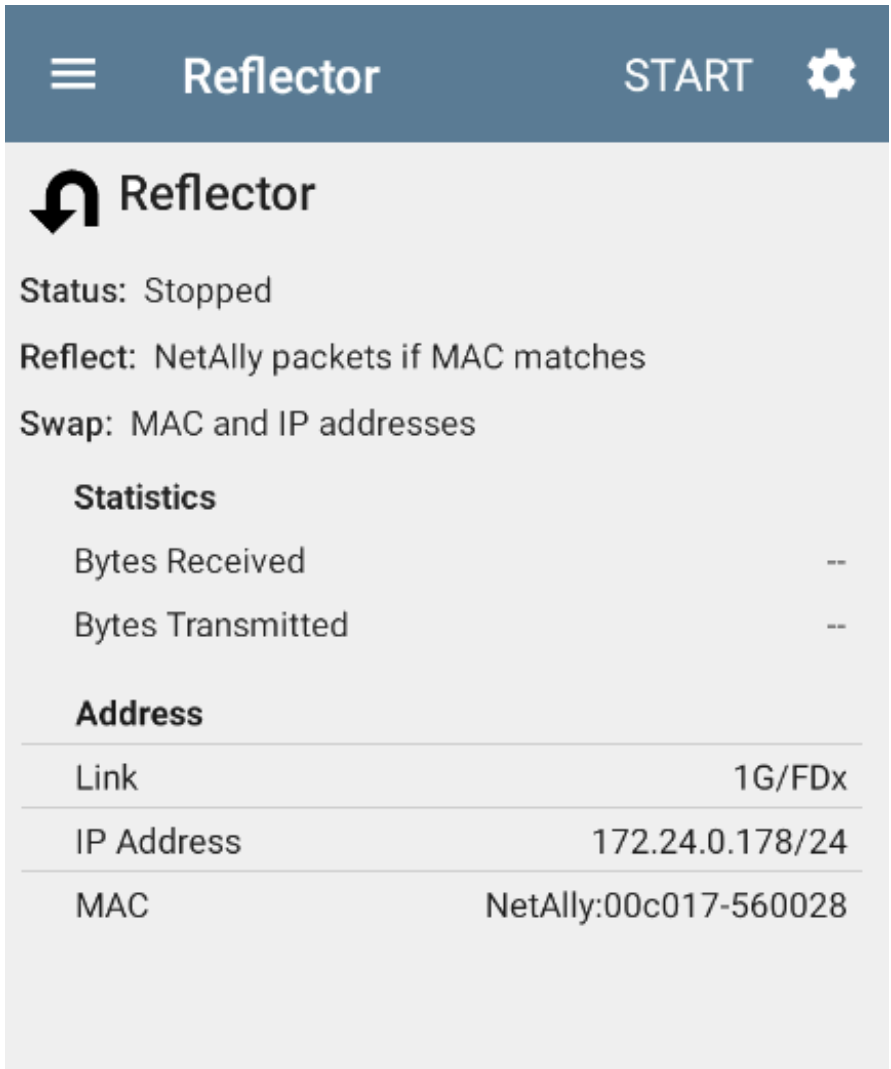
Back to Title and Contents

Running Reflector

After you have adjusted the Reflector settings to set the Reflect and Swap settings as required, you can run your LinkRunner AT 3000/4000 as a reflector.

1. To open the main Reflector screen, simply tap the Reflector icon on the LinkRunner AT 3000/4000 Home screen.
2. Ensure that your LinkRunner AT 3000/4000 is connected to an active network from the Wired Test Port (top RJ-45 or Fiber port).
3. Run an AutoTest Wired Profile to successfully establish link on the port.
4. Tap **Start** to begin the Reflector test. The Status indicates the test is running.

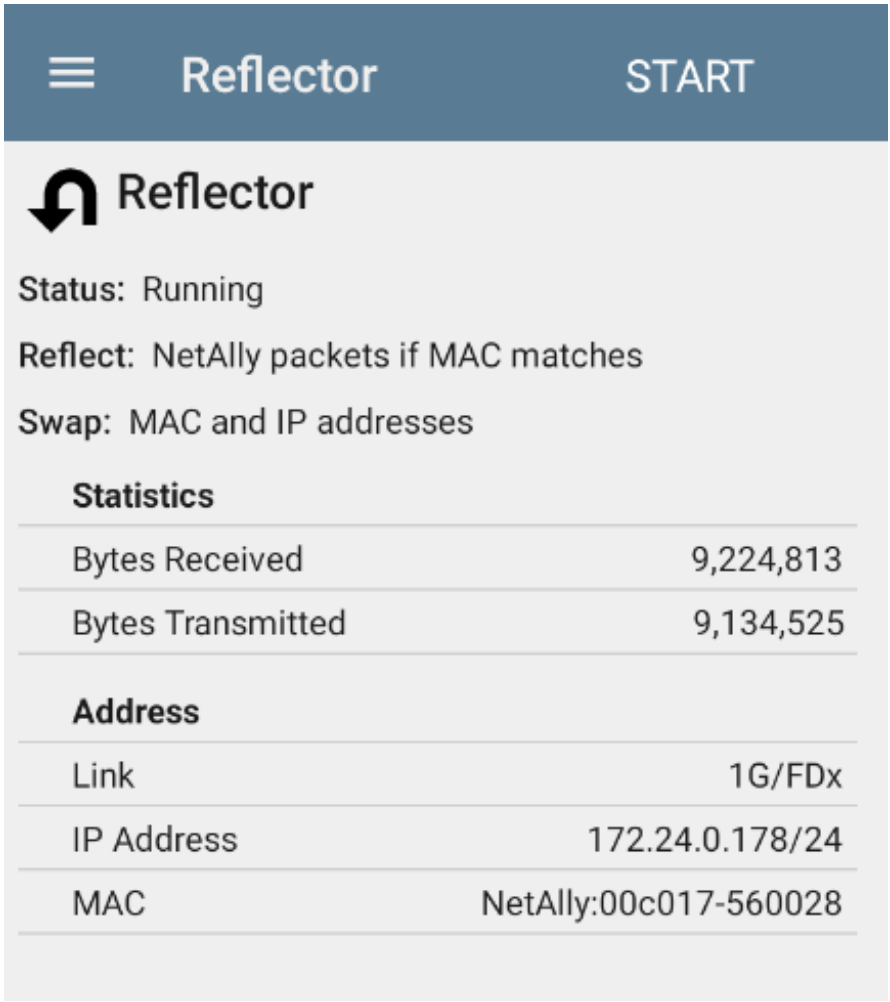
   NOTE: The IP address of the LinkRunner AT 3000/4000 is displayed at the bottom of the screen. Record the address to set up the master device that originates the test.



5. Follow the device instructions to set up the master device that sends the packets, and then start the test.
    - While running, the Reflector screen displays the bytes received and reflected.

- Your LinkRunner AT 3000/4000 remains on as long as the test is running.
- Navigating away from the Reflector app main screen stops the test. You can resume the test as long as both units are still running.

6. When you have gathered enough information, tap **Stop** to stop the Reflector app. The screen displays the numbers of bytes received and sent.



See the user documentation for the master device for information on viewing results.

Back to Title and Contents

iPerf Test App

iPerf is a standardized network performance tool used to measure UDP or TCP throughput and loss.

The iPerf app runs an iPerf3 performance test to a NetAlly Test Accessory or an iPerf server endpoint.

> NOTE: This application applies to the LinkRunner AT 4000 only.

The NetAlly Test Accessory runs network connection tests, uploads results to Link-Live Cloud Service, and acts as an iPerf server endpoint for iPerf tests run by other NetAlly handheld testers.

Learn more about the Test Accessory from **NetAlly.com/products/TestAccessory**.

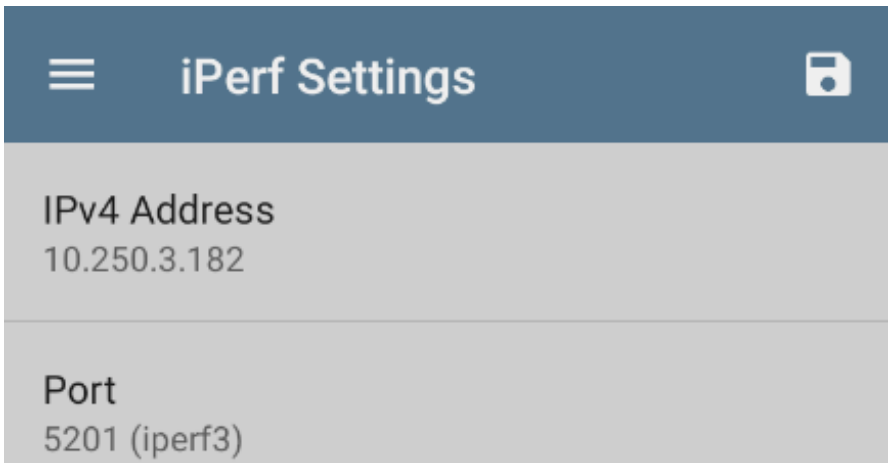
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the LRAT iPerf test. You can download iPerf server software from **https://iperf.fr**.

iPerf Settings

To run an iPerf test, you must configure your LRAT unit to communicate with your iPerf endpoint. You can manually enter an iPerf server address, or select a NetAlly Test Accessory's address in the iPerf settings.

Saving Custom iPerf Settings

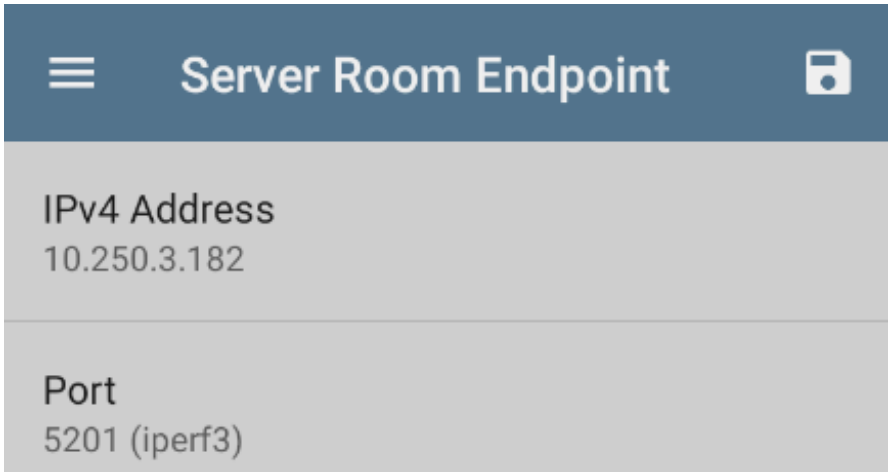
The iPerf app allows you to save a configuration of settings for running an iPerf test to the same endpoint later.

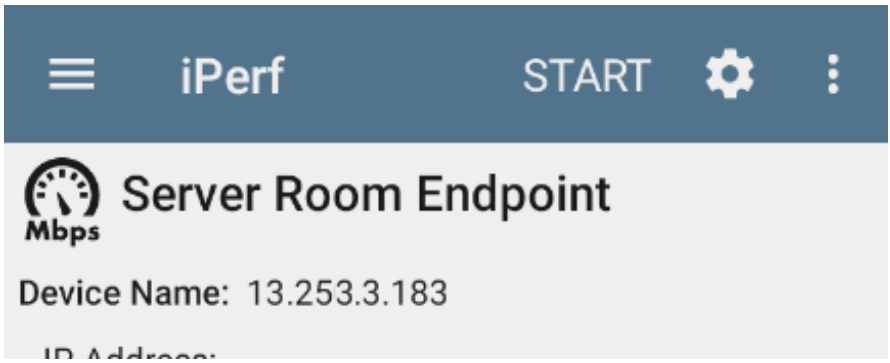


Tap the save icon to load, save, import, and export configured settings. See Saving App Settings Configurations for more instructions.

Once you save a settings configuration, the custom name you entered appears at the top of

the iPerf settings and results screens. In the example images here, the user has saved a custom iPerf configuration called "Server Room Endpoint."



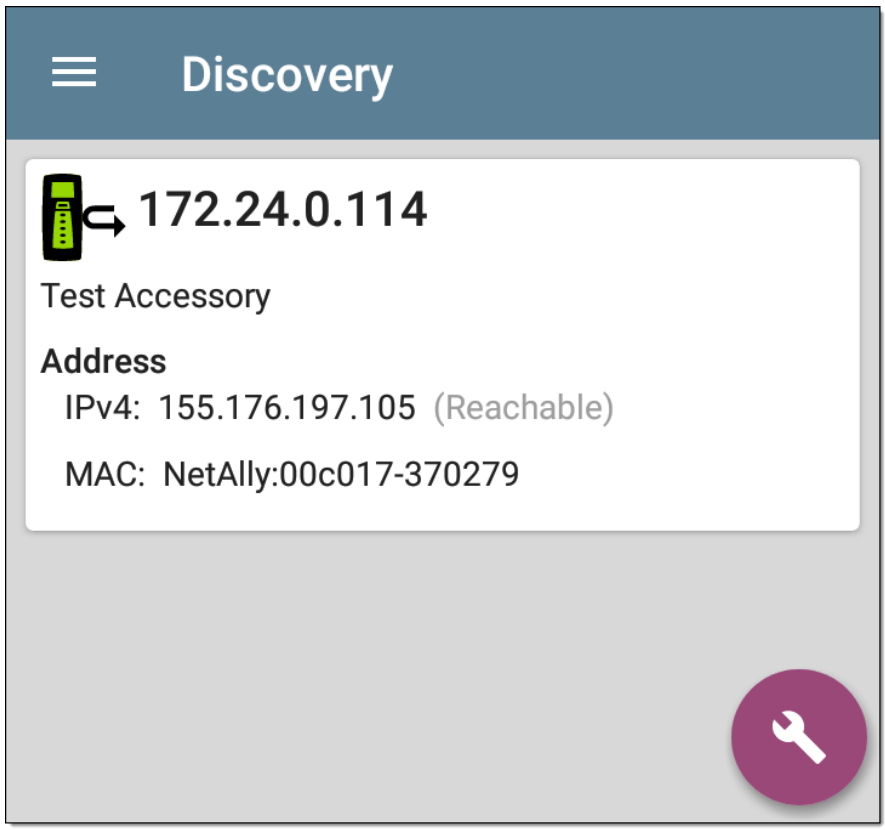


Test Accessories in Discovery

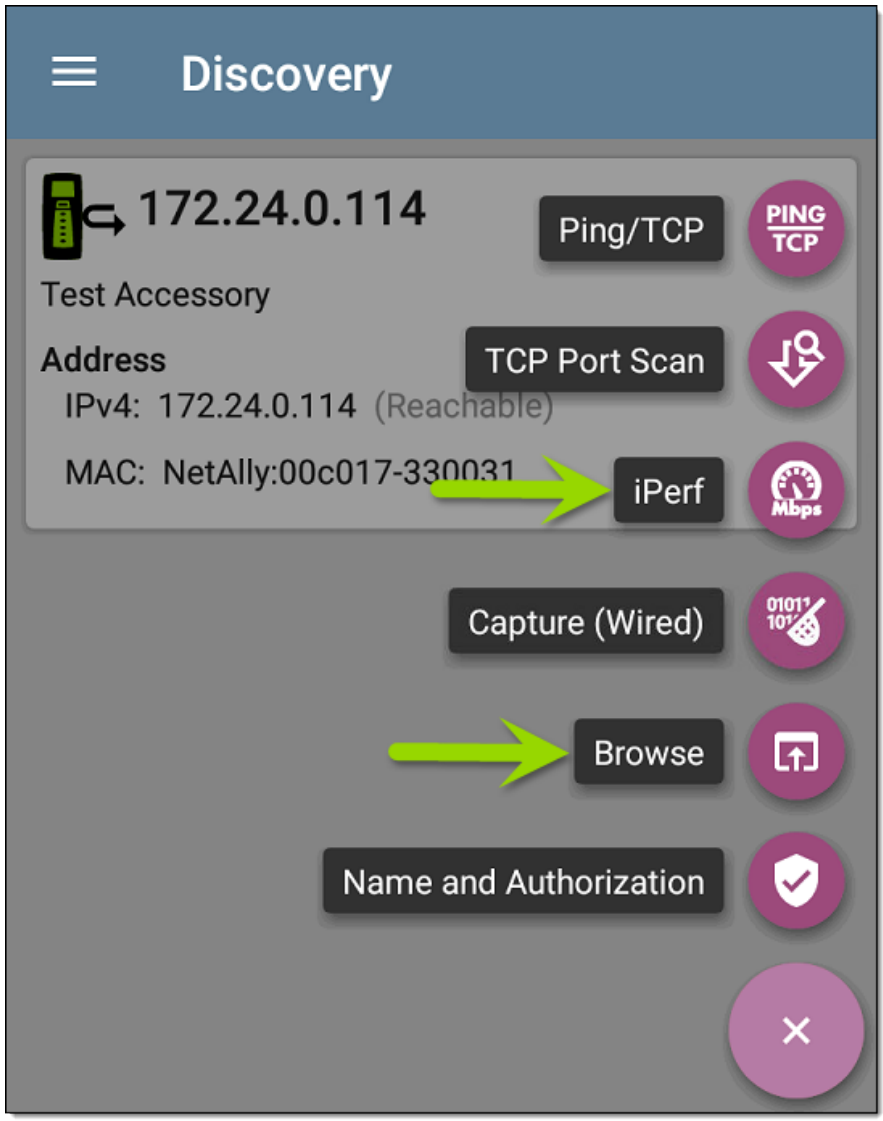
You can start an iPerf test from the Details screen for a Test Accessory in the Discovery app using the floating action button.

1. Open the Discovery app, and select an active **Test Accessory** from the main

Discovery list to open its Details screen.



2. Tap the floating action button (FAB) to open the action menu.



3. Select the **iPerf** app button to open the iPerf app with the IP address populated from the Test Accessory in Discovery.

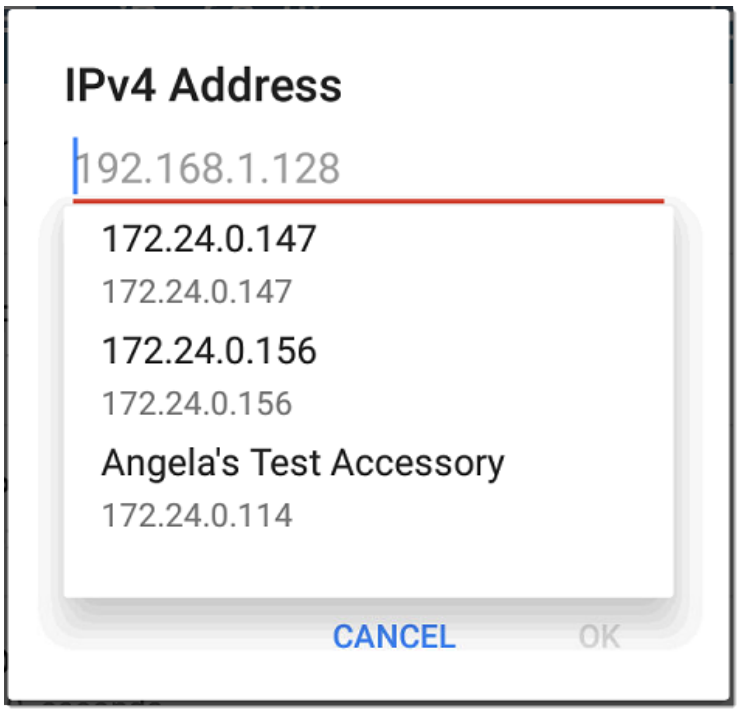
   NOTE: You can also select **Browse** in the FAB menu to open the Test Accessory's Web Interface, where you can view its status and configure its settings.

Configuring iPerf Settings

To configure the iPerf test settings manually, open the settings on the iPerf screen.

Tap each field to enter or revise selections as needed. Changed settings are automatically applied. When you finish configuring, tap the back button to return to the iPerf test screen.

IPv4 Address: Tap the field to enter or select the IPv4 address of the target iPerf server. Only IPv4 addresses are allowed for iPerf testing.



A drop-down list in the IPv4 Address dialog shows all the Test Accessories the LRAT has discovered through the discovery process, as

well as any Test Accessories that are claimed to the same Link-Live organization as your LRAT.

> NOTE: Clear the address field in the dialog to see the full list of discovered Test Accessory addresses.

Port: The default iPerf3 port number is 5201. Tap the field to enter a different port number.

> NOTE: The iPerf port number entered here must match the port number used by your iPerf server. If needed, consult the Test Accessory User Guide (NetAlly.com/products/TestAccessory).

Duration: This setting is the length of time for one direction, Upstream or Downstream, of the iPerf test. If the Direction setting below is set to both Upstream/Downstream, the total test time is twice the value set here. Tap the field to select a new duration or enter a custom value. The default is 10 seconds.

Protocol: TCP is the default protocol. Tap the UDP selector to switch to UDP.

> NOTE: iPerf tests running the TCP protocol automatically run at the fastest rate possible.

When running a UDP protocol test, the iPerf app attempts to run at the selected Bandwidth.

Direction: You can run an iPerf test Upstream, Downstream, or both. The default is Upstream and Downstream. Tap this field to set the test for only one direction.

Upstream and Downstream Bandwidth: These fields only appear if the **UDP Protocol** is selected. They specify the desired target bandwidth for the iPerf Test using the UDP protocol.

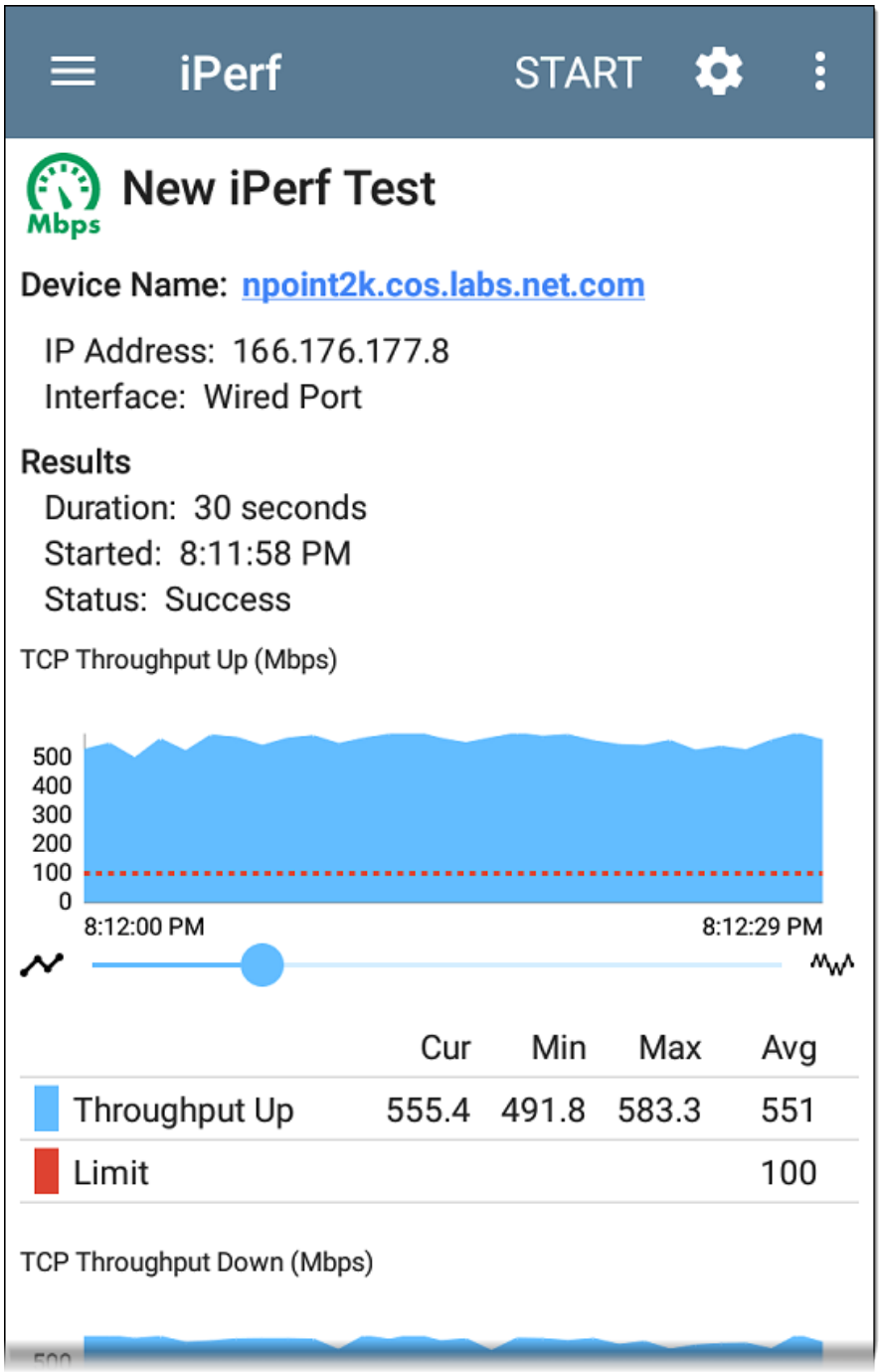
Upstream and Downstream Thresholds: Thresholds are the values the LRAT uses to grade the test as **Pass** or **Fail**. iPerf thresholds are throughput rates. The default is 10 Mbps. Tap the threshold fields to select a different value or enter a custom one.

Back to Title and Contents

Running an iPerf Test

Ensure that you have an active link on the Interface (Test Port) from which you are running the iPerf test. The Wired test port requires that an AutoTest Wired Profile (which runs automatically) has run to establish a link.

Tap the **START** button on the main iPerf screen to begin testing.



Test characteristics and status are displayed at the top of the iPerf results screen while the lower part of the screen displays a real-time graph of the TCP or UDP Upload and/or Download speeds.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

Device Name: Hostname or address of the iPerf server or Test Accessory.

IP Address: IPv4 address of the iPerf server.

Interface: The LRAT Test Port from which the test is running.

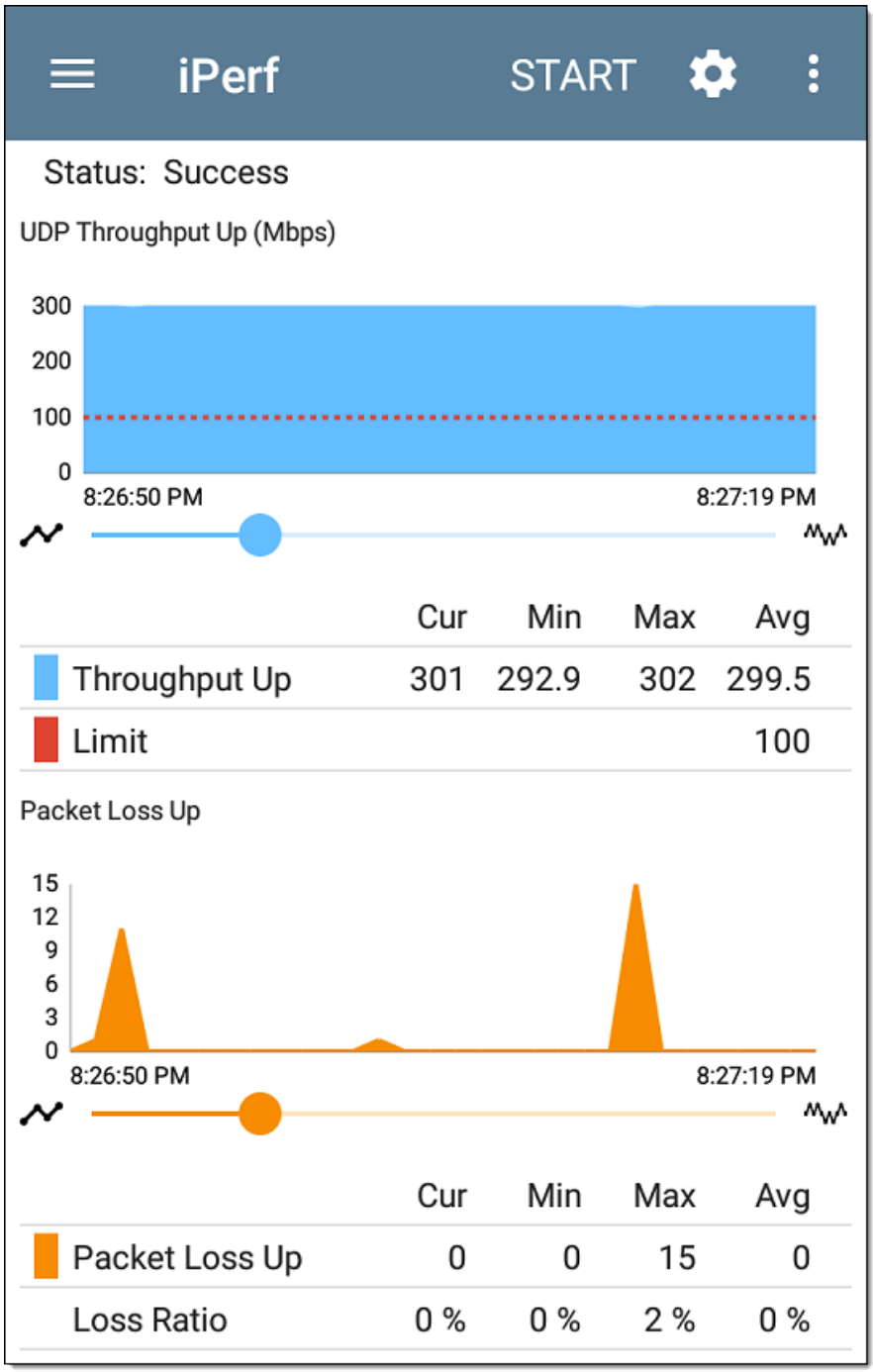
Results

- **Duration**: Configured Duration from the iPerf settings
- **Started**: Time the test started
- **Status**: Success or failure status of the test.

TCP/UDP Throughput Up and Down graphs: The iPerf graphs plot the throughput rate to (Up) or from (Down) the iPerf server in Mbps.

The table below each graph displays the Current, Minimum, Maximum, and Average rates.

Limit: This is the **Threshold** from the iPerf app's settings. The threshold value is also displayed on the graph as a red dotted line.



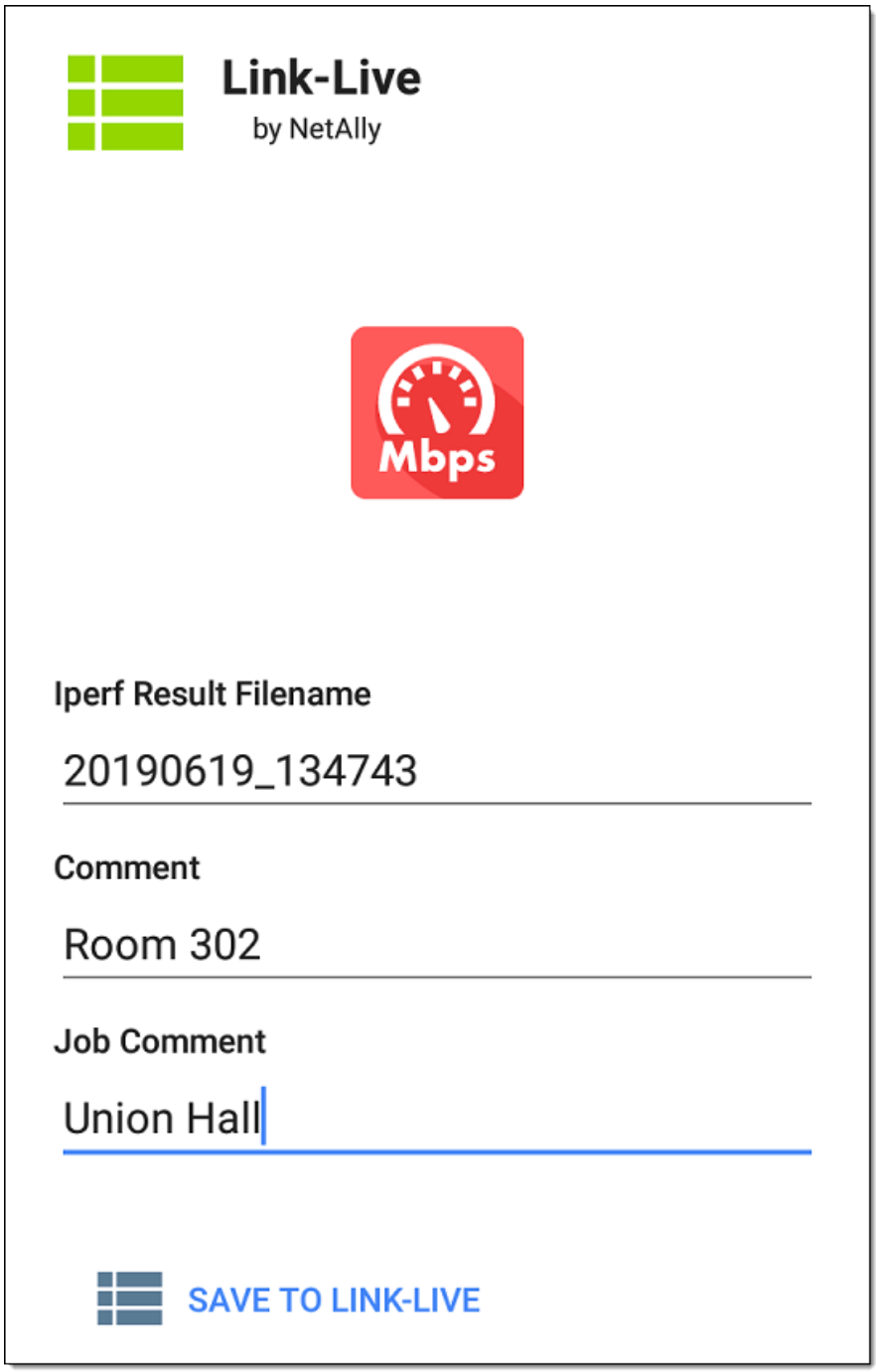
UDP Packet Loss Up and Down graphs: When running a UDP protocol test, the iPerf results also display graphs and tables of Packet Loss. Values for the number and percentage of packets lost are displayed in the table below the

graph. The Packet Loss Up graph and table do not display measurements until results are received from the iPerf server at the end of the upstream test.

Note that the Packet Loss Up number could be much less than the Packet Loss Down number.

Uploading Results to Link-Live

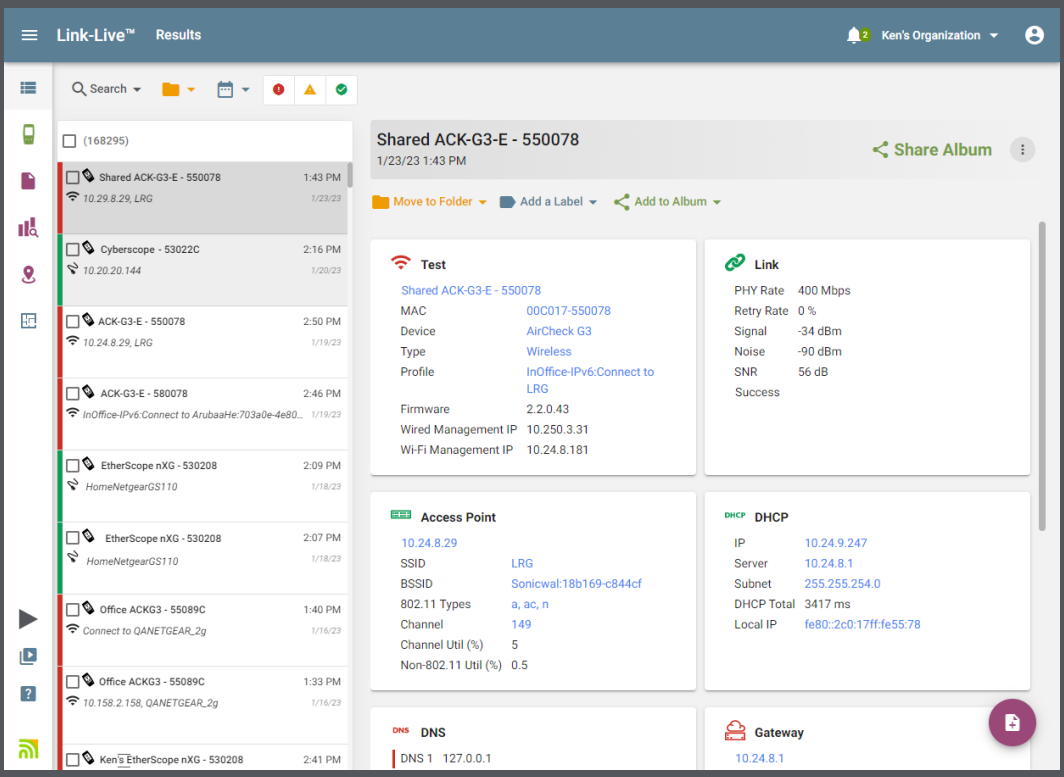
To send your iPerf results to the Link-Live website, tap the action overflow button  at the top right of the iPerf screen, and then tap **Upload to Link-Live**.



The Link-Live sharing screen opens and allows you to revise the auto-generated file name and attach comments to the iPerf result, which is displayed on the Results page on Link-Live.com.

Back to Title and Contents

Link-Live Cloud Service



Link-Live Cloud Service is a free, online system for collecting, tracking, organizing, analyzing, and reporting your test results. AutoTest results are automatically uploaded once your LRAT 3000-4000 is claimed.

The comprehensive LRAT 3000-4000 offers more features for analyzing your network in Link-Live than previous testers. Claim your LRAT to Link-Live.com to access these functions:

- Check for software updates and update your LRAT 3000-4000 software.
- Download third-party applications from the NetAlly App Store to use on your LRAT.
- Automatically upload AutoTest results each time you run AutoTest.
- Attach test and Job comments to Link-Live uploads, and automatically sort your results and files into folders in Link-Live.
- Upload test, discovery, and analysis results from the NetAlly apps, including Discovery, Path Analysis, and iPerf. See Link-Live and Testing Apps for more about uploading.

Getting Started in Link-Live Cloud Service

To start, create a user account at Link-Live.com, and sign in. You can open the Link-Live website in the LRAT's web browser to create and manage your account.

Claiming the Unit

On Link-Live.com

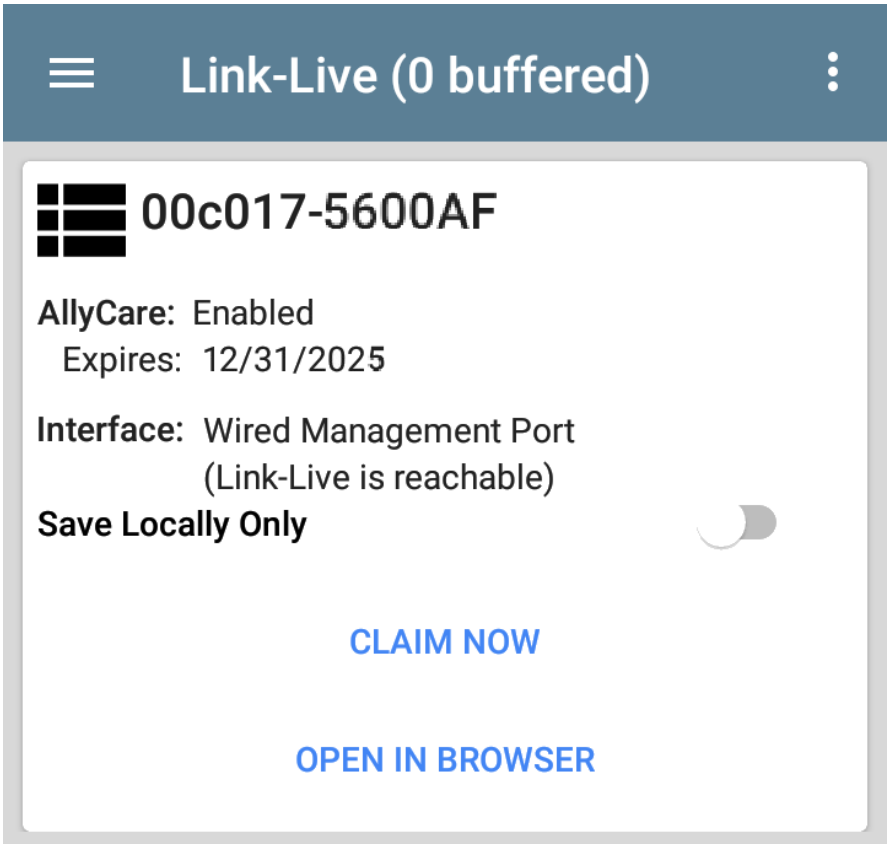
1. The first time you sign in to Link-Live.com, a pop-up window appears, prompting you to claim a device.

   If you already have a user account and other devices claimed to Link-Live, navigate to the **Units** page from the left side navigation drawer, and then click the **Claim Unit** button  at the lower right corner of the screen .

2. Then, select the LinkRunner AT 3000/4000 image, and follow the claiming instructions on the Link-Live website.

On the LRAT 3000-4000 Unit

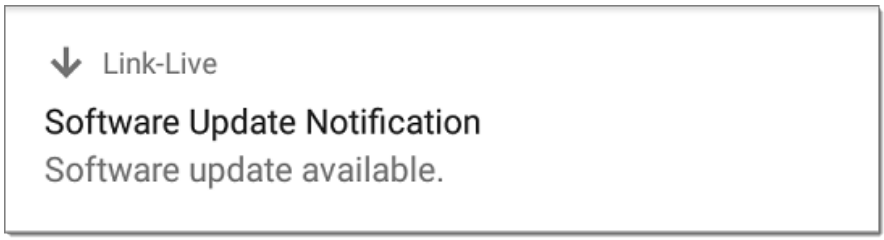
1. Open the Link-Live app. Your unit's MAC address is displayed.



2. Tap **CLAIM NOW** on the Link-Live app screen.
3. When prompted by the instructions on the Link-Live website, enter the MAC address.

After you claim your LRAT 3000-4000 to Link-Live, a software update may be available. If so, a notification appears in the Status Bar . Open

the Top Notification Panel, and select the notification to update your unit.



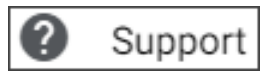
See Updating Software for more information.

After Claiming

Once your LRAT is claimed to the Link-Live Cloud Service, it automatically uploads your AutoTest results each time you run AutoTest. You can also upload a test comment and a picture with your test results using the floating action buttons (FABs) for the Wired Test Results. You can automatically sort your results into folders in Link-Live using test and Job comments.

If your LRAT is not connected to an active network, any test results, comments, or images are stored in memory (buffered) and uploaded once a connection is established.

For more information on how to the use the Link-Live.com website, click or tap the

navigation menu icon  at the top left of the Link-Live.com pages, and select 

.

Unclaiming

You may need to unclaim your unit from Link-Live to transfer it to another user or if you no longer want to send data to Link-Live.com.

To unclaim your LRAT from Link-Live, tap the navigation drawer icon  in the Link-Live app, tap About, and then tap **UNCLAIM**.

AllyCare Code

The AllyCare Code button appears at the bottom of the About screen next to the Export Logs button if your unit is not claimed.

Tap **AllyCare Code** to open a dialog to enter an AllyCare Activation Code.

Private Link-Live Settings

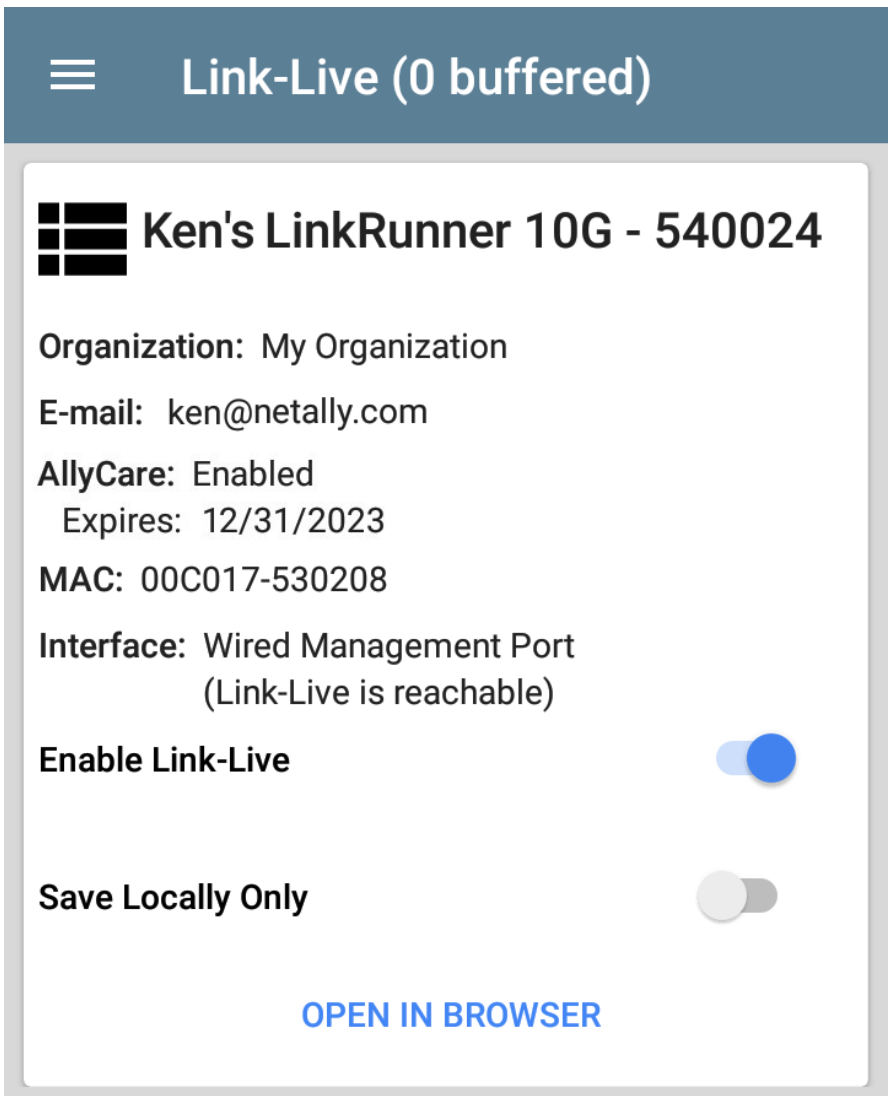
Use these settings only when your organization has deployed a private instance of Link-Live. Consult your IT organization for setting details.

Back to Title and Contents

Link-Live App Features

The main Link-Live app screen on your LRAT 3000-4000 facilitates the claiming process, displays Link-Live related information, and allows you to enable or disable Link-Live.com uploads as needed.

Link-Live App Screen



The LRAT unit's name that displays on the Link-Live.com is shown to the right of the Link-Live icon  . You can change this name on the Link-Live.com **Units**  page.

Organization is the Link-Live organization where the unit is claimed.

E-mail is the first e-mail address assigned to the unit, which receives test result notification emails.

The Organization and Email address shown here are assigned on the Link-Live.com website. The fields displayed in LRAT's Link-Live app are informational.

AllyCare indicates the status of NetAlly's optional AllyCare services. See NetAlly.-com/Support for more information.

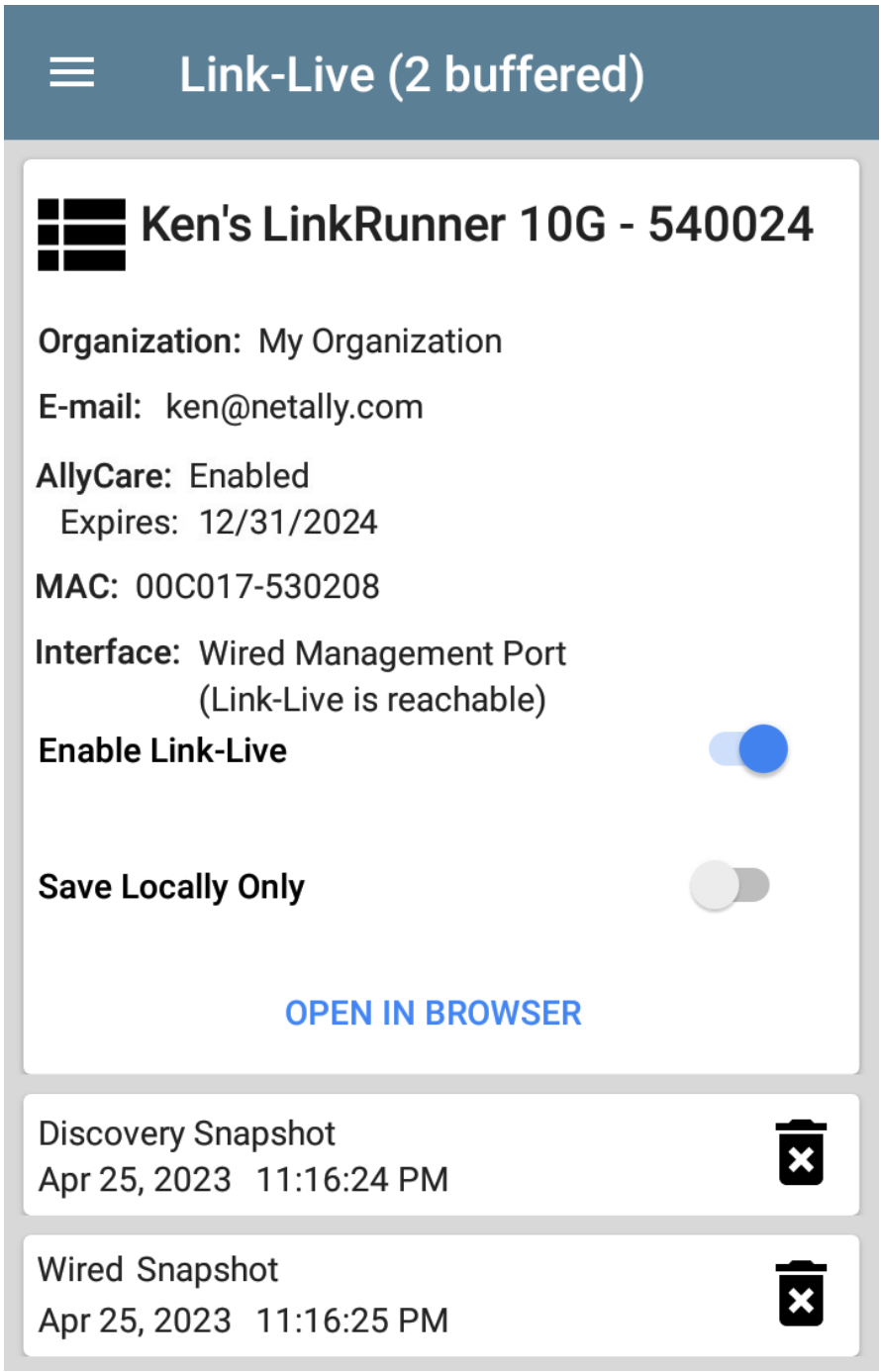
Interface shows which network interface Link-Live currently uses to post results and the network status.

The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the LRAT cannot upload test results or check for software updates. The

Upload to Link-Live options do not appear in the testing apps.

Tap the **OPEN IN BROWSER** link to open Link-Live.com on the LRAT's web browser.

The "(# buffered)" in the Link-Live screen header indicates the number of files stored in the device memory when no active network connection is available. The buffered file types are listed below the main app card.

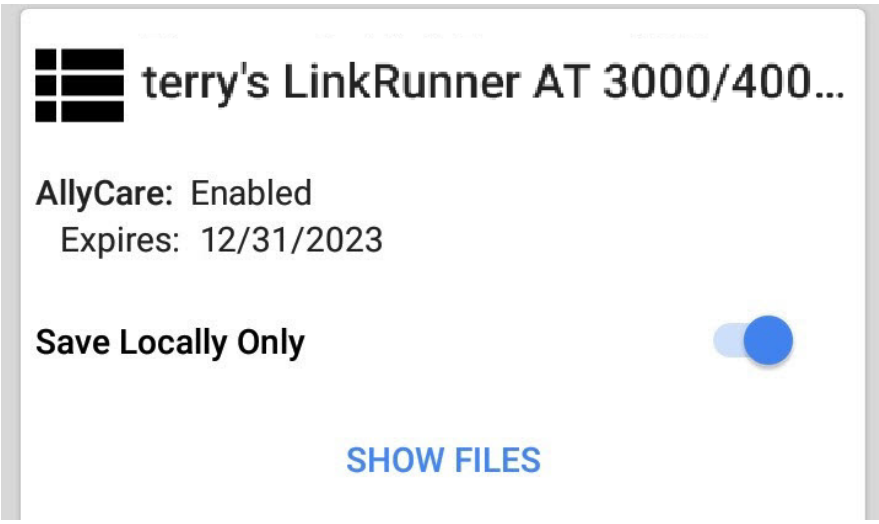


The buffered files displayed automatically upload to Link-Live.com once your LRAT connects to an active network.

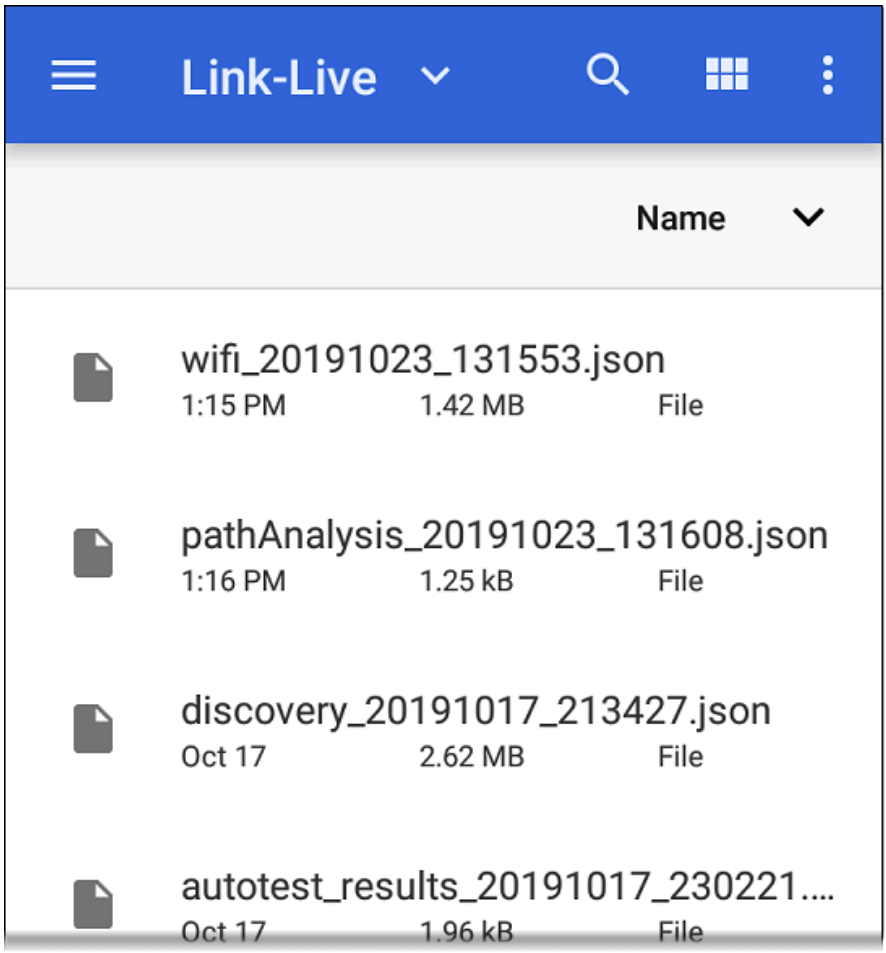
Saving Locally Only

If you do not want to send your results to the Link-Live website, you can still save results locally to your LRAT as JSON files.

Tap the **Save Locally Only** toggle field in the Link-Live app to save the JSON files to your unit.



Select **SHOW FILES** to open the Files app. The .json files are saved in the **Downloads > TestResults** folder.



See the Managing Files topic for an overview of the Files app.

You can transfer the JSON files to a PC for analysis, or you can download a JSON viewer app from the App Store ▶ on your LRAT.

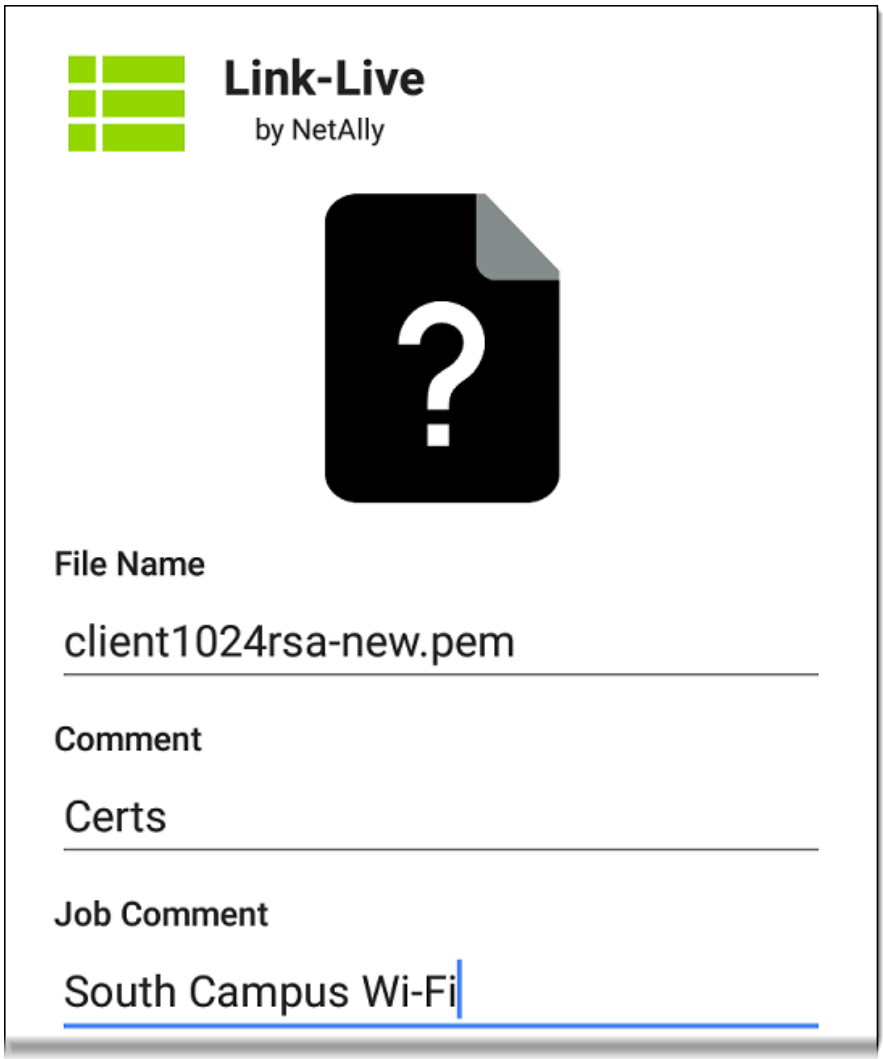
With **Save Locally Only** enabled, options for uploading or saving to Link-Live (described in the Link-Live and Testing Apps section below) still display in the NetAlly testing apps. However, the results are saved to the internal Link-Live

storage folder, and not uploaded to Link-Live.com.

Job Comment

The left-side navigation drawer for the Link-Live app lets you enter or change the Job Comment. The **Job Comment** attaches to all test results and files uploaded to Link-Live, until you change or delete it. In contrast, other **Comments**, like those attached to WiredAutoTest results or Discovery results, are only attached to one set of test results or uploaded file.

Both comment types appear on Link-Live sharing screens like the one below:



To enter or change the Job Comment in the Link-Live app:

1. With the Link-Live app open, tap the menu icon or swipe right from the left side of the screen.

2. Tap the **Job:** field.
3. Enter a comment in the dialog box.
4. Tap **SAVE**.

Note that the **Job Comment** field appears in other Link-Live sharing screens, allowing you to change it from multiple locations on the LRAT. No matter where you change the Job Comment, it is updated everywhere on the unit.

Software Updates

The left-side navigation drawer for the Link-Live app also lets you check for and download any available software updates. See Updating Software in the Software Management chapter.

System Notifications

Link-Live can send messages to your test unit. They are displayed in the system Notification Panel.

Link-Live and Testing Apps

Once your unit is claimed, the Link-Live app works with several of the testing apps to upload test results, discovery and analysis data, comments, and images to the Link-Live website. Link-Live.com categorizes the uploads from different apps on corresponding webpages, as shown below:

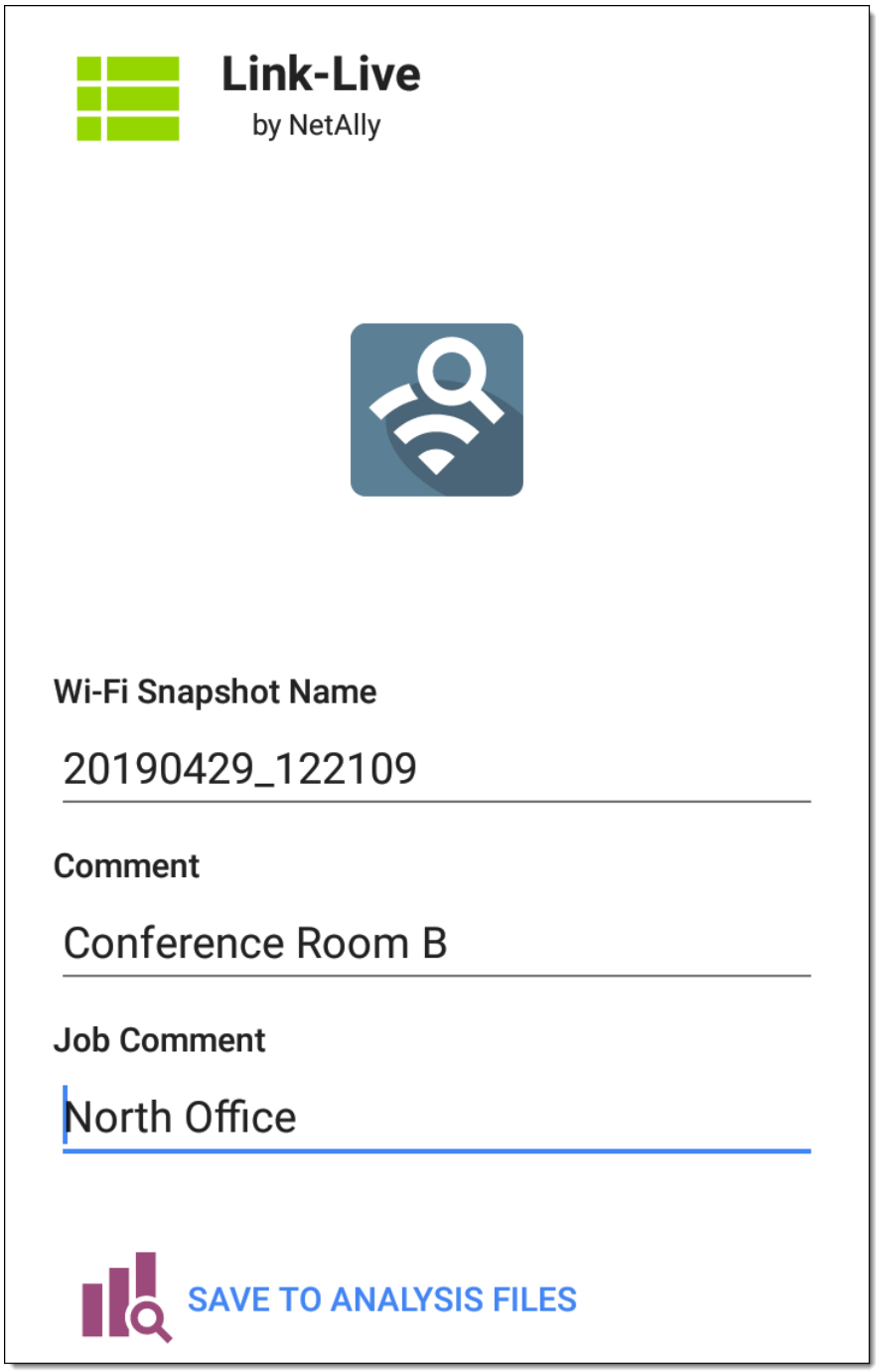
Link-Live Webpage	App Uploads
Results	AutoTest, Performance, iPerf, and Cable Test results Images, connect logs, and other files when saved to a test result
Uploaded Files	Captures, images, connect logs, and other file types
Analysis	Discovery and Path Analysis results

If your unit is not claimed to Link-Live.com or if Link-Live is disabled on the app screen, the links and buttons for uploading to Link-Live in the testing apps do not appear.

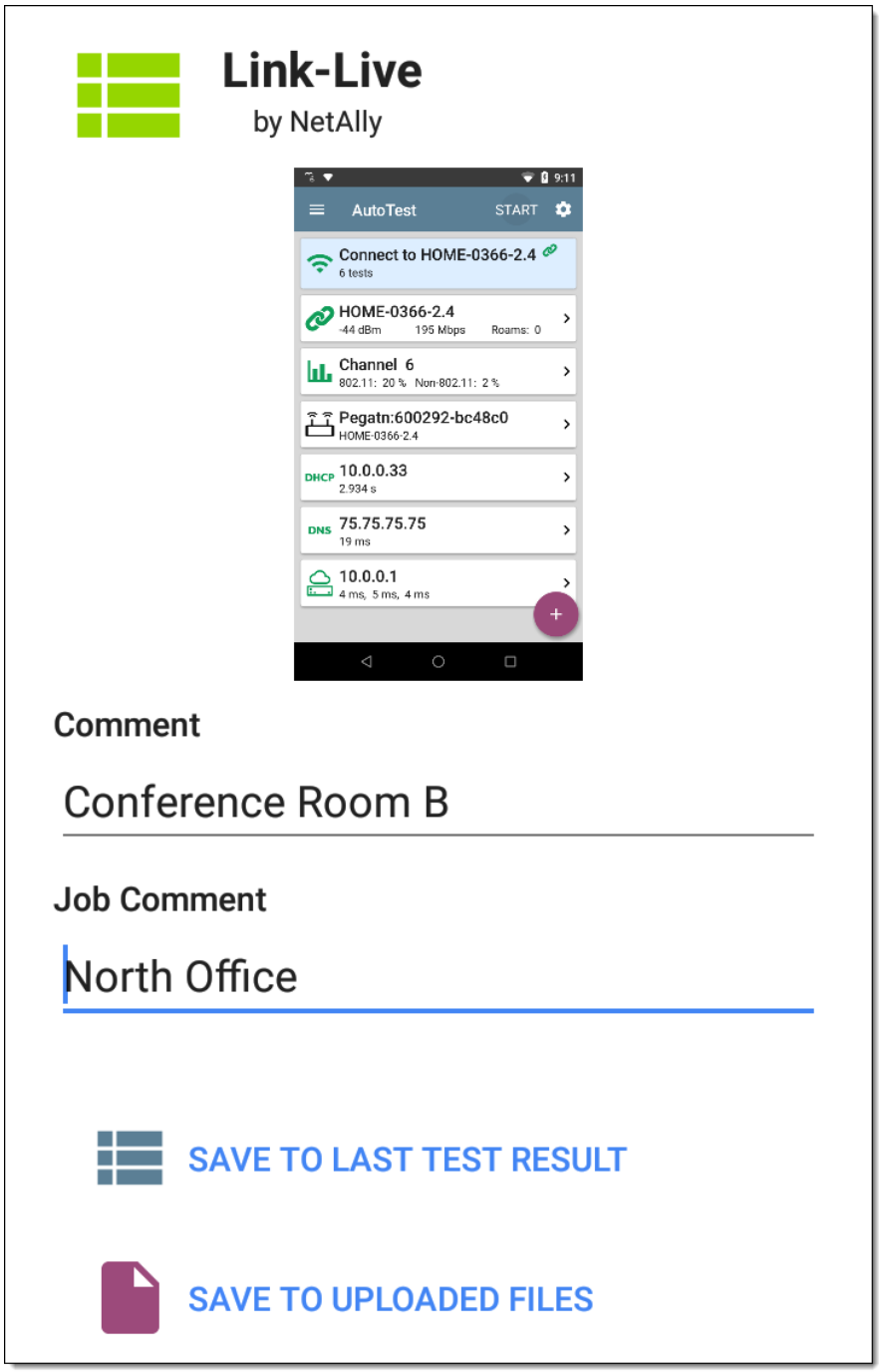
Link-Live Sharing Screens

Whenever you select a button or link, like those above, to Upload, Save, or Share to Link-Live, a Link-Live sharing screen appears with the appropriate options for the data type.

For example, the Link-Live sharing screen for Discovery app data allows you to upload to the Analysis page on Link-Live.com.



The Link-Live sharing screen for a screenshot or other image allows you to attach it to the most recently run test result (AutoTest, Performance, iPerf, or Cable Test) on the Results page, or to the Uploaded Files page on Link-Live.com.

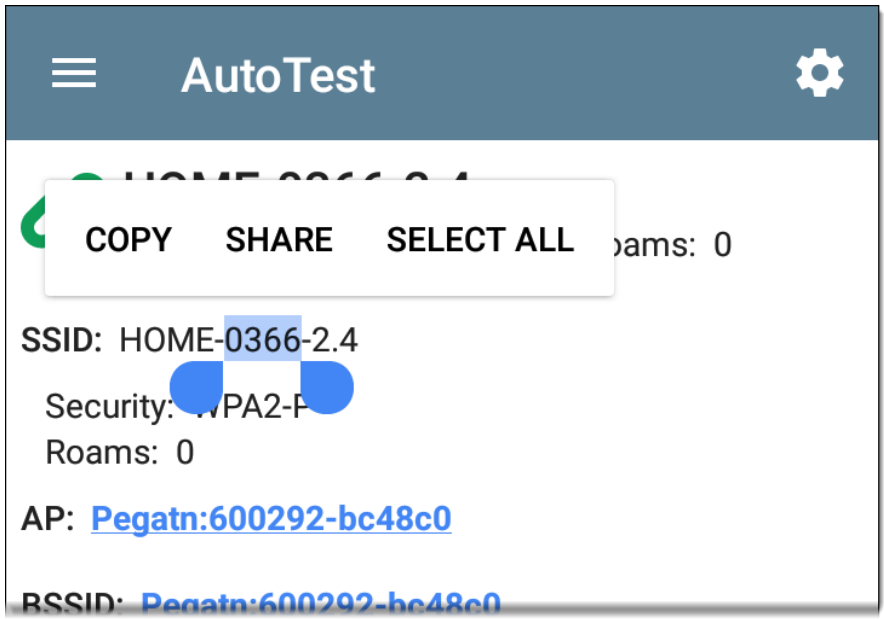


Remember, the regular **Comment** field uploads only to the current result or file, while the **Job Comment** field uploads with all results and files until you change it.

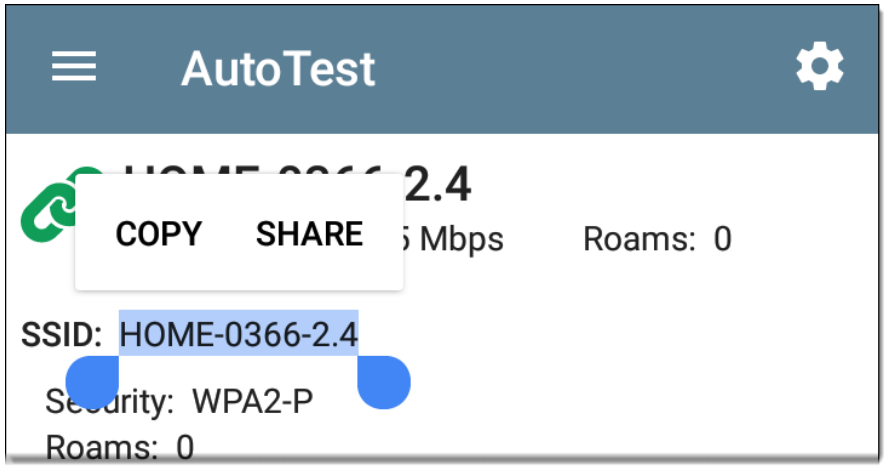
Sharing a Text File to Link-Live

You can also select and share text by long pressing text on the unit's screen. Text files are attached to the last test results on Link-Live.com.

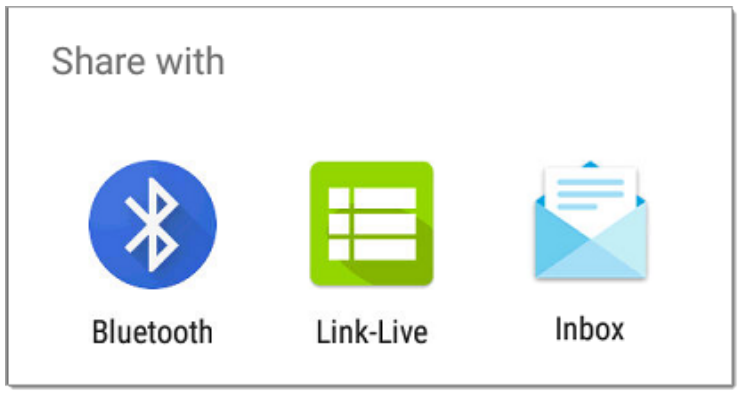
1. Long press a text string to select it.



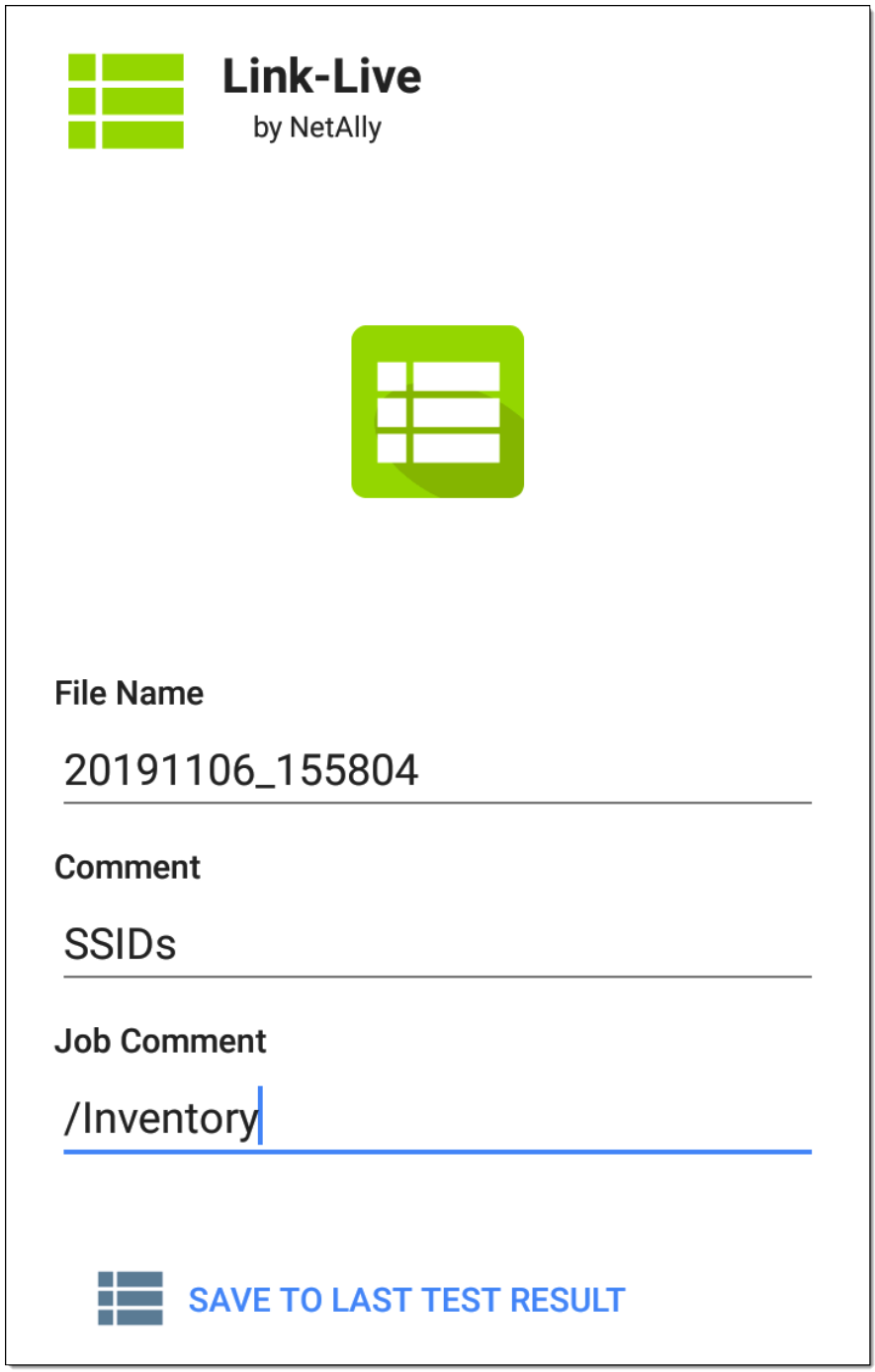
2. Tap **Select All** if needed.



3. Tap **SHARE**.



4. Select the Link-Live icon to open the Link-Live sharing screen.



5. Enter any comments as needed, and then tap **SAVE TO LAST TEST RESULT**.

Back to Title and Contents

Back to Title and Contents

Specifications and Compliance

This chapter contains device specifications and required compliance information.

LRAT 3000-4000 Specifications

General

Dimensions	4.02 in x 7.72 in x 1.65 in (10.2 cm x 19.6 cm x 4.2 cm)
Weight	1.06 lbs (0.48 kg)
Battery	Rechargeable lithium-ion battery pack (3.63 V, 9.75 Ah, 36.39 Wh)
Battery Run Duration, Charge Time	Typical run duration: 9 hours Typical charge time: 3 hours
Display	5.0-inch color LCD with capacitive touchscreen (720 x 1280 pixels)
Host Interfaces	RJ-45 Ethernet test port RJ-45 cable test port (1) USB Type-A Port (1) USB Type-C On-the-Go Port
Memory	Approximately 8 GB available for storing test results and user applications

Charging Adapter	USB Type-C 65-W adapter: AC Input Power 100-240 V, 50-60 Hz; DC Output Power 15 V (3 A)
PoE Charging	802.3 af/at
Supported IEEE Standards	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 (Battery Status Indicator)

Environmental Specifications

Operating Temperature	32°F to 113°F (0°C to +45°C) NOTE: The battery will not charge if the internal temperature of the unit is above 113°F (45°C).
Operating relative humidity (% RH without condensation)	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)

Storage Temperature	-4°F to 140°F (-20°C to +60°C)
Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	IEC 61010-1:2010: Pollution degree 2
Altitude	Operating: 4,000 m; Storage: 12,000 m
EMC	IEC 61326-1: Basic Electromagnetic Environment CISPR 11: Group 1, Class A

Group 1: Equipment has intentionally generated and/or uses conductively-coupled radio frequency energy that is necessary for the internal function of the equipment itself.

Class A: Equipment is suitable for use in all establishments other than domestic and those directly connected to a low-voltage power supply network that supplies buildings used for domestic purposes. There may be potential difficulties in ensuring electromagnetic compatibility in other environments due to conducted and radiated disturbances.

⚠ **CAUTION:** Changes or modifications not expressly approved by the party responsible for

compliance could void the user's authority to operate the equipment.

	Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.
	Conforms to relevant Australian Safety and EMC standards.
	Listed by the Canadian Standards Association.
	Conforms to relevant European Union directives.
	Complies with United Kingdom and European Economic Area radiation exposure limits.
	Conforms to relevant South Korean EMC Standards.

Additional South Korean EMC Standards Information

Electromagnetic Compatibility. Applies to use in Korea only. Class A Equipment (Industrial Broadcasting & Communications Equipment) [1] [1] This product meets requirements for industrial (Class A) electromagnetic wave equipment and the seller or user should take notice of it. This equipment is intended for use in business environments and is not to be used in homes.

Caution: Any changes or modifications made to the equipment without the approval of man- ufacturer could void the user’s authority to operate this equipment.

The device is for indoor use. This equipment may only be operated indoors. Operation outdoors is in violation of 47 U.S.C. 301 and could subject the operator to serious legal penalties.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is

permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Innovation, Science and Economic Development Canada

Innovation, Sciences et Développement économique Canada

Industry Canada Class A emission compliance statement: This Class A digital apparatus complies with Canadian ICES-003. Avis de conformité à la réglementation d'Industrie Canada Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada. This device is not capable of transmitting in 5600-5650 MHz. This restriction is for the protection of Environment Canada's weather radars operating in this band.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired

---

operation.

L’exploitation est autorisée aux deux conditions suivantes: 1. L’appareil ne doit pas produire de brouillage; 2. L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

Class A: Equipment is suitable for use in all establishments other than domestic and those directly connected to a low-voltage power supply network that supplies buildings used for domestic purposes. There may be potential difficulties in ensuring electromagnetic compatibility in other environments due to conducted and radiated disturbances.

This device complies with the following EU Directives: Directives 2014/53/EU, 2014/35/EU, and 2014/30/EU.

Accessory Information:

Adapter Model No.: FSP065-A1BR3

Input: AC 100-240 V, 50/60 Hz 1.2 A

Output: DC 15 V, 3 A

Back to Title and Contents

Back to Title and Contents

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W