



# LINKRUNNER<sup>®</sup> 10G

## 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](#)



[Ping/TCP](#)



[Capture](#)



[Cable](#)



[Discovery](#)



[Path Analysis](#)



[Performance](#)



[iPerf](#)



[LANBERT™](#)



[Link-Live](#)



[App Store](#)

# Contents

<b>Contact Us</b> .....	<b>13</b>
<b>Introduction</b> .....	<b>14</b>
<b>How to Use this Guide</b> .....	<b>15</b>
<b>Buttons and Ports</b> .....	<b>19</b>
<b>Charging and Power</b> .....	<b>24</b>
PoE Charging .....	24
<b>Safety and Maintenance</b> .....	<b>27</b>
<b>Legal Notification</b> .....	<b>30</b>
<b>Home and System Interface</b> .....	<b>31</b>
<b>Home Screen</b> .....	<b>32</b>
<b>Navigating the System</b> .....	<b>34</b>
<b>System Status Bar and Notifications</b> ...	<b>38</b>
Notification Panel .....	38
<b>Apps Screen and Store</b> .....	<b>41</b>
<b>Device Settings</b> .....	<b>45</b>
Quick Settings Panel .....	46
<b>Connecting to Wi-Fi</b> .....	<b>49</b>
Captive Portals .....	52
Configuring Wi-Fi Connections With Enterprise Security .....	53
<b>Sharing</b> .....	<b>62</b>

Sharing a Screenshot .....	65
Changing the Device Language .....	67
<b>LinkRunner 10G Settings and Tools .</b>	<b>69</b>
<b>Navigation Drawer</b> .....	<b>70</b>
About Screen .....	71
Exporting Logs .....	72
Exporting Settings for All Apps .....	72
<b>Test and Management Ports</b> .....	<b>74</b>
Test Ports .....	75
Selecting Ports .....	77
<b>Test and Port Status Notifications</b> .....	<b>80</b>
Test Port Notifications .....	81
Management Port Notifications .....	82
Discovery Notifications .....	83
PoE .....	84
VNC/Link-Live Remote .....	84
<b>LinkRunner 10G General Settings</b> .....	<b>85</b>
Wired .....	87
Management .....	89
Preferences .....	92
<b>Trending Graphs</b> .....	<b>94</b>
<b>Common Icons</b> .....	<b>98</b>

<b>Floating Action Button (FAB) and Menu</b>	<b>99</b>
<b>Common Tools</b>	<b>101</b>
Web Browser/Chromium	101
Telnet/SSH	101
Camera and Flashlight	103
<b>Software Management</b>	<b>104</b>
<b>Managing Files</b>	<b>105</b>
Files Application	105
How to Move or Copy a File	108
Using a Micro SD Card	109
Using a USB Drive	110
Ejecting Storage Media	112
Using a USB Type-C to USB Cable	112
<b>Updating Software</b>	<b>115</b>
<b>Remote Access</b>	<b>120</b>
Using VNC	121
Using Link-Live Remote	122
<b>Managing NetAlly App Settings</b>	<b>124</b>
Resetting Testing App Defaults	124
Saving App Settings and Configurations	128
Importing and Exporting Settings	132



Importing and Exporting Settings for All Apps .....	142
<b>Resetting LinkRunner 10G Factory Defaults .....</b>	<b>144</b>
<b>LinkRunner 10G Testing Applications .....</b>	<b>147</b>
<b>AutoTest App and Profiles .....</b>	<b>148</b>
<b>AutoTest Overview .....</b>	<b>150</b>
<b>Managing Profiles and Profile Groups .....</b>	<b>152</b>
Factory Default Profiles .....	152
Adding New Profiles .....	153
Profile Groups .....	155
Creating New Profile Groups .....	160
Importing and Exporting AutoTest Profiles .....	163
<b>Main AutoTest Screen .....</b>	<b>164</b>
<b>Periodic AutoTest .....</b>	<b>166</b>
Periodic AutoTest Settings .....	166
Running Periodic AutoTest .....	168
<b>Wired AutoTest Profiles .....</b>	<b>171</b>
<b>Wired Profile Results .....</b>	<b>176</b>
PoE Test Results .....	178

Wired Link Test Results .....	181
802.1X Test Results .....	187
VLAN Test Results .....	189
Switch Test Results .....	192
Wired Profile FAB .....	199
<b>Wired Profile Settings .....</b>	<b>203</b>
PoE Test Settings .....	204
Wired Connection Settings .....	207
VLAN Settings .....	214
Stop After .....	216
HTTP Proxy .....	217
<b>DHCP, DNS, and Gateway Tests .....</b>	<b>219</b>
DHCP or Static IP Test .....	220
DNS Test .....	232
<b>Test Targets for Wired AutoTests .....</b>	<b>241</b>
Adding and Managing Test Targets ...	242
AutoTest TCP Connect Test .....	255
FTP Test .....	268
<b>Ping/TCP Test App .....</b>	<b>278</b>
<b>Ping/TCP Settings .....</b>	<b>279</b>
Populating Ping/TCP from Another App .....	279

Configuring Ping/TCP Settings	
Manually .....	282
Running Ping/TCP Tests .....	286
<b>Capture App .....</b>	<b>290</b>
Capture Settings .....	291
Running and Viewing Captures .....	295
<b>Discovery App .....</b>	<b>299</b>
Introduction to Discovery .....	301
Main Discovery List Screen .....	303
Searching the Discovery List .....	306
Filtering the Discovery List .....	308
Sorting the Discovery List .....	311
Security Auditing – Batch	
Authorization .....	313
Refreshing Discovery .....	318
Uploading Results to Link-Live .....	319
Discovery Details Screens .....	321
Top Details Card .....	323
Lower Cards in Device Details .....	329
Problems .....	331
Addresses .....	332
TCP Port Scan .....	334

VLANs .....	336
Interfaces .....	337
SNMP .....	343
Connected Devices .....	344
Resources .....	345
SSIDs .....	346
Discovery App Floating Action Menu .	348
<b>Device Types .....</b>	<b>353</b>
Routers .....	354
Switches .....	355
Unknown Switches .....	356
Network Servers .....	357
Hypervisors .....	358
Virtual Machines .....	359
Wi-Fi Controllers .....	360
Access Points (APs) .....	361
Wi-Fi Clients .....	362
VoIP Phones .....	362
Printers .....	364
SNMP Agents .....	365
Network Tools .....	366
Hosts/Clients .....	367
<b>Device Names and Authorization .....</b>	<b>370</b>

Assigning a Name and Authorization to a Device .....	370
<b>Discovery Settings .....</b>	<b>382</b>
Active Discovery Ports .....	385
Extended Ranges .....	385
ARP Sweep Rate .....	390
Refresh Interval .....	391
SNMP Configuration .....	391
<b>Problem Settings .....</b>	<b>403</b>
<b>TCP Port Scan Settings .....</b>	<b>406</b>
<b>Path Analysis App .....</b>	<b>409</b>
<b>Introduction to Path Analysis .....</b>	<b>410</b>
<b>Path Analysis Settings .....</b>	<b>411</b>
Populating Path Analysis from Another App .....	411
Configuring Path Analysis Manually ..	411
<b>Running Path Analysis .....</b>	<b>414</b>
Path Analysis Results and Source LinkRunner Cards .....	416
Layer 3 Hops .....	419
Layer 2 Devices .....	424
Uploading Results to Link-Live .....	429
<b>Performance Test App .....</b>	<b>431</b>

<b>Introduction to Performance Testing</b>	<b>433</b>
<b>Performance Test Settings</b>	<b>435</b>
Saving Custom Performance Tests	436
Configuring the Source LinkRunner	
10G	441
<b>Configuring Performance Endpoints</b>	<b>458</b>
OneTouch 10G Performance Peer	459
LinkRunner G2 Reflector	461
LinkRunner AT Reflector	463
NPT Reflector Software	465
<b>Running a Performance Test</b>	<b>467</b>
Performance Test Results	468
Performance Service Detailed Results	470
Uploading Results to Link-Live	478
<b>Running LinkRunner 10G as a Performance Peer</b>	<b>482</b>
<b>iPerf Test App</b>	<b>486</b>
<b>iPerf Settings</b>	<b>488</b>
Saving Custom iPerf Settings	488
Test Accessories in Discovery	489
Configuring iPerf Settings	492
<b>Running an iPerf Test</b>	<b>496</b>

Uploading Results to Link-Live .....	500
<b>LANBERT™ Test App .....</b>	<b>502</b>
<b>LANBERT Settings .....</b>	<b>503</b>
Configuring LANBERT Generator Settings .....	503
Configuring LANBERT Loopback Settings .....	508
<b>Running a LANBERT Test .....</b>	<b>509</b>
Uploading Results to Link-Live .....	516
<b>Link-Live Cloud Service .....</b>	<b>519</b>
<b>Getting Started in Link-Live Cloud     Service .....</b>	<b>521</b>
Claiming the Unit .....	521
After Claiming .....	523
Unclaiming .....	524
AllyCare Code .....	525
Private Link-Live Settings .....	526
<b>Link-Live App Features .....</b>	<b>527</b>
Saving Locally Only .....	531
Job Comment .....	533
Link-Live and Testing Apps .....	536
Link-Live Sharing Screens .....	537

Sharing a Text File to Link-Live .....	540
<b>Cable Test App .....</b>	<b>543</b>
<b>Cable Test Settings .....</b>	<b>544</b>
<b>Running Cable Test .....</b>	<b>545</b>
Open Cable TDR Testing .....	546
Terminated WireView Testing .....	549
Toning Function .....	551
Uploading Results to Link-Live .....	552
<b>Specifications and Compliance .....</b>	<b>553</b>
<b>LR10G-100/200 Specifications .....</b>	<b>554</b>
General .....	554
Environmental Specifications .....	556
<b>Certifications and Compliance .....</b>	<b>557</b>



# Contact Us

Online: [NetAlly.com](http://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/LinkRunner10G](http://NetAlly.com/Products/LinkRunner10G)

For customer support, visit:  
[NetAlly.com/Support](http://NetAlly.com/Support)

## Register your LinkRunner 10G

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](#).

## Introduction

The LinkRunner 10G 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](http://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](http://Link-Live.com) and "Claim" your LinkRunner to access these features.


# How to Use this Guide

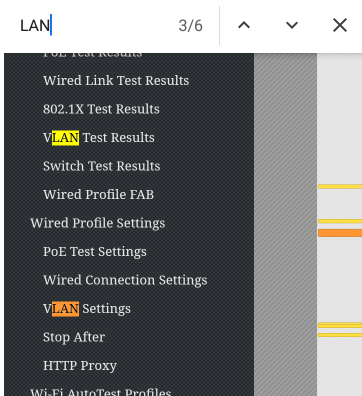
This user guide describes the LinkRunner 10G's testing functionality and basic elements of the system interface.

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

The LinkRunner 10G is also referred to as just LinkRunner 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

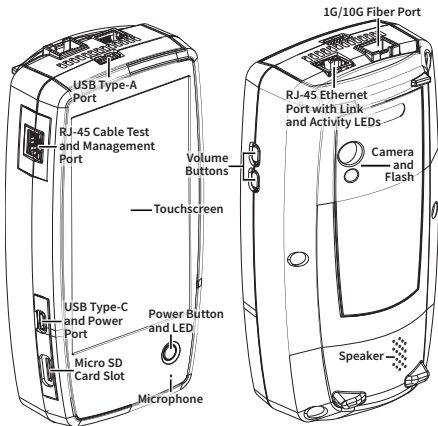
- Manuals are also available for download at: <https://www.netally.com/support/user-guides/>
- To view the User Guide on your LinkRunner 10G, you must have a network connection with access to the internet (see [Connecting to Wi-Fi](#)). When you tap on **Guides > User Guide** on the "[Home Screen](#)" 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 LinkRunner 10G user guide is available if you [change the device language](#) to one of those languages. If you choose Japanese, the English user manual is used.

# Buttons and Ports

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



## FEATURE

**Fiber Port**  
**1G/10GBASE-X**

## DESCRIPTION

Connects to an SFP adapter and fiber cable for network testing. NOTE: 100FX SFPs are not supported.

<b>FEATURE</b>	<b>DESCRIPTION</b>
<b>RJ-45 LAN Port 10M/100M/1G/ 2.5G/5G/10G- BASE-T</b>	Connects to a copper Ethernet cable for network testing Supports PoE (with compatible unit hardware)
<b>Transmit LEDs</b>	Green LED lit: Linked Yellow LED flashing: Activity
<b>USB Type-A Port</b>	Connects to any USB device
<b>RJ-45 Cable Test and Management Port</b>	Connects to an Ethernet cable for patch cable testing and unit management
<b>USB Type-C On-the-Go Port</b>	Connects to a USB Type-C connector for file transfer and to the included AC adapter for charging the unit
<b>Microphone</b>	Allows voice input
<b>Camera and Flash</b>	Captures images and acts as a flashlight
<b>Micro SD Card Slot</b>	Used for removable storage expansion (See Inserting a Micro SD Card below.)
<b>Volume Buttons</b>	Increase or decrease the audio volume
<b>Speaker</b>	Produces audio



FEATURE	DESCRIPTION
Power Button	Press and hold to display menu for <b>Power off</b> or <b>Restart</b> Green LED: Unit is powered on Red LED: Unit is charging

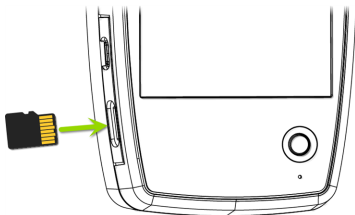
See [Test and Management Ports](#) for detailed explanations of the port functions.

See [Updating Software](#) for requirements on updating system software.

Refer to the product [Specifications](#) if needed.

## Inserting a Micro SD Card

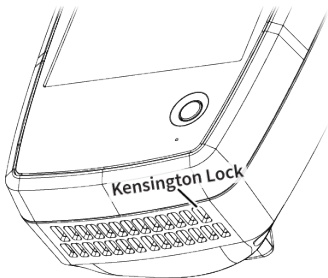
A Micro SD card must be inserted with the *metal contacts facing the front* (towards the touchscreen) of the unit, as shown below.



The card should slide in easily when properly oriented. You may need a paperclip or thumbnail to carefully push the SD card in far enough to engage the spring mechanism for insertion and removal.


## Using a Kensington Lock

The Kensington Lock slot is the right, front vent hole on the bottom of the unit, as shown below.



# Charging and Power

Your LinkRunner 10G 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 4-8 ( $\geq 25.5$  W) provide enough power to run the test unit indefinitely and to charge the battery.

- Negotiated PoE class levels 0-3 ( $\leq 15.4$  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 LinkRunner 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 turns green.
- When the display goes into Sleep mode, the Power Button LED remains on. 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.


# 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.

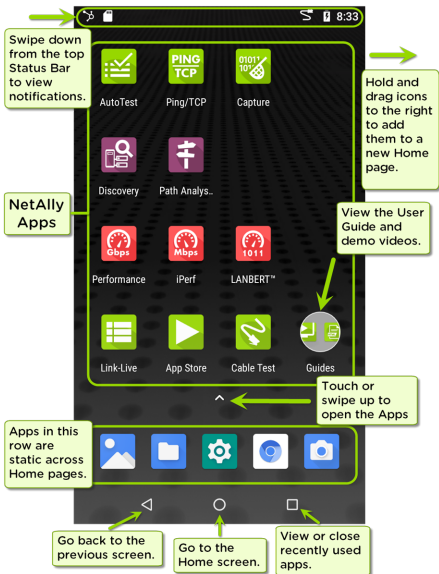
© 2019-2023 NetAlly

# 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 LinkRunner 10G 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



Like other hand-held devices, your LinkRunner 10G 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 LinkRunner 10G 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 them. 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).

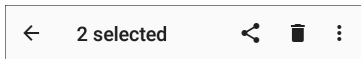
## Swiping


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.

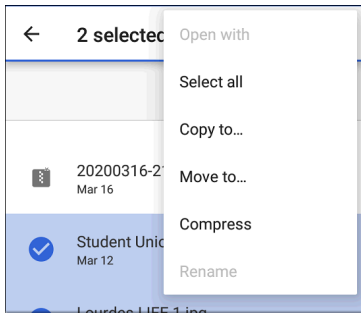
## Long Pressing

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 .

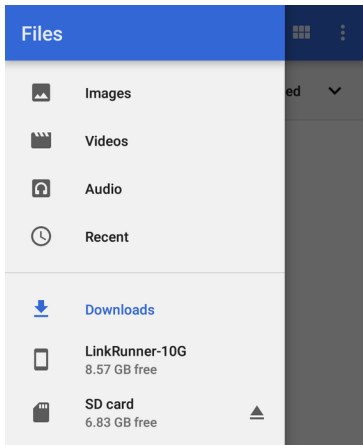



You can also long press on text on most screens to open options for copying and [sharing](#) the text.

## Left-Side Navigation Drawer

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

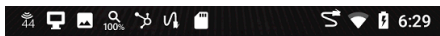




NOTE: In the Files app, you may need to tap the action overflow icon  at the top right and select **Show Internal Storage** to navigate to the **LinkRunner-10G** folder and sub-folders, as shown above.

See the [Navigation Drawer](#) topic for additional information.

# System Status Bar and Notifications



The Status Bar across the top of the screen displays notification icons from the system as well as LinkRunner 10G-specific icons related to your network connections and test statuses.

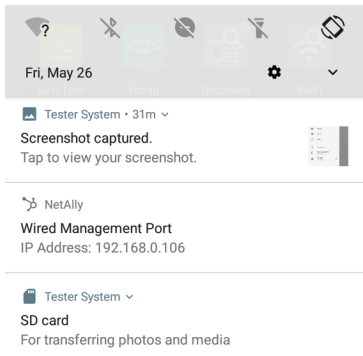
See [Test and Port Status Notifications](#) for details about the icons and notifications related to LinkRunner 10G network connections, testing, and management.


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.




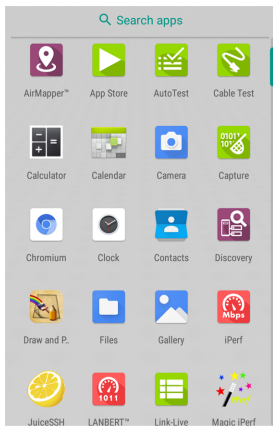
- Tap the title and down arrow  on a notification (or swipe down on it) to expand the box and view more details or options.
- Tap the middle of a notification to open the related app, image, or device settings or to perform other related actions.
- Swipe left on a notification to dismiss it.

NOTE: Because they are essential to the LinkRunner 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 .

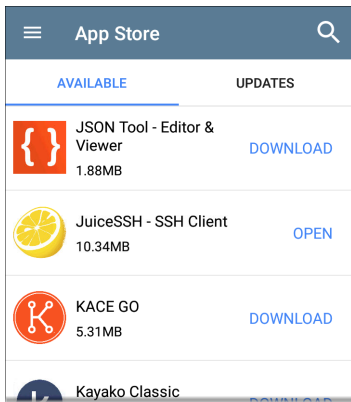


The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.


- 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

From the Home Screen or Apps Screen, open the NetAlly  App Store to download third-party system applications to use on your LinkRunner 10G.



NOTE: Your unit must be "claimed" to [Link-Live Cloud Service](#) at [Link-Live.com](http://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-](#)

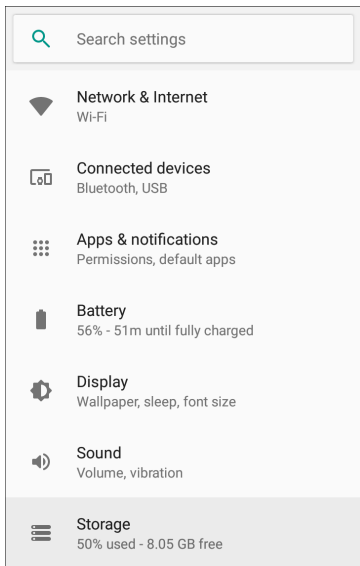
[Live.com](https://www.live.com), and select the floating action button (FAB) at the lower right corner to

▶ **Request or Upload an App.**



# Device Settings

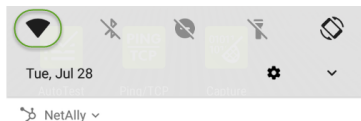
To access the system device settings, tap the Settings  icon at the bottom of the [Home screen](#).



The device settings screen lets you adjust the display; adjust sound (including volume for external USB speakers or headsets); set date and time; view installed applications and memory devices; [connect to Wi-Fi](#); or [reset to factory defaults](#).



## Quick Settings Panel

You can also access some of the most common device settings, like Wi-Fi, 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. For example, touch and hold the Auto-Rotate icon  to open Display settings.
- Tap the pencil icon  at the bottom of the Quick Settings Panel to configure the icon controls that appear in the panel.

## 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 English, Japanese, and Chinese language displays. See "[Changing the Device Language](#)" on page 67 for information on changing the language.

## Connecting to Wi-Fi

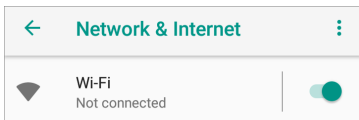
Basic connectivity to Wi-Fi is done using the Wi-Fi Management Port, which is configured in the system network settings. The [Wi-Fi Management Port](#) is separate from the Wi-Fi test port. It can access the internet, be used by other system applications, upload test results to the Link-Live web site, and be used for remote control. The management port also provides a more stable network connection than the test port, which can change connections during AutoTests or be disconnected during Wi-Fi scanning. See [Test and Management Ports](#) for more information.

NOTE: NetAlly testing apps use the Wi-Fi Test Ports and Wi-Fi AutoTest Profiles to connect to Wi-Fi networks during testing. See [Test and Management Ports](#) for more information.

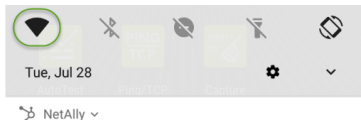
To connect your LinkRunner to a Wi-Fi network, access the system Wi-Fi Device Settings using either method below:

- Open the device Wi-Fi settings from the main [Device Settings](#) screen by tapping the Settings icon  and selecting **Network &**

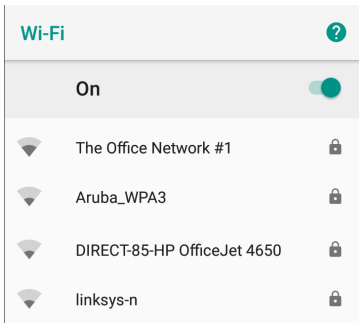
## Internet &gt; Wi-Fi.



- Open device Wi-Fi settings from the [Quick Settings panel](#) by dragging down the top Status Bar and tapping and holding (long pressing) the Wi-Fi icon.




Either path opens the Wi-Fi settings screen.




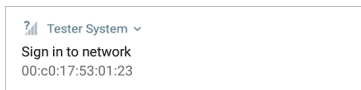
1. Ensure the Wi-Fi feature is **On**.
2. Tap an available Wi-Fi network in the list.
3. Enter the network's security credentials. (Most networks only require a password, but depending on the security settings, some may also require a company username, EAP type, authentication type, certificate, or other credentials.)
4. Tap **CONNECT**.

The network you selected moves to the top of the list, and your connection status is displayed below its name in device and quick settings.


The Status Bar displays the Wi-Fi status icon  at the top right of the screen.

## Captive Portals

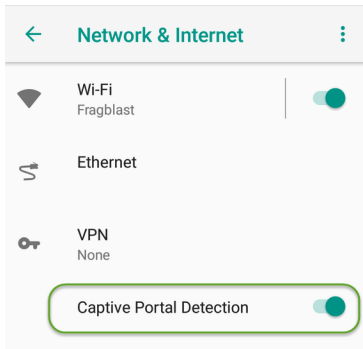
When you try to connect to a network with a Captive Portal requirement, this system notification icon  appears in the top [Status Bar](#). Drag down from the top of the screen to open the notification.



Tap the notification to open a web browser window where you can enter the required information for the captive portal. When finished, you can access the internet through the connected network.

If you are trying to connect to a network with a captive portal, but the system notification is not appearing, check that the **Captive Portal Detection** setting is enabled in [Device Settings](#)  > **Network & Internet**.





## Configuring Wi-Fi Connections With Enterprise Security

Enterprise security requirements for WPA/WPA2/WPA3 Enterprise now require a CA certificate file to be imported to your unit. Some EAP types also require a client certificate and key. This procedure assumes that you are trying to connect to an AP using WPA2-E with PEAP.

- [Before You Begin](#)
- [Import the Certificate Authority File](#)

- [Test Wi-Fi Management Using WPA2-E with PEAP](#)
- [Import the Client Certificate](#)

## Before You Begin

You may depend on your IT department to provide authorization certificates, which may be created by a Trusted Root Authority like VeriSign or DigiCert. If so, contact your IT department for the certificate resources. You will need:

- CA certificate in .pem format
- Client certificate in .p12 format with private key (EAP TLS only)
- Common name, domain name, username, and password for the server you to which you want to connect.

If you have the ability to generate your own self-signed certificates, such as a FreeRADIUS server, you can create these resources as needed. This procedure uses examples generated by a FreeRADIUS server as a certificate source, although other sources are available.

## Import the Certificate Authority File

1. Copy the self-signed Certificate Authority (CA) file (in .pem format) onto a USB thumb drive.
2. Transfer the USB thumb drive to your LinkRunner 10G, and then copy the .pem file to the **Downloads** folder.
3. Open the Settings app.
4. Navigate to **Security > Encryption & credentials > Install a certificate > Wi-Fi certificate**. This opens the file picker.
5. Navigate to the Downloads folder, and select the .pem file that contains your CA certificate.
6. Rename this certificate (for example, **CA FreeRadius self-signed**). A message confirms that the Wi-Fi certificate has been installed.
7. (Optional) Verify the CA certificate installed correctly:

- a. Tap the system **BACK** button to return to Encryption & credentials.
  - b. Tap **User credentials**.
  - c. Verify that the name of your CA file (for example, **CA FreeRadius self-signed**) is displayed.
8. If you are creating your own certificate:
- a. Verify the common name for the enterprise server. For example, using a FreeRADIUS server, create a common name of Example Server Certificate by entering:

```
sudo -s
```

```
cd /etc/freeradius/certs
```

```
openssl x509 -in server.pem  
-text | grep Subject |  
grep CN
```

**Output:**

```
Subject: C=FR, ST=Radius,  
O=Example Inc., CN=Example  
Server Certificate
```

```
emailAddress=  
admin@example.org
```

- b. On the same server, create a user login to access the enterprise server. For example, with a FreeRADIUS server, you would edit `/etc/freeradius/users`, locate the section for "# The canonical testing user", and then create the new user by inserting 2 lines:

```
entuser1 Cleartext-Password  
:= "randompw"  
Reply-Message := "Hello, %  
{User-Name}"
```

This creates a user login called **entuser1** with a password of **randompw**.

## Test Wi-Fi Management Using WPA2-E with PEAP

1. Open the Settings app on your unit and navigate to **Network & internet**.
2. Toggle the Wi-Fi button to On/Enabled.
3. Tap **Wi-Fi** to view available networks.

4. Scroll down to and then select the SSID of the enterprise server you wish to connect to using WPA2-E (for example, **TEST-Ruckus-WPA2-E**).
5. Configure the following WPA2-E options in the pop-up dialog:
  - EAP method: **PEAP**
  - Phase 2 authentication: **MSCHAPV2**
  - CA certificate: (use whatever name you chose for your CA certificate, for example, **CA FreeRadius self-signed**)
  - Online Certificate Status: **Do not validate**
  - Domain: (enter the Common Name recorded above, for example, **Example Server Certificate**)
  - Identity: (enter whatever test user name was set up for the server, for example, **entuser1**)
  - Anonymous identity: (leave blank)

- Password: (enter the password set up for the server)
6. Tap the **CONNECT** button to apply settings and close the configuration page.
  7. Verify that the test SSID appears at the top of the list with a status of Connected.

## Import the Client Certificate

NOTE: Applies to EAP TLS only.

1. Obtain a client certificate in .p12 format. Be sure it includes the private key.

NOTE: Although the imported CA certificate is a .pem file, NetAlly recommends a .p12 file format for the client certificate. Below is a sample openssl command to convert a client certificate from .pem to .p12 format:


```
<path_to_openssl_bin>\openssl.exe  
pkcs12 -legacy -provider-path  
<openssl_path>/providers -export  
-inkey <privateKey>.key  
-in <client_cert>.pem  
-out <client_cert>.p12
```

2. Rename the certificate file, for example, **client.p12**.
3. Copy the .p12 file to a USB thumb drive.
4. Transfer the USB thumb drive to your LinkRunner 10G, and then copy the .p12 file to the **Downloads** folder.
5. Open the Settings app.
6. Navigate to **Security > Encryption & credentials > Install a certificate > Wi-Fi certificate**. This opens the file picker.
7. Navigate to the **Downloads** folder, and select the .p12 file that contains your client certificate (for example, **client.p12**). A message prompts you to enter the password.
8. Enter the client certificate password to extract the certificate.
9. Rename the certificate, for example, **FreeRadius client**. A message confirms that the Wi-Fi certificate has been installed.





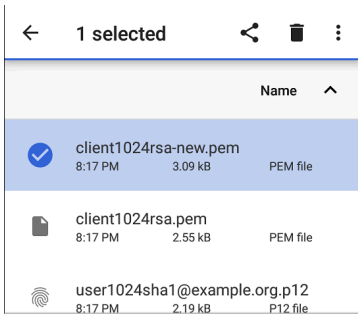
10. (Optional) Verify the client certificate installed correctly:
  - a. Tap the system **BACK** button to return to Encryption & credentials.
  - b. Tap **User credentials**.
  - c. Verify that the name of your client certificate file (for example, **FreeRadius client**) is displayed.
11. Press the system **BACK** button to return to Encryption & credentials. You can now securely connect to your enterprise server.


# Sharing

The system **Files**  app lets you share files from internal or external storage can to Bluetooth, 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 Navigation menu  or the [left-side navigation drawer](#).
3. Long press on one or multiple files to select it.



4. Tap the  share icon in the top toolbar to open the Share pop-up dialog.


Share via




Link-Live



Bluetooth


5. Tap to choose a sharing method and follow the system prompts to share the file or files.
  - a. If uploading to [Link-Live](#), tap the  **Link-Live** option.


**Link-Live**  
by NetAlly

**File Name**  
client1024rsa-new.pem

**Comment**  
Certs

**Job Comment**  
South Campus Wi-Fi

 [SAVE TO LAST TEST RESULT](#)

 [SAVE TO UPLOADED FILES](#)

- 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. (The **SAVE TO LAST TEST RESULT** option attaches the image to your most recently run AutoTest, Performance, iPerf, or Cable Test results on Link-Live.com.)

See the [Link-Live](#) chapter for more information on using Link-Live with your LinkRunner 10G.

## 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 procedure in [Sharing](#) to share the image using Link-Live, Bluetooth, or another configured application.

# Changing the Device Language

The LinkRunner 10G supports Chinese, English, and Japanese 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 LinkRunner displays the chosen languages, as available, in the priority order shown on the Language preferences screen.

NOTE: The LinkRunner 10G supports Chinese, English, and Japanese. This user guide supports Chinese and English. If you choose Japanese 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/>





# LinkRunner 10G

## Settings and Tools

The LinkRunner 10G 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 LinkRunner 10G*.


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

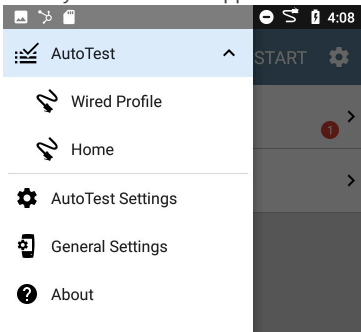
Access common settings and informational screens for the NetAlly testing apps (like AutoTest or Capture) by opening the left-side Navigation Drawers  or Settings .

# 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



### LinkRunner 10G Analyzer

**Model:** LR10G-100

**Serial:** 2008011

#### MAC Addresses

Wired: 00c017-540024

Wired Management: 00c017-540025

**System Version:** 2.1.0.167

**AllyCare:** Enabled

Expires: 6/24/2024

#### SFP Details

Type: 1000BASE-SX (850 nm)

Vendor: AVAGO

Version: --

Model: AFBR-57M5APZ

Rx Power: --

[EXPORT LOGS](#)

The About screen displays the model number, serial number, MAC addresses, software versions, SFP details, and current AllyCare contract status for your LinkRunner 10G.


If a **User-Defined MAC** is enabled in an NetAlly apps' [General Settings](#) or in the "[Wired Profile Settings](#)" on page 203, (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](#).)

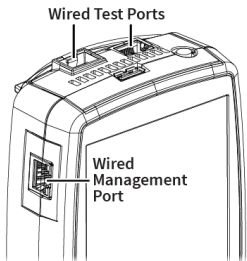
## Exporting Settings for All Apps

The action overflow icon  on the About Screen supports the importing or exporting of settings for *all* applications that allow import/export. See

[Importing and Exporting Settings for All Apps](#) for details.

# Test and Management Ports

The LinkRunner 10G has two wired RJ-45 copper ports and a fiber port, each with specific test or management functions described in this section.



Either the top copper port or fiber port can act as the Wired Test Port, so in total, the LinkRunner has *two* network interfaces: 1) Wired Test, and 2) Wired Management.

See the sections below for more information on the ports. Also see [Buttons and Ports](#) and the technical if 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.



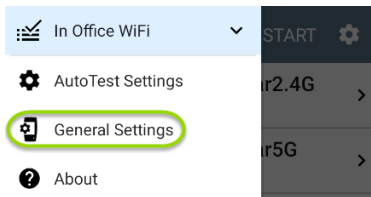
**Wired Fiber Test Port:** The SFP and fiber test port is also on the top of the unit. To disable, unplug the connection.

NOTE: If both the top fiber and copper ports are connected to an active network, the LinkRunner uses the fiber link as the Wired Test Port connection.

LinkRunner runs Wired AutoTests, Captures, Discovery, and other comprehensive network analysis apps over the test port. The Wi-Fi test radio is primarily controlled by the settings in applications, especially AutoTest.

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 LinkRunner 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

** Wired Management Port:** The wired management port is the RJ-45 port on the left side of the unit.

The Wi-Fi management radio is set up by the system network settings. The management port provides full Internet access and a more stable network connection than the Test Ports, which may frequently drop links and reconnect or resume scanning.

LinkRunner can run Discovery, Ping/TCP Connect tests, Path Analysis, and iPerf tests on




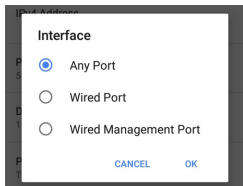
the management port, but not AutoTests, packet captures, or Performance tests.

## Selecting Ports

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

- You may want to verify that you are getting a reliable connection to the Internet and the Link-Live cloud service while you are actively using the Wi-Fi Test port to perform an AirMapper survey. To check connectivity, you can configure the Ping/TCP app to use the Wi-Fi Management port to run a continuous background ping to the Internet.
- Each port can connect to different networks. For example, an organization might have one network for visitors and another for staff. You can use the management and the test port to check connectivity on each network without the need to link and relink through a single interface.

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

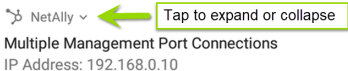


- The top Wired Port refers to the Test port.
- An AutoTest [Wired Profile](#) must run to establish test port links.
- The last listed [Wired Profile](#) runs automatically when you start up the LinkRunner if a connection is available.

# Test and Port Status Notifications

LinkRunner 10G 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 LinkRunner 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.



A **Wired Test Port** connection, called the "Wired Port" in app settings, is established in either the top RJ-45 Ethernet [port](#) or the top Fiber port.

 NetAlly ▾

**Wired Port**

Speed: 1 G Fdx

IP Address: 10.250.2.191

**NOTE:** If both the fiber and top copper ports are connected to an active network, the LinkRunner 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.

 AutoTest ^
**Periodic AutoTest Running**

Passed: 3

Failed: 2

Skipped: 1

Time Remaining: 54 m

## Management Port Notifications



A **Management Port** connection is established through the left-side RJ-45 Management **port** and/or the main system Wi-Fi adapter.

 NetAlly
**Wired Management Port**

IP Address: 192.168.0.123



A **Wired Management Port** connection is established through the left-side RJ-45 Management **port**. Its details are displayed under the Management Port notification (above).

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



now

No Management Port Connection

## Discovery Notifications

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](#).

## 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](#).

---

 NetAlly ^

Remote Connected

Clients


10.0.0.14

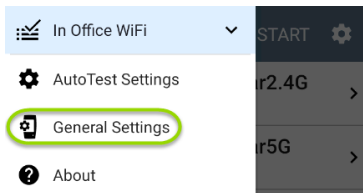
---



# LinkRunner 10G General Settings

LinkRunner'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.



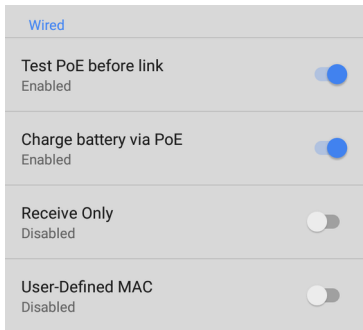
See also [Test and Management Ports](#) and [Test and Port Status Notifications](#) for related information on port functionality and status icons.

NOTE: Both Wi-Fi and Wired test ports have their own User-Defined MAC settings.



## Wired

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 LinkRunner 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 LinkRunner 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:** Enabling this setting prevents the LinkRunner 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.

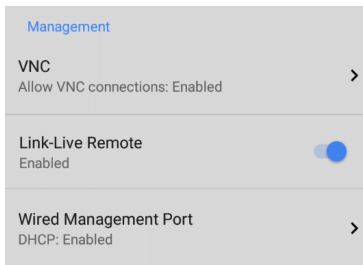
**User-Defined MAC:** This setting affects the [Wired Test Port](#) only. Tap the toggle switch to enable a user-defined MAC address. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. Tap the lower field to

enter your desired MAC address for the LinkRunner. 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](#)" on page 207 for more information.

## Management

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



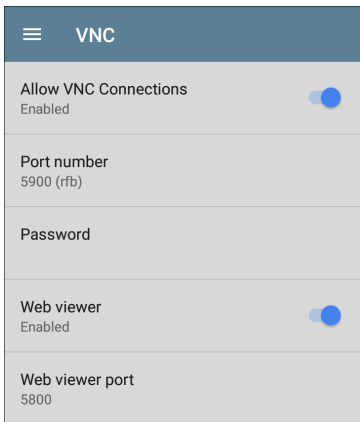
The screenshot shows a settings menu with a grey background. At the top, the word "Management" is written in blue. Below it are three settings items, each with a right-pointing chevron icon. The first item is "VNC" with the status "Allow VNC connections: Enabled". The second item is "Link-Live Remote" with the status "Enabled" and a blue toggle switch that is turned on. The third item is "Wired Management Port" with the status "DHCP: Enabled".

Setting	Status
VNC	Allow VNC connections: Enabled
Link-Live Remote	Enabled
Wired Management Port	DHCP: Enabled



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 LinkRunner 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 LinkRunner'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 LinkRunner must

be [claimed](#). See [NetAlly.com/Support](https://www.netally.com/support) for more information.

Access the Remote function on the **Units**  page at Link-Live.com by selecting the claimed LinkRunner 10G.

## Wired Management Port

**DHCP:** This setting controls IP address assignment of the [RJ-45 Wired Management Port](#) on the left side of the LinkRunner. By default, DHCP is enabled. Tap this field and tap the toggle button to disable DHCP and enter static IP information.

## Preferences

### Preferences

#### Distance Unit

Feet

**Distance Unit:** This is the unit LinkRunner 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 savings files. (The default is to give you the option to save to [Link-Live](#) or locally.)

## Trending Graphs

Many of the LinkRunner 10G 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](#).



Ping

STOP

**PING**  
**TCP** www.google.com

Device Name: --

IP Address: 172.217.11.228

MAC Address: --

Interface: Wired Port

**Results**

Started: 4:43:12 PM

Status: Success

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

## Response Time



Cur    Min    Max    Avg

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

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

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.

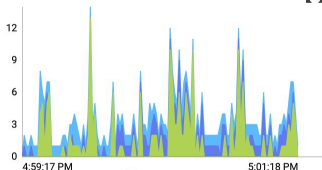
For another example, the image below shows the [Capture](#) app graph.



## Wired Capture


Status: Stopped

Captured Packets/sec



Packet Type	Captured	Total
 Unicast	141	141
 Broadcast	103	103
 Multicast	186	186
All	430	430

- 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](#)
- [Discovery – Interface Statistics](#)
- [Performance](#)
- [iPerf](#)

# 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 LinkRunner icons that appear in the Status Bar at the top of the screen, see [Test and Port Status Notifications](#).

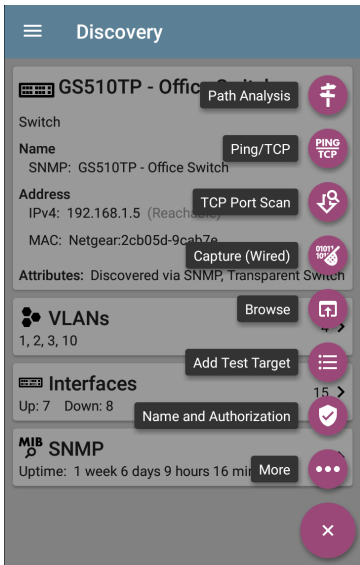
## Floating Action Button (FAB) and Menu

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 main AutoTest app screen allows you to add a new [Wired Profile](#).



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

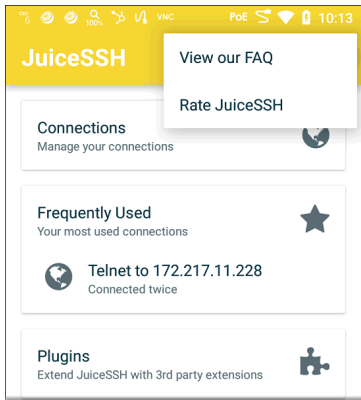
Some of the testing apps, like AutoTest, Ping/TCP, and Discovery, give you the option to **Browse** to internet addresses using a web browser application. LinkRunner has the Chromium browser pre-installed.

## Telnet/SSH

Starting with v1.1, LinkRunner has the JuiceSSH  application pre-installed. Both the AutoTest and Discovery apps provide options 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**.



## Camera and Flashlight

The camera lens and flash are located on the back of the unit. (See [Buttons and Ports](#).)

The Camera application  is located in the Apps screen and on the Home screen by default. Tap the icon to open the camera app and take a photo, which you can then [share](#) to other applications.

Additionally, once a Wired [AutoTest](#) Profile has completed, the [floating action button](#) appears and provides the option of opening the camera application to take and attach a picture to the AutoTest result uploaded to [Link-Live Cloud Service](#).

The Flashlight feature can be accessed from the [Quick Settings Panel](#) by swiping down twice from the top of the screen.

# Software Management

This chapter explains how to save and transfer files, reset app and device defaults, update your software, and remotely access your LinkRunner 10G.

Tap a link below to skip to a topic:

[Managing Files](#)

[Updating Software](#)

[Remote Access](#)

[Resetting App Defaults](#)


[Restoring Factory Defaults](#)


# Managing Files

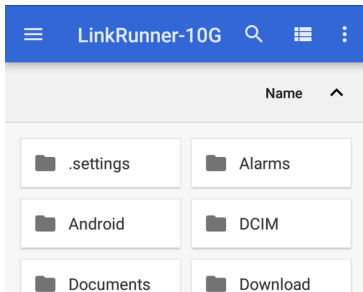
The LinkRunner 10G operating system, images, documents, and other files reside in a folder system, where you can copy, move, and paste them between folders or to external storage locations.


See also [Sharing](#).

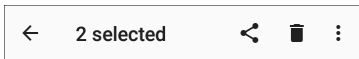
## Files Application


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

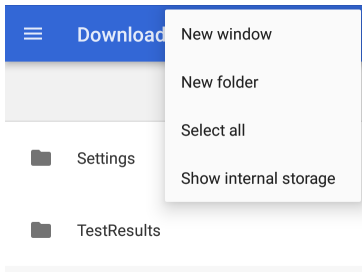
NOTE: To select the device sub-folders in the Files app as shown below, you may need to open the [navigation drawer](#) by swiping from the left side of the screen or by tapping the navigation icon  at the top left and then tapping the **LinkRunner-10G** folder.



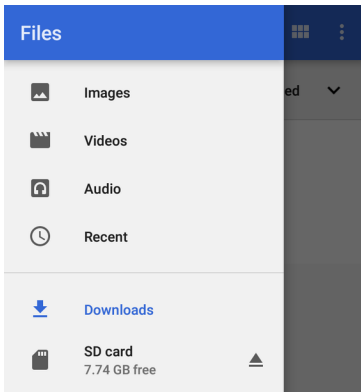
- Tap a folder or file to open it.
- **Long press** on folders or files to select multiple and to view additional file management operations in the top toolbar, including the **Share**  and Delete buttons.



- 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.

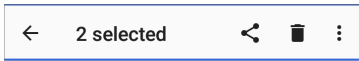



- Open the left-side [navigation drawer](#) ☰ to easily navigate through the top-level folders and attached storage devices.



## How to Move or Copy a File

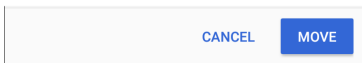
1. Long press on a file to select it. You can then select more files as needed by tapping them.



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 Micro SD Card

To use a Micro SD card for storage, insert it into the [Micro SD card slot](#) on the left side of your LinkRunner 10G. See [Inserting a Micro SD card](#).

A Micro SD card icon  appears in the Status Bar at the top of the screen. Pull down the top [Notification Panel](#) to reveal the SD card notification.

---

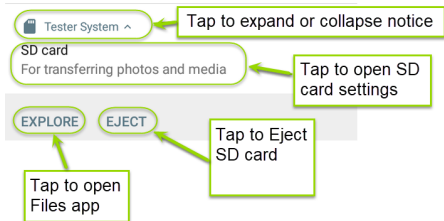
 Tester System ▾


SD card

For transferring photos and media

---

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




The **SD card** storage location is also available from the **Files**  application.

**⚠ CAUTION:** Use the system **EJECT** function before physically removing your Micro SD card from the USB port to avoid potential corruption of your storage device's file system.

## Using a USB Drive

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

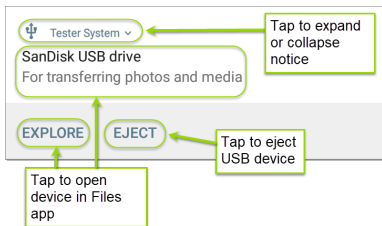
A USB icon  appears in the Status Bar at the top of the screen. Pull down the top **Notification Panel** to reveal the USB drive notification.


⚡ Tester System ▾

Kingston USB drive

For transferring photos and media

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

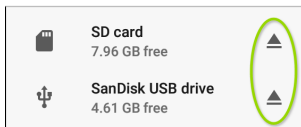


The **USB storage** location is now available from the **Files**  application.


**⚠ 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.

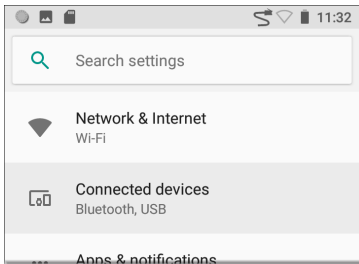
## Ejecting Storage Media

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).

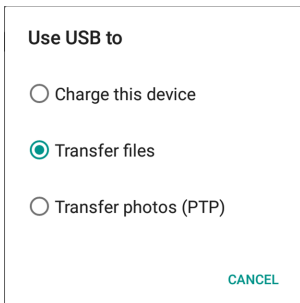


## Using a USB Type-C to USB Cable

1. Plug a USB-C cable into the [USB-C](#) port on the left side of the LinkRunner, and connect to a PC or tablet.
2. On the LinkRunner 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: LinkRunner does not charge through a USB cable connected to a PC.

6. On a PC or tablet, navigate to the LinkRunner 10G folder, and then move, copy, and paste files to and from the LinkRunner 10G's file system.


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

# Updating Software

Your LinkRunner 10G 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 LinkRunner 10G unit at [Link-Live.com](http://Link-Live.com). Then your LinkRunner can find and download software updates. See [Getting Started in Link-Live](#).

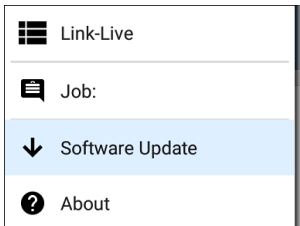
The first time you claim your LinkRunner 10G to Link-Live, a software update may be available. If so, an update icon  appears in the Status Bar. Slide down the [Top Notification Panel](#), and then select the notification to update your unit.

 Link-Live

**Software Update Notification**

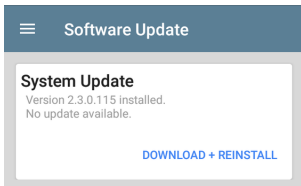
Software update available.

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 acquire update files by contacting NetAlly's Technical Support at [NetAlly.com/Support](https://NetAlly.com/Support) or by downloading them from [Link-Live.com](https://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 (lr10g-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 Micro SD card, and then insert the card into your LinkRunner.
2. Power off your LinkRunner 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 SD card**,

and then press the **Power** button to confirm the selection.

5. Use the volume buttons to highlight the correct update file on the Micro SD card, and then press the **Power** button to confirm. The LinkRunner 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 Micro SD card completed with status 0.' should show on the install line.
6. Use the volume keys and **Power** button to select **reboot system now**. Your unit should boot normally.

## Remote Access

LinkRunner 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 LinkRunner must be **claimed**. See [NetAlly.com/Support](https://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 LinkRunner ports. Swipe down from the [Status Bar](#) to view them.

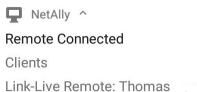


Wired Management Port

IP Address: 192.168.0.123

For a wired management connection, you must have an Ethernet cable with an active network connection plugged into the left-side RJ-45 [Management Port](#).

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



## Using VNC

Remotely access the LinkRunner 10G 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 LinkRunner 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 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 LinkRunner.

On your LinkRunner, 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](https://link-live.com) to access the Link-Live Remote feature. Your LinkRunner must be [claimed](#).

2. Navigate to the **Units**  page at Link-Live.com.
3. Select the LinkRunner 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 LinkRunner interface.
5. If necessary, at the top of the window, enter the Password set in **General Settings > Management > VNC** on the LinkRunner 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 individual NetAlly testing apps, such as AutoTest, Discovery, and Performance.

For instructions on restoring factory defaults to the entire test unit, see [Restoring LinkRunner 10G 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.

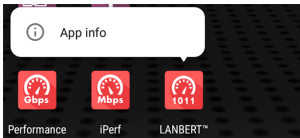
 **CAUTION:** This operation deletes all saved settings, including testing profiles and other application data.

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

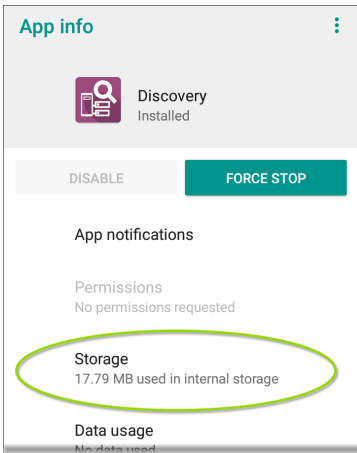
1. Access the **App Info** screen by long pressing (touch and hold) on an app's icon on the




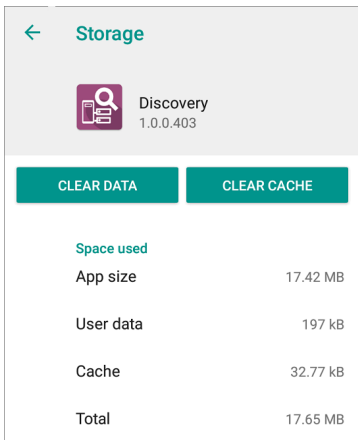
Home or Apps screen.



2. Tap App info.




3. On the App info screen, select **Storage**.  
(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 DATA**.



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

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

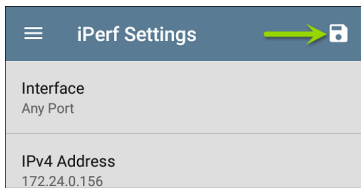
## Saving App Settings and Configurations

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.

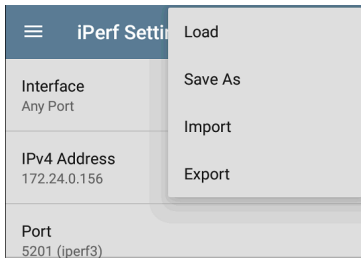
The following apps enable you to save and load settings configurations:

- [AutoTest, including Profile Groups](#)
- [Discovery](#)
- [Discovery Problem Settings](#)
- [Performance](#)
- [iPerf](#)
- [Spectrum](#)

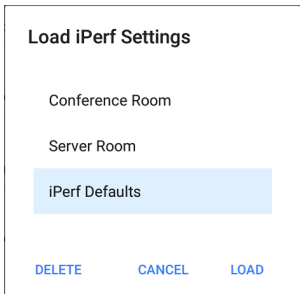
The iPerf app is shown below as an example.



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.

### Save iPerf Settings

Conference Room

Server Room

iPerf Defaults


Server Room



CANCEL SAVE

- **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 and 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.

## Importing and Exporting Settings

LinkRunner 10G provides functionality for importing and exporting saved test app settings for transfer to additional units or exporting to Link-Live. USB and other devices

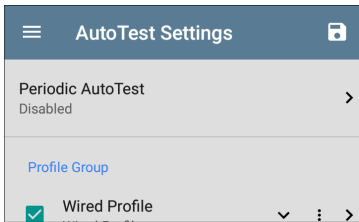
NOTE: You can import and export settings only between the same kind of NetAlly products. For example, both units must be LinkRunner 10Gs for a transfer to work.


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

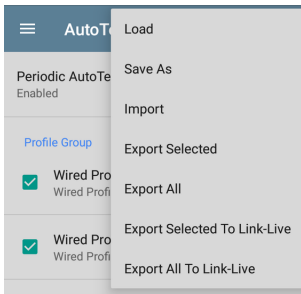
- [AutoTest Settings, including Profile Groups](#)
- [Discovery Settings](#)
- [Discovery > Problem Settings](#)
- [Performance Settings](#)
- [iPerf Settings](#)

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

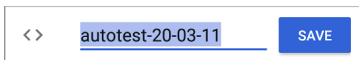




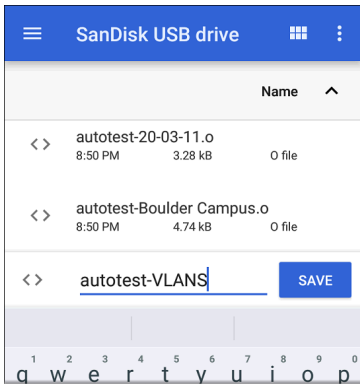
- Tap the save button  to import new app settings or export the *currently active and selected* app settings.



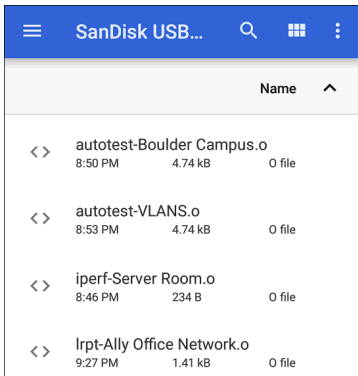
- Selected (checked) items in shared lists of configurations are the only ones exported when you choose **Export Selected**. This can include any checked items in submenus (such as AutoTest Test Targets or Community Strings in [Discovery Settings](#)). You can also select **Export All** to export all 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.



	Name			
<>	autotest-Boulder Campus.o	8:50 PM	4.74 kB	0 file
<>	autotest-VLANS.o	8:53 PM	4.74 kB	0 file
<>	iperf-Server Room.o	8:46 PM	234 B	0 file
<>	lrpt-Ally Office Network.o	9:27 PM	1.41 kB	0 file

- 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 LinkRunner

10G 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.

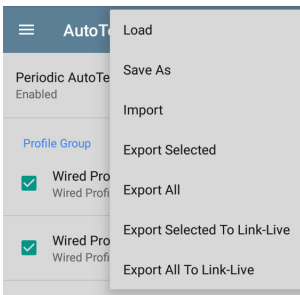
### Before You Begin

- 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 LinkRunner 10G 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" on page 521](#) 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.




**Link-Live**  
by NetAlly



**Settings File Name**  
autotest-shared settings

**Comment**  
Update for all units


**Job Comment**  
New profiles

 **EXPORT TO 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. Click the main menu icon .
3. Click on **Settings** to open the settings menu.
4. Select **LinkRunner 10G** 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.
- 

 AutoTest

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

---

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.

## Importing and Exporting Settings for All Apps

Your LinkRunner 10G 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 10Gs for a transfer to work.


To perform a group export or import:

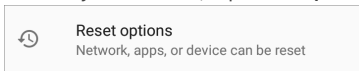
1. Open the About Screen by tapping the navigation menu icon  in any NetAlly application and then tapping **About**.
2. Tap the action overflow icon  to display the export/import menu.
3. To import settings:

- a. Tap **Import LinkRunner 10G 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 10G 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 LinkRunner 10G 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 LinkRunner 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 LinkRunner'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 an attached Micro SD card or a USB thumb drive. (Do not delete your backup files.)



# LinkRunner 10G 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 LinkRunner 10G. 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, like Ping/TCP, Capture, and Performance.

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



# AutoTest Chapter Contents

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

[AutoTest Overview](#)

[Managing Profiles and Profile Groups](#)

[Main AutoTest Screen](#)

[Periodic AutoTest](#)

[Wired AutoTest Profiles](#)

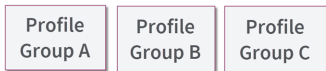
[DHCP, DNS, and Gateway Tests](#)

[Test Targets](#)

# 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.

## Profile Groups



## Profiles



## Test Targets



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.

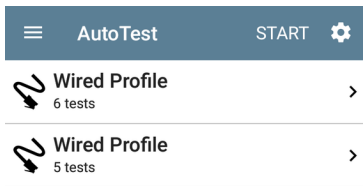
# Managing Profiles and Profile Groups


Profiles are a series, or suite, of tests designed to analyze the different characteristics of your networks. The LinkRunner 10G AutoTest app features one type of test profile:

**Wired Profiles** test copper and fiber connections.

## Factory Default Profiles

The LinkRunner 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.

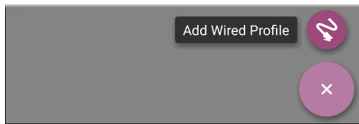
NOTE: Tapping the settings icon on the main AutoTest screen (shown above) opens the [AutoTest Settings and Profile Group](#) screen, not the individual Profile settings.

- 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](#).


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.




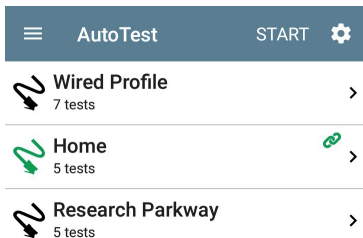
The profile's configuration screen appears after you select the type of profile you want to add. See the topic for each profile type for a description of its settings.

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

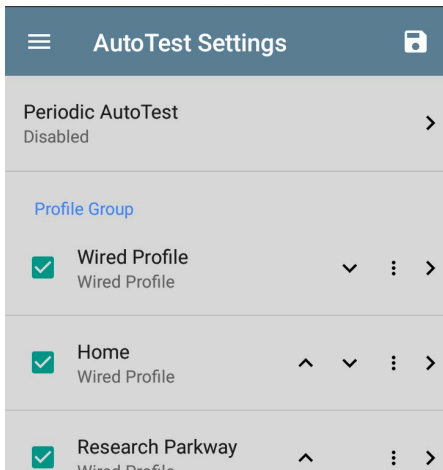
LinkRunner 10G also allows you to save Profile Groups. Profile Groups are simply **the included list of test Profiles and the order in which they run** when you start an AutoTest. (See [AutoTest Overview](#) for more explanation of Profile Groups.) You can configure and select Profiles and Profile Groups 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.




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.

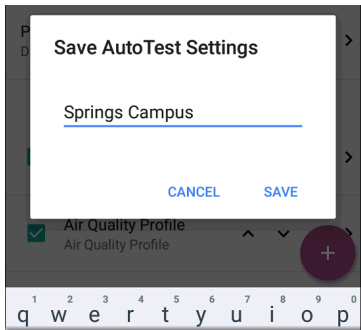
See [Exporting and Importing App Settings](#) for more details.

Each Profile Group can run one or many of the three Profiles types. Your 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.


The screenshot shows the 'Site Test' screen in the AutoTest app. At the top, there is a dark blue header with a hamburger menu icon on the left, the text 'Site Test' in the center, and the word 'START' followed by a gear icon on the right. Below the header, there is a list of three profile groups, each with a circular icon, a title, a subtitle, and a right-pointing chevron. The first group is 'Home' with a green icon and '5 tests'. The second is 'Research Parkway' with a black icon and '5 tests'. The third is 'Wired Profile' with a black icon and '5 tests'.

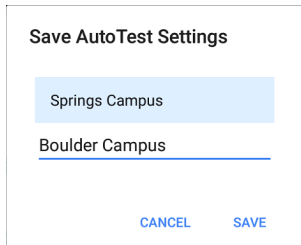
## Creating New Profile Groups

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 LinkRunner returns to the Profile Group screen with the new group name shown as the title.


Research Sites					
Periodic AutoTest Disabled		>			
Profile Group					
<input checked="" type="checkbox"/>	Home Wired Profile	∨	⋮	>	
<input checked="" type="checkbox"/>	Research Parkway Wired Profile	∧	∨	⋮	>
<input checked="" type="checkbox"/>	Boulder Office Wired Profile	∧	⋮	>	
<input type="checkbox"/>	Palo Alto Office Wired Profile		⋮	>	

# Importing and Exporting AutoTest Profiles

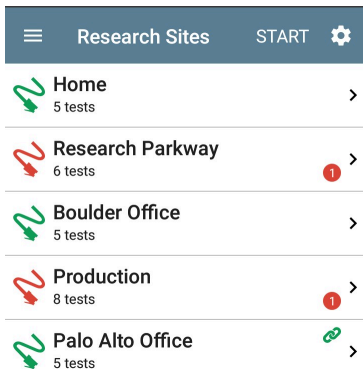
In addition to creating new profiles or using defaults, you can also:

- Import and export profile settings to any connected external or internal storage. See ["Importing and Exporting Settings" on page 132.](#)
- 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" on page 136.](#)

## 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 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.

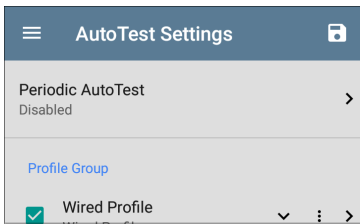
Each profile and test is summarized on a card. Tap a profile's or individual test's card to open and view test result details, including the causes of any Warnings or Failures.

# Periodic AutoTest

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

## 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.

☰ Periodic AutoTest

Periodic AutoTest  
Enabled

Interval  
10 minutes

Duration  
2 hours

Add Comment  
Enabled

Comment  
AT Boulder Site

Append Date & Time  
Enabled

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](https://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. AutoTests continues to run at the set Interval for the selected Duration or until you tap **STOP** in AutoTest.


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

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

Below the list is a light gray separator bar, followed by a dark blue box containing the 'Periodic AutoTest Status' summary:

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

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.



AutoTest ^

**Periodic AutoTest Running**

Passed: 3

Failed: 2

Skipped: 1

Time Remaining: 54 m

**NOTE:** AutoTest has priority control of the [Test Ports](#), so other apps, including [Discovery](#), are paused while AutoTest completes.



# Wired AutoTest Profiles

A Wired Profile runs a series of tests over your copper or fiber network connection.

The screenshot shows the AutoTest app interface. At the top, there is a blue header bar with a hamburger menu icon on the left, the text "AutoTest" in the center, and the word "START" followed by a gear icon on the right. Below the header is a list of profile cards. The first card is highlighted in light blue and is titled "Wired Profile" with a green lightning bolt icon and a link icon, and it indicates "8 tests". Below this are several other profile cards, each with a specific test icon and details:

- 50.6 V**: Includes a lightning bolt icon, "Class: 3", and "13.0 W".
- 100M/1G/2.5G/5G/10G**: Includes a link icon, "RJ-45", and "HDx/FDx".
- EXTREME\_48**: Includes a keyboard icon, "Port: 1/37".
- DHCP 10.250.3.161**: Includes "31 ms".
- DNS Compass.netally.eng**: Includes "6 ms".
- COS\_DEV\_SW1**: Includes a cloud and server icon, and "8 ms, 7 ms, 2 ms".
- HTTP google**: Includes "HTTP" in green and "google".


Each card has a right-pointing chevron icon. A purple circular button with a white plus sign is located at the bottom right of the list.

Like the main AutoTest screen, Wired Profile tests are summarized on cards. Tap a card to view individual test screens.

Each test icon (except the switch) displays green, yellow, or red to indicate the status of the completed test step: **Success/Warning/Fail**. The Switch Test card shows the name and port of the nearest switch, but does not turn green to indicate success.

## When Wired Profiles Run Automatically

The last enabled Wired Profile in the currently active Profile Group runs automatically when a copper cable is connected or energy is detected to the top RJ-45 port, unless the AutoTest app is open in the foreground and there is more than one enabled Wired Profile. A Wired Profile does not start automatically if **Periodic AutoTest** is running.

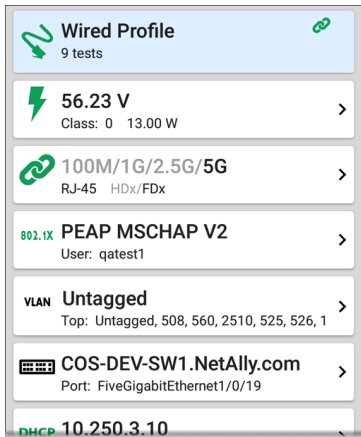
After a Wired Profile runs, a wired network link is maintained for further testing. Wired Test Port linkage is indicated in the top **Status Bar** with this notification icon: .



## Wired-Profile-Specific Tests

The following tests are specific to a Wired Profile:

- [PoE](#)
- [Wired Link](#)
- [802.1X](#)
- [VLAN](#)
- [Switch](#)



The screenshot displays a vertical list of test cards within a 'Wired Profile' container. The profile is indicated by a blue header with a green plug icon and a link icon, and it contains 9 tests. The test cards are as follows:

- 56.23 V**: Represented by a lightning bolt icon, with a class of 0 and 13.00 W.
- 100M/1G/2.5G/5G**: Represented by a link icon, with RJ-45 and HDx/FDx options.
- 802.1X PEAP MSCHAP V2**: Represented by a green '802.1X' icon, with a user of qatest1.
- VLAN Untagged**: Represented by a 'VLAN' icon, with a list of top VLANs: Untagged, 508, 560, 2510, 525, 526, 1.
- COS-DEV-SW1.NetAlly.com**: Represented by a keyboard icon, with a port of FiveGigabitEthernet1/0/19.
- DHCP 10.250.3.10**: Represented by a 'DHCP' icon.

The 802.1X card only appears if the **802.1X** setting is enabled for the Wired Profile.

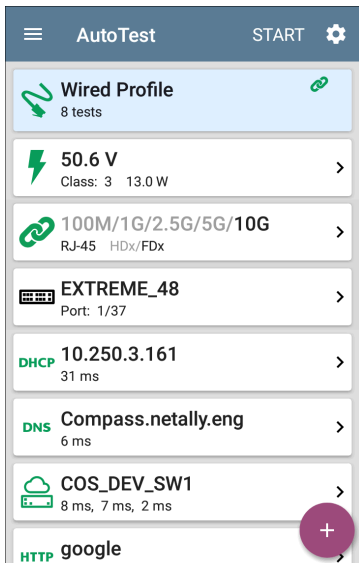
The VLAN test card appears if the **VLAN** setting is enabled or if VLAN-tagged traffic is detected during the AutoTest.

PoE, Wired Link, 802.1X, VLAN, and Switch Results are described next.

- Skip to [Wired Profile Settings](#).
- Skip to [DHCP, DNS, and Gateway Tests](#).
- Skip to [Test Targets](#).

# Wired Profile Results

The image below shows a completed AutoTest Wired Profile.







The screenshot displays the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" with a gear icon on the right. Below the header is a list of test results for a "Wired Profile" (indicated by a lightning bolt icon and a link icon). The profile contains 8 tests. The results are as follows:


- Wired Profile** (8 tests)
- 50.6 V** (Class: 3, 13.0 W)
- 100M/1G/2.5G/5G/10G** (RJ-45 HDx/FDx)
- EXTREME\_48** (Port: 1/37)
- DHCP 10.250.3.161** (31 ms)
- DNS Compass.netally.eng** (6 ms)
- COS\_DEV\_SW1** (8 ms, 7 ms, 2 ms)
- HTTP google**

A purple circular button with a white plus sign is located at the bottom right of the list.

On the Wired Profile screens, you can perform these actions:

- Tap any of the test result cards, like  PoE,  Link, or  Switch to open the individual test result screens.
- From any individual test screen, tap the settings icon  to go directly to the settings for the current test.
- On the individual test screens, tap [blue underlined links](#) to open a [Discovery](#) app Details screen showing the selected device or ID.

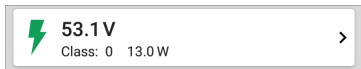
NOTE: You may need to [Configure SNMP](#) settings in the Discovery app to see all the available information about a network component, such as name and port information.

- Tap other **BLUE LINKS** or the blue action overflow icon  at the bottom of the test results screens for additional actions.

NOTE: Blue links and action icons do not appear on every test results screen, and if the active connection is dropped, you may

need to rerun the Profile to re-establish link and enable additional actions.

## PoE Test Results

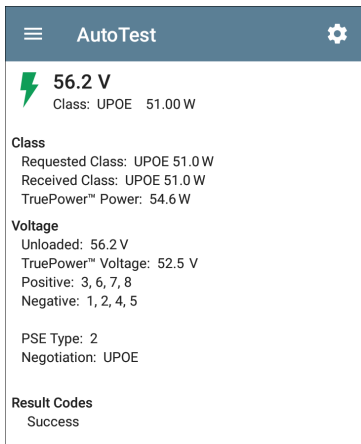


The card for the Power over Ethernet (PoE) test displays the measured Voltage, Class, and Wattage.


Refer to [PoE Settings](#) if needed.

Tap the card to open the PoE results screen.

## PoE Test Results Screen



☰ AutoTest ⚙️

 **56.2 V**  
Class: UPOE 51.00 W

**Class**  
Requested Class: UPOE 51.0 W  
Received Class: UPOE 51.0 W  
TruePower™ Power: 54.6 W

**Voltage**  
Unloaded: 56.2 V  
TruePower™ Voltage: 52.5 V  
Positive: 3, 6, 7, 8  
Negative: 1, 2, 4, 5

PSE Type: 2  
Negotiation: UPOE

**Result Codes**  
Success

In addition to the information from the PoE card, the PoE test screen shows these results:

### Class

**Requested Class:** Class selected in the PoE test settings

**Received Class:** Class acknowledgment received from the switch

**TruePower™ Power:** Measured wattage with load.

NOTE: The PoE card displays additional TruePower™ results only if TruePower is enabled in the Wired Profile [PoE Settings](#).

## Voltage

**Unloaded:** Measured voltage without load

**TruePower™ Voltage:** Measured voltage with load

**Positive:** Positive PoE cable pair IDs

**Negative:** Negative PoE cable pair IDs

**PSE Type:** Switch's advertised Power Sourcing Equipment (PSE) type. Recognized types are 1 – 4, LTPoE++, Cisco UPOE, and PoE Injectors. PSE supporting UPOE are classified under Type 2. If the type cannot be determined, "1/2" is displayed.

**Negotiation:** Negotiation status for UPOE and Class 4 (UPOE or LLDP)



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

## Wired Link Test Results

The Wired Link card indicates whether you can connect to an active network switch.




The Link test card for a copper Ethernet connection displays the advertised speed and duplex capabilities in **gray text** and the detected speed and duplex in **black text**.

LinkRunner can test and display information for link speeds up to 10G.



For a Fiber connection, the Link test card shows the connection speed and duplex.

The link icon turns yellow  (displays a Warning) under the following conditions:

- LinkRunner has linked at a speed slower than the maximum advertised speed.
- The link is using half duplex.
- For links faster than 1G, LinkRunner has detected a minimum SNR value below the set threshold.

Tap the card to open the Link test screen.

## Wired Link Test Screen



AutoTest



**100M/1G/2.5G/5G/10G**

RJ-45 FDX

### Speed

Advertised Speeds: 100M/1G/2.5G/5G/10G

Actual Speed: 10G

### Duplex

Advertised Duplex: FDX

Actual Duplex: FDX

### RJ-45 Details

Rx Pair: All

### Multi-Gigabit Details

Channel	Delay Skew	SNR	Avg SNR
A	REF	8.8 dB	8.7 dB
B	-1.25 ns	6.7 dB	6.8 dB
C	-3.75 ns	5.9 dB	5.9 dB
D	-1.25 ns	8.9 dB	8.7 dB
Threshold			1 dB

### Result Codes

Success

The Wired Link test screen shows the following:

## Speed

**Advertised Speed:** Speed capability as reported by the switch

**Actual Speed:** Link speed as measured by LinkRunner 10G

## Duplex

**Advertised Duplex:** Duplex capabilities reported by the switch

**Actual Duplex:** Duplex in use as detected by LinkRunner

## RJ-45 Details (Copper)

**Rx Pair:** Link receive pair

## Multi-Gigabit Details (Copper)

This table appears only when the Wired Profile is linked at speeds higher than 1G. Each twisted pair channel is graded based on the minimum SNR observed. Data in the table updates each second as long as the link persists.

**Channel:** Channels A, B, C, and D representing the twisted pairs in the cable

**Delay Skew:** Difference in propagation delay between sets of wired pairs. Channel A acts as the reference for the other channel measurements.

**SNR:** Current signal-to-noise ratio on each channel

**Avg SNR:** The average SNR measurement since link was established

**Threshold:** Multi-Gigabit SNR Threshold from the [Wired Connection settings](#)

## SFP Details (Fiber)

**1G**

SFP FDx

### Speed

Advertised Speeds: 1G

Actual Speed: 1G

### Duplex

Advertised Duplex: FDx

Actual Duplex: FDx

### SFP Details

Wavelength: 850 nm

Temperature: 42 C

Voltage: 3.29 V

Tx Bias Current: 5.99 mA

Tx Power: -4.42 dBm

Rx Power: -7.67 dBm

Reference Power: -7.67 dBm

Power Difference: 0 dB

### Result Codes

Success

[SET REFERENCE](#)[CLEAR REFERENCE](#)

The SFP Details are defined as follows:

**Wavelength:** Wavelength (in nanometers) at which the fiber connection is operating

**Temperature:** Temperature in degrees Celsius

**Voltage:** SFP transceiver power supply voltage (~3.3 V)

**Tx Bias Current:** Transmitter bias current

**Tx Power:** Transmitter power

**Rx Power:** Link receiver power

**Reference Power:** The user can set a Reference Power by pressing the **SET REFERENCE** button. This sets the current Rx Power as the reference. The value is saved until cleared by the **CLEAR REFERENCE** button. It is saved across reboots.

**Power Difference:** The difference between the current Rx Power and the reference. The number is positive if the current value is greater than the reference value.

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

## 802.1X Test Results

The 802.1X test card only displays if the [802.1X setting](#) is enabled in the Wired Profile Settings.

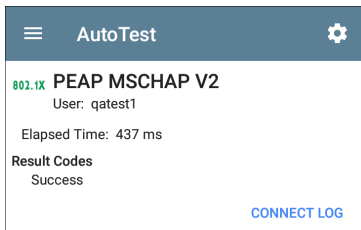
**802.1X** PEAP MSCHAP V2

User: qatest1



The card shows the EAP type selected in the Wired Connection settings and the username or certificate used. The 802.1X icon turns green if the connection is successful and yellow if 802.1X authentication fails.

## 802.1X Test Screen





The 802.1X screen also shows the time it took for the authentication process to complete along with Result Codes.

Tap the blue **CONNECT LOG** link to view the 802.1X Connect Log.



Connect Log		Save to Link-Live
3:59:45.654 PM	Supplicant: PEAP_MSCHAP_V2	
3:59:45.775 PM	Received EAP Fail	
3:59:45.777 PM	Identity: qatest1	
3:59:45.781 PM	Identity: qatest1	
3:59:45.808 PM	NAK: GOT (4) EAP-MD5 WANT (25) EAP-Peap	
3:59:45.822 PM	PEAP: Selecting Version: 0	
3:59:45.824 PM	PEAP: Received EAP Start request, sending Client Hello	
3:59:45.851 PM	PEAP: Received Server Hello	
3:59:45.923 PM	PEAP: Server Certificate unverified:	

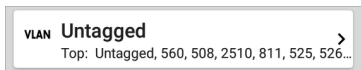
Select the action overflow icon  at the top right on the Connect Log screen to attach the log to its associated AutoTest result on the [Link-Live](#) website. You can also attach the Connect Log from the [floating action menu](#)  on the main Wired Profile screen.

## VLAN Test Results

The VLAN card only displays if the [VLAN setting](#) is enabled in the Wired Profile Settings or if AutoTest detects VLAN-tagged traffic.

<b>VLAN 508, Best Effort (0)</b>	<b>&gt;</b>
Top: Untagged	

The top line on the VLAN test card shows the configured VLAN settings (image above) or "Untagged" (image below) if VLAN disabled but VLAN-tagged traffic is seen.

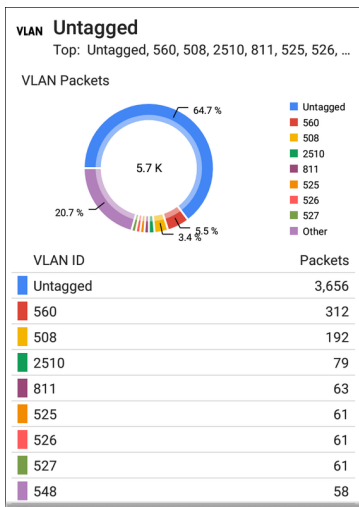


Untagged indicates that no VLAN tag is present in either received or transmitted frames, also referred to as the Native VLAN.

The second line on the VLAN card displays the top VLANs with the most detected traffic.

Tap the card to open the full VLAN screen.

## VLAN Test Screen



The VLAN test screen displays the real-time traffic the LinkRunner detects on the top VLANs. Up to nine VLANs with the highest traffic are displayed as colored portions of the pie chart.

The table on the lower part of the VLAN screen lists all the VLANs seen.

## Switch Test Results

The results available for the Switch Test are based on Discovery Protocol advertisements and SNMP system group information. SNMP forwarding table data is used to determine the Nearest Switch. See [Discovery Settings](#) for [SNMP configuration](#) instructions.



The Switch test card displays the Nearest Switch and the port name. The Switch icon remains black if the test is successful.

- If the LinkRunner does not detect any network traffic moving through the switch after 45 seconds, the switch icon turns yellow.



- If the connection is lost while the Wired Autotest is running, the switch icon turns red.



- If the LinkRunner was unable to identify the nearest switch, "Nearest Switch Not Found" displays on the Switch card.



The LinkRunner continues to search for the nearest switch, even after the AutoTest completes.

Tap the Switch card to open the full switch results screen.

## Switch Test Results Screen

Information on the Switch Test screen is organized by the order in which it was received, either via Discovery Protocol advertisements or SNMP.



## COS-DEV-SW1.NetAlly.com

Port: Fi1/0/42

### Status:

Network traffic seen in 196 ms from  
NetAlly:00c017-53009d

### Nearest Switch: [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42

Description: Test Port

VLAN ID: 500

Voice VLAN ID: 3333

IP Address: 10.250.0.2

MAC Address: Cisco:7802b1-b0caaa

Location: COS-DEV Lab Rack S2

Contact: Erik

Model: cisco C9300-48UN

Type: CDP (First Seen)

Last Seen: 3:39:11 PM

### Switch: [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42

Description: Test Port

VLAN ID: 500

IP Address: 10.250.0.2

MAC Address: Cisco:7802b1-b0ca80

Model: Cisco IOS Software [Fuji], Catalyst L3 Switch  
Software (CAT9K\_IOSXE), Version 16.9.3,

Type: LLDP

Last Seen: 3:39:12 PM

Each section represents a unique port advertisement as defined by protocol type and MAC address.

The switch results screen shows the following data fields:

**Status:** Time elapsed after link was established before network traffic was received from the switch. The MAC address of the device that sent the packet is also shown.

**Nearest Switch:** Name of the switch determined to be closest to the LinkRunner

**Port:** Detected Port name

**Description:** Configured description reported by the switch

**VLAN ID:** VLAN ID number (if present)

**Voice VLAN ID:** Voice VLAN ID number (if present)

**IP and MAC Addresses:** Discovered switch addresses

**Location:** Configured location reported by the switch. This field only appears if the LinkRunner has SNMP access to the Nearest Switch.

**Contact:** Configured contact person reported by the switch. This field only appears if the

LinkRunner has SNMP access to the Nearest Switch.

**Model:** Switch model name and/or number

**Type:** Discovery Protocol - CDP, LLDP, EDP, FDP, or SNMP. (First Seen) displays next to the protocol type first seen by the LinkRunner.

**Last Seen:** For non-SNMP discovery protocols (CDP, LLDP, EDP, or FDP), the time the advertisement was last received by the LinkRunner

**Last Updated:** For SNMP only, the time the information was gathered from SNMP tables

SNMP information, if available, appears at the bottom of the screen once the discovery process has acquired relevant data.



Software (CAT9K\_IOSXE), Version 16.9.3,  
Type: LLDP  
Last Seen: 3:39:12 PM

**Switch:** [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42  
Description: Test Port  
VLAN ID: 500  
IP Address: 10.250.0.1  
MAC Address: Cisco:00000c-07ac01  
Model: CAT9K\_IOSXE  
Type: SNMP  
Last Updated: 3:39:05 PM

[INTERFACE DETAILS](#)   [BROWSE](#)   [...](#)

**Switch:** Below the Nearest Switch, other switches seen via advertisements or SNMP

At the bottom of the switch test screen, tap the blue links or the action overflow icon **...** to open other apps or tools with the target (in this case, the **Nearest Switch**) pre-populated.

Voice VLAN ID: 201  
IP Address: 172.24.0.1  
MAC Address: Cisco:c0  
Model: cisco C9300-48  
Type: CDP  
Last Seen: 4:09:04 PM

Switch: [Battle Room](#)

Port: g4  
IP Address: 10.1.1.23  
MAC Address: Ntgear:b  
Model: Netgear Gigabit  
Type: LLDP  
Last Seen: 4:08:59 PM

TCP Connect  
Capture  
Browse  
Telnet  
SSH

[INTERFACE DETAILS](#)    [PING](#)    ...

For example, **INTERFACE DETAILS** opens the Interface Details screen for the Switch Port in the [Discovery](#) app.

**NOTE:** The **Interface Details** action link only appears in the Switch results if LinkRunner has current [Discovery](#) data, and AutoTest was able to identify the nearest switch and connected interface.

The **Ping**, **TCP Connect**, and **Capture** selections open the corresponding NetAlly apps, populated with the switch's address. **Browse** opens the

Chromium browser, and [Telnet or SSH](#) opens the JuiceSSH app.

## DHCP, DNS, and Gateway Results

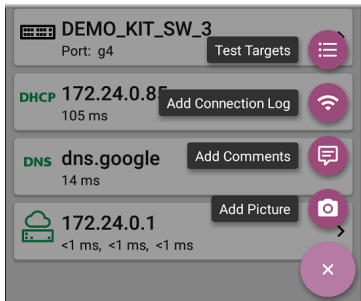
See [DHCP, DNS, and Gateway Tests](#).

### **PING FTP TCP HTTP** Target Tests

See the [Test Targets](#) topic for information on target test results.

## Wired Profile FAB

The floating action button (FAB) on AutoTest Profile screens allows you to add Test Targets to the Profile, as well as attach comments, an image, and an 802.1X connect log to this AutoTest result on the [Link-Live](#) website.



- The **Test Targets** option opens the [Test Targets](#) screen, where you can add Ping, TCP Connect, HTTP, and FTP target tests to the current profile.
- **Add Connection Log** opens a Link-Live sharing screen that allows you to custom name the log file before saving to the test result.



Connection Log Name

20191022\_122355



SAVE TO TEST RESULT

Tap the field to enter your desired log name, and tap **SAVE TO TEST RESULT** to upload.

- **Add Comments** also opens a Link-Live [sharing](#) screen where you can enter comments.

Comment

Conference Room

Job Comment

North Office



SAVE TO TEST RESULT


Tap the fields to enter your desired comments, and tap **SAVE TO LAST TEST RESULT** to upload them.

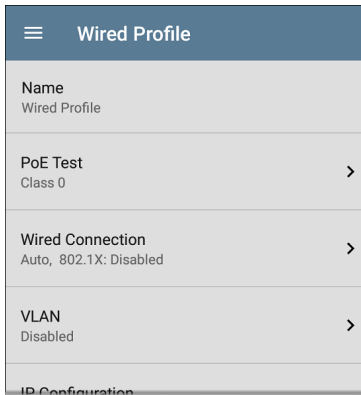
- The **Add Picture** function lets you open the **Gallery** or **Camera** app to select or take a photo that is then uploaded and attached to your test result.


See the [Link-Live App](#) chapter to learn about Link-Live and uploading.

# Wired Profile Settings

These settings control the wired test port connection, PoE test, the thresholds for **Pass/Warning/Fail** results, and any user-added test targets.

Tap the settings icon  on the Wired profile screen, or add a new Wired profile, to configure the profile's settings.



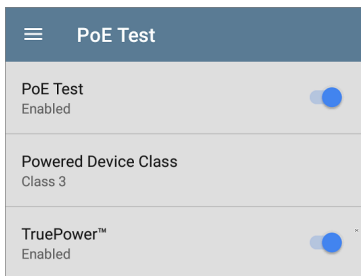
On the **Wired Profile** settings screen, tap each field described below as needed to configure the profile. Changed settings are automatically applied. When you finish configuring, tap the back button  to return to the profile.

## Name

Tap the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Wired Profile screen header.

## PoE Test Settings

Open PoE Test settings to enable or disable PoE and configure the PD Class.





## PoE Test

Tap the toggle button to enable or disable the PoE test portion of the current Wired Profile.

## Powered Device Class

Tap to select a PoE class setting to match your switch's (or active PoE injector's) available class. LinkRunner supports these classes:

- 802.3af Classes 0-3
- 802.3at PoE+ Class 4
- Cisco's UPOE, which can provide up to 51 W
- 802.3bt Classes 5-8

Select **Passive PoE Injector** if you are using a non-IEEE injector.

NOTE: LinkRunner may not receive the total wattage advertised by your switch or injector because of power loss over the cable.

NOTE: LinkRunner automatically negotiates Cisco UPOE over LLDP, up to 51 W. LLDP must be enabled on the switch for negotiation to succeed. If the UPOE Class is selected on your LinkRunner but LLDP is not

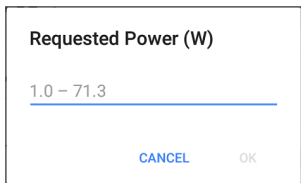
enabled on your Cisco switch, negotiation fails.

## LLDP

This toggle button appears if Class 4 (25.50 W) is selected. Enable this setting if LLDP is enabled on the switch you are testing. Class 4 LLDP must be enabled on the switch for AutoTest to detect it successfully. If the LLDP setting is enabled but your switch does not support LLDP, negotiation fails.

## Requested Power (W)

This setting appears if **UPOE** is selected in the **Powered Device Class** setting shown above or if the Powered Device Class is set to **Passive PoE Injector** and **TruePower** is enabled. Tap to enter a Requested Power other than the default, if needed. If you tap the backspace button on the pop-up number pad and clear the default value, the valid power range is displayed.



## TruePower™

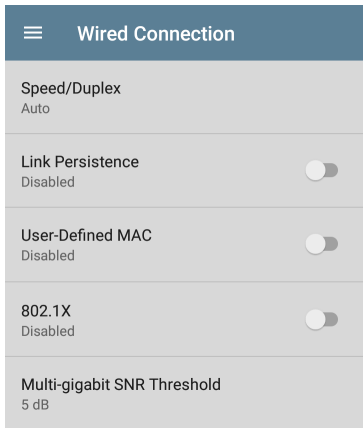
TruePower validates that the Switch (Power Sourcing Equipment) and cabling can provide the requested power under load by applying a load equivalent to the selected class to mimic a Powered Device (PD). Tap the toggle button to enable the TruePower feature.

## General Settings that Affect PoE

See the Wired section in [General Settings](#) for a description of the **Test PoE before Link** setting.

## Wired Connection Settings

Open **Wired Connection** settings to configure speed/duplex, link persistence, user-defined MACs, 802.1X settings, and multi-gigabit SNR threshold.



## Speed/Duplex

Tap to select the speed and duplex option that you want to test your network against. The default is Auto negotiation.

When speed is set to Auto, LinkRunner auto-negotiates to the highest possible speed/duplex supported by the link partner. You can select a fixed speed/duplex for the copper interface. For

10 and 100 Mbps you can optionally force the speed and duplex.

This setting does not force the link speed/duplex on the fiber interface, but does control which speed is attempted first when using a multi-rate SFP. As a result, this setting can enable the test unit to connect faster via fiber.

## Link Persistence

Link Persistence controls product behavior prior to link and also after link goes down.

**Link Persistence and Establishing Link:** When enabled there is no timeout on how long to wait for link to be established. When disabled, the link step fail if not successful in 25 to 30 seconds.

**Link Persistence and Link Dropping:** When enabled and link drops, the unit attempts to relink. When disabled and link drops, the profile is considered done and no further link attempts are done until a Wired Profile is run again.

The default setting for Link Persistence is disabled.

## User-Defined MAC

Tap the toggle field to enable a user-defined MAC for this profile and display the current user-defined MAC definition:



This setting affects the [Wired Test Port](#) only. Tap the toggle switch to enable a user-defined MAC address specifically for this profile. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. (If there is no currently value for this profile, the field shows the user-defined MAC address (if any) defined in the "[Wired](#)" on [page 87](#) section of the General Settings.) Tap the lower field to enter your desired MAC address for the LinkRunner. When this user-defined MAC is enabled, **(User-defined)** appears next to the MAC address on the [About](#) screen and on relevant test result screens.

You can use this feature for tasks such as testing ACL lists (for example, finding out if specific MAC addresses are allowed on the network) or for determining if specific IPv4 addresses should be assigned to specific MAC addresses.

## 802.1X

Tap the toggle field to enable wired 802.1X authentication in the current Profile. Enabling this setting also enables an [802.1X test card](#) on the Wired AutoTest results screen.

The following settings appear when 802.1X authentication is enabled. Enter all necessary credentials, such as EAP type, username and password, or certificate.

802.1X Enabled	<input checked="" type="checkbox"/>
EAP Type PEAP MSCHAP V2	
Username	
Password	
Alternate ID	

## EAP Type

Tap to select a different EAP type if needed. The default is PEAP MSCHAP V2.

## Certificate

This setting appears if one of the following EAP types is selected in the setting above: **EAP TLS**, **PEAP TLS**, or **TTLS EAP TLS**.

See [How to Import a Certificate](#).



## Username

This field appears along with multiple authentication types. Tap the **Username** field to enter your username.

## Password

This field appears along with multiple authentication types. Tap the **Password** field to enter the network password.

## Alternate ID

Enter an Alternate ID if necessary. This is an Advanced Authentication setting.

## Multi-gigabit SNR Threshold


When a Wired Profile links at speeds higher than 1 Gbps, a table appears on the [Link Test screen](#) showing Multi-gigabit Details. This threshold grades SNR measurements on the four twisted pairs. A Minimum SNR below the selected threshold displays a yellow warning condition. The default is 5 dB. If more than one signal is below the Minimum SNR, the signal with the lowest value is shown.

# VLAN Settings



Tap to open the VLAN settings screen. Slide the toggle to the right to enable VLAN testing. Enabling this setting also enables a [VLAN test card](#) on the Wired AutoTest results screen. Once enabled, **VLAN ID** and **VLAN Priority** fields appear. Tap these fields to open a pop-up number pad and enter the correct ID and priority. Tap **OK** to save them.

## Wired Profile

- Wait For Network Traffic**  
Enabled 
- IP Configuration**  
DHCP: Enabled >
- DNS Test**  
www.google.com >
- Gateway Test**  
Timeout Threshold: 100 ms >
- Test Targets**  
1 target(s) >
- Stop After**  
All
- HTTP Proxy**  
Disabled >

## Wait For Network Traffic

Wait for Network Traffic controls whether there is any delay after link comes up before proceeding to the next step. When enabled there

is a delay waiting for packets to be forwarded from the network by the nearest switch. This is useful for switches that are configured to search for networking loops prior to forwarding traffic. On networks with very little traffic, the user may choose to disable this delay. The maximum time to delay is 45 seconds.

## DHCP, DNS, and Gateway Settings

See [DHCP, DNS, and Gateway Tests](#).

### **PING FTP TCP HTTP** Test Targets

Tap the **Test Targets** field to open the Test Targets screen and add custom Ping, TCP Connect, HTTP, or FTP tests to your AutoTest profile.

See [Test Targets for Wired Profiles](#).

## Stop After

This setting directs the Wired Profile to stop testing after the selected test step (**Link**, **Switch**, **DHCP**, **DNS**, **Gateway**, or **All**). The excluded test cards do not appear on the Profile results screen.

## HTTP Proxy

The Proxy control lets you specify a proxy server through which the LinkRunner establishes a network connection. In AutoTest, these settings are used when HTTP Proxy is enabled in an [HTTP](#) or [FTP](#) Test Target.


To use the proxy settings with a web browser, run the Profile, and then, open the web browser while the unit remains linked.

Open the **HTTP Proxy** screen to enable proxy settings.


HTTP Proxy	
Address	Disabled
Port	80 (www-http)
Username	
Password	


Tap each field to open a pop-up keyboard and enter the appropriate **Address**, **Port**, **Username**, and **Password**. Tap **OK** to save your entries.

# DHCP, DNS, and Gateway Tests

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

These tests are included in [Wired](#) AutoTest Profiles.


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

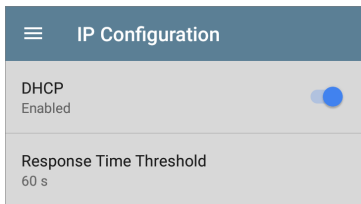
Tap [blue links](#) or the blue action overflow icon  on the test results screens for additional actions.

## DHCP or Static IP Test

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

### DHCP Settings – IP Configuration

Access the DHCP test settings from the Wired Profile settings or by tapping the settings button  on the DHCP test results screen.



By default, DHCP is enabled. On the **IP Configuration** screen, you can adjust the **DHCP Response Time Threshold** or configure a **Static IP Address**.



## DHCP

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

### **(DHCP only) Response Time Threshold**

This field only appears if DHCP is enabled. The Response Time Threshold controls how long the LinkRunner waits for a DHCP server response before failing the Link and DHCP tests.

## Static IP Address

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

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

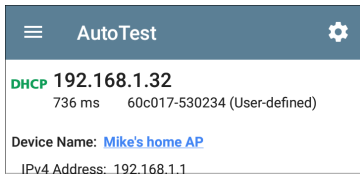
When DHCP is enabled, the DHCP test card and results screen are displayed in the Profile.



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

**DHCP** 10.250.2.168

&lt;1 ms

Device Name: [COS\\_DEV\\_SW1](#)

IPv4 Address: 10.250.0.2

MAC Address: Cisco:001cb1-da2cc6

**Results**

Offered: 10.250.2.168

Accepted: 10.250.2.168

Subnet Mask: 255.255.252.0

Subnet: 10.250.0.0/22

Lease Time: 1 day 0 seconds

Expires: 4/26 2:39 PM

Relay Agent: --

Metric	Result
 Offer	<1 ms
 Acknowledge	<1 ms
Total Time	<1 ms
Threshold	60 s

End User Response Time

50.0 %  Offer Acknowledge

**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 LinkRunner

**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

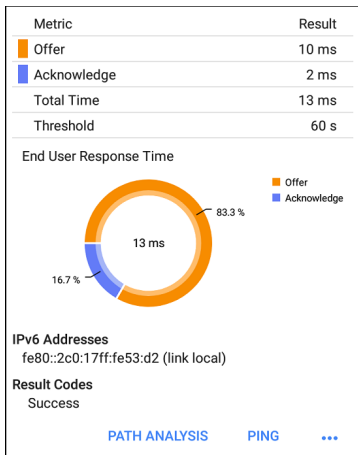
**Lease Time:** The amount of time the IP address is leased to the LinkRunner by the DHCP server

**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 LinkRunner sent the discovery and received an address offer from the DHCP server

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

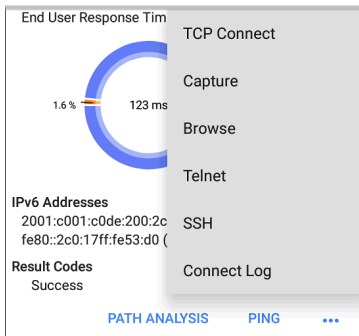
**Total Time:** Total amount of time consumed by the DHCP process

**Threshold:** The DHCP Response Time Threshold from the DHCP test settings, which controls how long the LinkRunner 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)

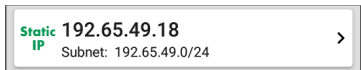


The additional actions available on the DHCP test screen include opening the [Path Analysis](#), [Ping/TCP](#), or [Capture](#) apps populated with the DHCP server address, browsing to the IPv4 address in the web browser, starting a [Telnet](#) or [SSH](#) session, or viewing the [Connect Log](#).

## Static IP Test Results

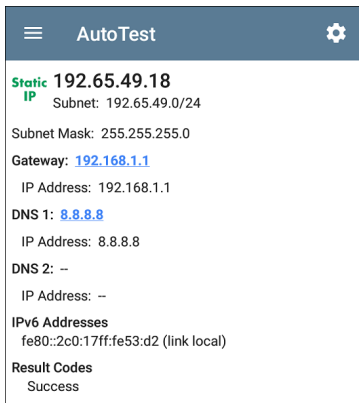
If DHCP is disabled, the DHCP test becomes a "Static IP" test and the Subnet and addresses that were entered in the DHCP test settings are displayed.





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: [BRW2C6FC94A974E](#)

MAC Address: HonHai:2c6fc9-4a974e

**IPv6 Addresses**

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

**Result Codes**

IP address already in use (11)

**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.

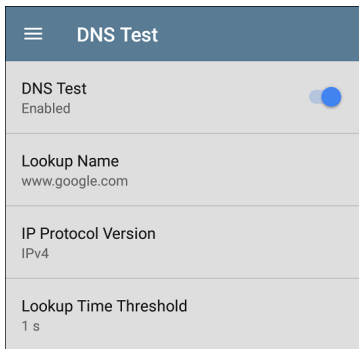
**MAC Address:** MAC of the device using the IP address

## 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 LinkRunner obtains DNS addresses through DHCP or static address configuration.

### DNS Test Settings



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

## DNS Test

If desired, you can tap the top field on the DNS Settings screen and switch the toggle to disable the DNS test in your current AutoTest. When this setting is disabled, the DNS card does not appear on the main AutoTest results screen, and the following settings are hidden.

### 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

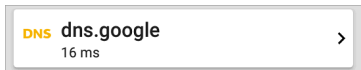
Tap the field to switch between IPv4 and IPv6.

### Lookup Time Threshold

This threshold controls how long the LinkRunner 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.

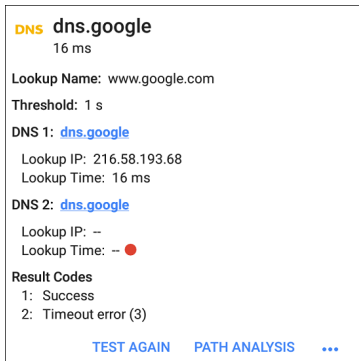
## DNS Test Results

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

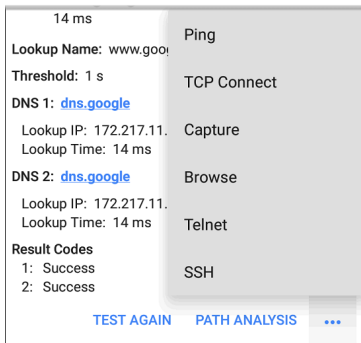
**Threshold:** Lookup Time Threshold from the DNS test settings

**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



14 ms

Lookup Name: www.google.com

Threshold: 1 s

DNS 1: [dns.google](#)

Lookup IP: 172.217.11.100

Lookup Time: 14 ms

DNS 2: [dns.google](#)

Lookup IP: 172.217.11.100

Lookup Time: 14 ms

**Result Codes**

1: Success

2: Success

Ping

TCP Connect

Capture

Browse

Telnet

SSH

TEST AGAIN PATH ANALYSIS ...

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.

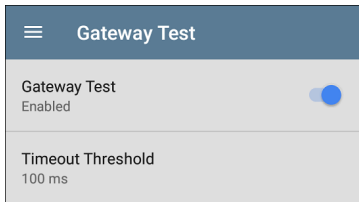


## Gateway Test

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



### Gateway Test

If desired, you can tap the top field on the Gateway Test screen and switch the toggle to disable the Gateway test in your current AutoTest. When this setting is disabled, the Gateway card does not appear on the main AutoTest results screen, and the following setting is hidden.

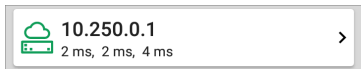


## Timeout Threshold

The only other setting for the Gateway Test is the timeout threshold, which indicates how long the LinkRunner 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.

## Gateway Test Results

LinkRunner 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 LinkRunner'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

The screenshot shows the 'AutoTest' application interface. At the top, there is a blue header with a hamburger menu icon on the left, the text 'AutoTest' in the center, and a gear icon on the right. Below the header, the main content area has a white background. It starts with a green cloud icon and a server rack icon next to the text 'COS\_DEV\_SW1'. Below this, it shows '2 ms, 2 ms, 3 ms'. The 'IPv4 Gateway Name' is 'COS\_DEV\_SW1' (underlined). Below that, it lists 'IPv4 Address: 10.250.0.1' and 'MAC Address: Cisco:00000c-07ac01'. The 'IPv6 Gateway Name' is 'Andromeda Automation Procurve' (underlined). The 'Protocols' section lists 'RIP, OSPF, HSRP, Statically Configured Router, Proxy ARP Agent, Virtual Router (HSRP)'. The 'Ping Results' section shows 'Response Times: 2 ms, 2 ms, 3 ms' and 'Threshold: 100 ms'. The 'Result Codes' section lists '1: Success', '2: Success', and '3: Success'. At the bottom, there are three blue buttons: 'TEST AGAIN', 'PATH ANALYSIS', and '...'.

**AutoTest**

**COS\_DEV\_SW1**  
2 ms, 2 ms, 3 ms

**IPv4 Gateway Name:** COS\_DEV\_SW1

IPv4 Address: 10.250.0.1  
MAC Address: Cisco:00000c-07ac01

**IPv6 Gateway Name:** Andromeda Automation Procurve

**Protocols:** RIP, OSPF, HSRP, Statically Configured Router, Proxy ARP Agent, Virtual Router (HSRP)

**Ping Results**  
Response Times: 2 ms, 2 ms, 3 ms  
Threshold: 100 ms

**Result Codes**  
1: Success  
2: Success  
3: Success

**TEST AGAIN**    **PATH ANALYSIS**    ...

**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 LinkRunner 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

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

Gateway Name: [COS-IT-SW1](#)

IPv4 Address: 172.24.0.1  
MAC Address: Cisco:6c:00:01:00:00  
IPv6 Address: --

Protocols: Statically Configured

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

**Result Codes**  
1: Success  
2: Success  
3: Success

Ping  
TCP Connect  
Capture  
Browse  
Telnet  
SSH

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

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.

# Test Targets for Wired AutoTests

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

AutoTest

Target tests are user-assignable endpoints to which LinkRunner 10G 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](#)

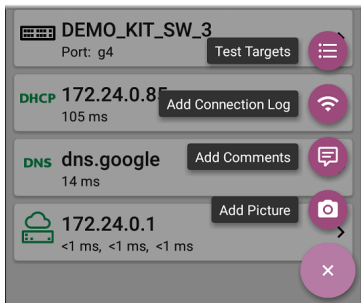
[TCP Connect](#)

[HTTP](#)

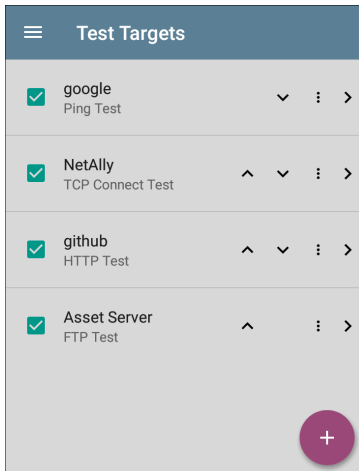
[FTP](#)

## 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 Profile](#) results screens.





The Test Targets screen lists all of the defined and saved Test Targets. Checked boxes indicate the Test Targets that are enabled in the current Profile. Remember, Test Targets can be added to and used in any number of Wired Profiles.

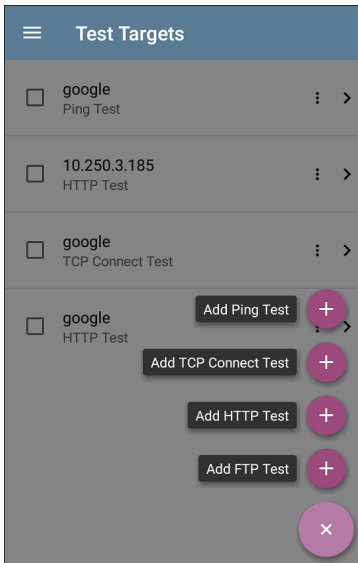


On the Test Targets screen, you can perform these actions:

- 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.





- 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](#)
- [FTP Test](#)

## 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.

**PING google**

9 ms, 33 ms, --

**Device Name:** [172.217.1.196](#)

IPv4 Address: 172.217.1.196

MAC Address: --

**Results**

Lookup Time: 3 ms

Response Times: 9 ms, 33 ms, -- ●

Threshold: 250 ms

**Result Codes**

1: Success

2: Success


3: Timeout error (3)

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

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

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 ANALYSIS](#) to open the Path Analysis app. The path Destination is configured with the current target.
- Tap the action overflow icon  to open the listed apps or tools with the target pre-populated, for example:
  - Open the [Ping/TCP](#) app with the current target address.
  - Run a packet [Capture](#) on traffic from the test target.
  - Browse to the target URL on the internet with your [web browser](#) app.

## 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).

## Ping Test Settings

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

**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.

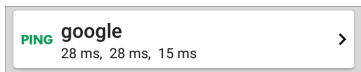
**IP Protocol Version:** IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

**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 LinkRunner waits for a response from the target before failing the test.

## 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

**PING google**  
4 ms, 4 ms, 5 ms

**Device Name:** [www.google.com](http://www.google.com)

IPv4 Address: 172.217.12.4  
MAC Address: --

**Results**  
Lookup Time: 1 ms  
Response Times: 4 ms, 4 ms, 5 ms  
Threshold: 1 s

**Result Codes**  
1: Success  
2: Success  
3: Success

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

**Device Name:** Hostname or address of the target device

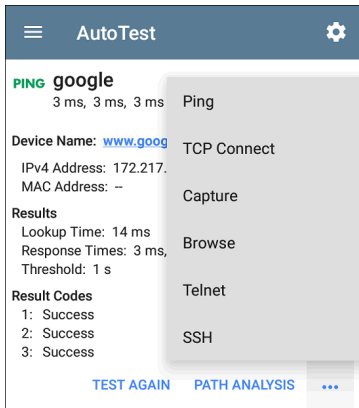
- **IPv4 or IPv6 Address:** IP address of the target device
- **MAC Address:** Target device's MAC address. The two dashes -- indicate that no MAC address was provided from the server.



## Results

- **Lookup Time:** How long it took to resolve the URL into an IP address
- **Response Times:** How long it took for the LinkRunner to receive a response from the target after sending each of the three Pings
- **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



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

☰ TCP Connect Test	
<b>Name</b>	NetAlly
<b>Device Name</b>	NetAlly.com
<b>IP Protocol Version</b>	IPv4
<b>Port</b>	80 (www-http)
<b>Timeout Threshold</b>	1 s

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

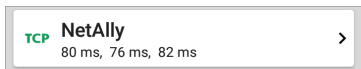
**Device Name:** Enter the IP address or URL of the target you want to test. If you enter an IP address, the DNS lookup portion of the test is skipped.

**IP Protocol Version:** IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

**Port:** Specify the TCP port number for the LinkRunner to use to connect to the target.

**Timeout Threshold:** This threshold controls how long the LinkRunner waits for a response from the target before failing the test.

## 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

AutoTest

**TCP** **NetAlly**  
50 ms, 44 ms, 42 ms

Device Name: [ip-184-168-221-49.ip.secureserver.net](http://ip-184-168-221-49.ip.secureserver.net)

IPv4 Address: 184.168.221.49  
MAC Address: --  
Port: 80 (www-http)

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

**Result Codes**  
1: Success  
2: Success  
3: Success

TEST AGAIN    PATH ANALYSIS    ...

**Device Name:** DNS name of the device tested

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

**MAC Address:** Device's MAC address. The 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 LinkRunner 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

## HTTP Test

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 criteria based on responses and return code in addition to the time threshold.

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

## Name

This field allows you 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 LinkRunner 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	
Response Must Not Contain	
Return Code 200 - OK	
HTTP Proxy Disabled	<input type="checkbox"/>

## 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 LinkRunner receives a different return code, the test fails.

## 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

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

**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

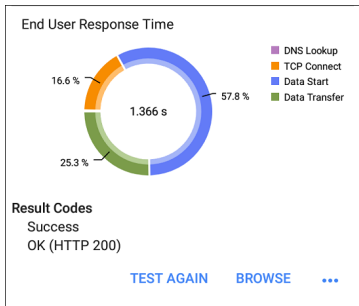
**Total Time:** The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

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

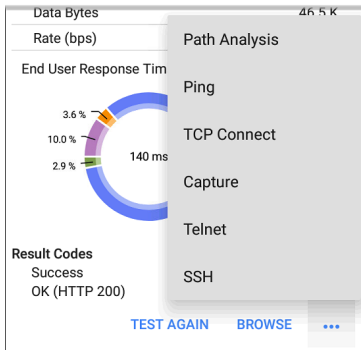
**Rate (bps):** The measured data transfer rate



**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.

## FTP Test

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.



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

## 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 LinkRunner 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 LinkRunner.
- 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 LinkRunner, and the test string is repeated to produce the set file size.

## Response Time Threshold

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

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

## 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.

## 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

Metric	Result
<b>FTP Asset Server</b>	
171 ms	
Device Name: <a href="#">10.250.2.218</a>	
IPv4 Address: 10.250.2.218	
MAC Address: --	
Get File: /internal/iperf3	
<b>Results</b>	
Ping	50 ms
DNS Lookup	--
TCP Connect	44 ms
Data Start	116 ms
Data Transfer	10 ms
Total Time	171 ms
Threshold	60 s
Data Bytes	24 K
Rate (bps)	1.2 M

**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.

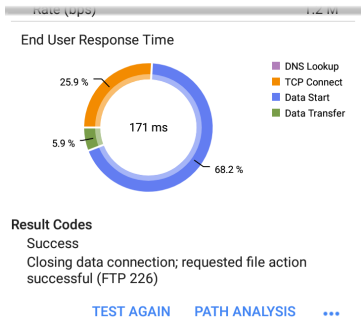
If the Response Time Threshold is exceeded during a step in the test, the current phase of the test (DNS, Lookup, TCP Connect, Data Start, or Data Transfer) is denoted with a red dot, and the rest of the test is aborted.

**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.



## 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.

**cos-lab-vm-cisco**  
Router  
Name  
SNMP: cos-lab-vm-cisco  
Address  
IPv4: 10.250.0.11 (Reachable)  
MAC: Cisco:40f4ec-f47681  
Protocols: Statically Configured Router  
Attributes: Discovered via SNMP, Switch, Port Aggregation

**Addresses** → Ping/TCP  
IPv4: 2 MAC: 1

**VLANs** Capture (Wired)  
1, 196, 500, 508, 526, 560

**Interfaces** Browse  
Up: 2 Down: 41

**MIB** SNMP

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

☰ Ping START ⚙️


**PING**  
**TCP** 10.250.0.11

Device Name:  
IP Address: 10.250.0.11  
MAC Address: --  
Interface: Any Port

Results

Started

# Configuring Ping/TCP Settings Manually

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

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

**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 LinkRunner 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):** This setting only appears if the **Ping** Protocol is selected. It specifies the total size of the payload and header the LinkRunner 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:** This setting only appears if the **Ping Protocol** is selected. It controls how much time passes between each Ping sent from the LinkRunner. 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:** This setting only appears if the **TCP Connect Protocol** is selected. It indicates the port number your LinkRunner 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 LinkRunner waits for a response from the target before the test is failed.


**Do Not Fragment:** This setting only appears if the **Ping Protocol** is selected. Tap the toggle



button to enable. See the Frame Size setting description above.

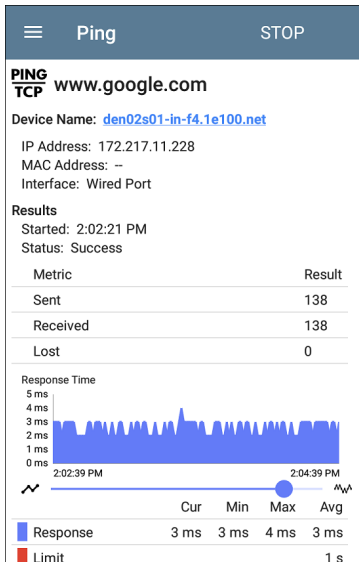
## Running Ping/TCP Tests

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 LinkRunner 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 LinkRunner 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



## Capture App

Packet capture is the process of recording network traffic in the form of packets as data streams back and forth over 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.


## 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 LinkRunner.

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.

Capture Settings	
<b>File Size Limit</b>	1 MB
<b>Slice Size</b>	Full Packet
<b>Wired Filters</b>	
<b>MAC</b>	Disabled
<b>IP</b>	Disabled
<b>VLAN</b>	Disabled
<b>Port</b>	Disabled

**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 1000 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 Full Packet.

## 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.

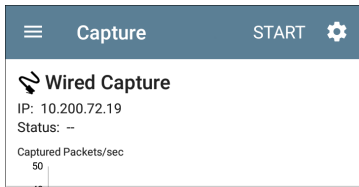
**VLAN:** Enter a VLAN number to capture only traffic tagged for that VLAN.

**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 LinkRunner 10G captures all traffic *except* traffic to and from 10.250.0.70 on port 80.

# Running and Viewing Captures

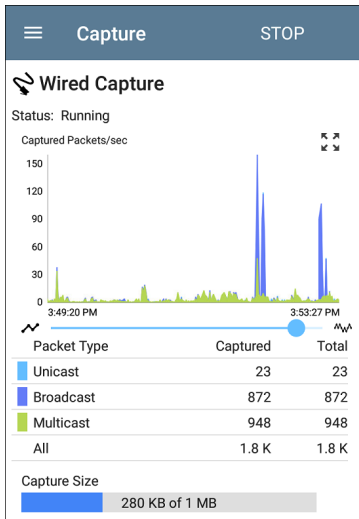
To start Capturing, tap **START** at the top of the app screen.



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.

View the real-time status of the capture as it is running. If you navigate away from the Capture app, the capture process continues to run in the background until the File Size Limit (in [Capture Settings](#)) is reached.

Tap **STOP** to stop the running capture before it reaches the File Size Limit.



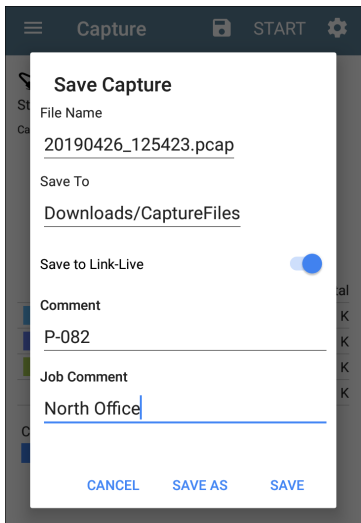
The graph plots the type and number of packets being captured while the capture is running and includes Unicast, Broadcast, and Multicast packet types.

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.

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

Tap the Save icon  to reopen this dialog.



**Save Capture**

File Name  
20190426\_125423.pcap

Save To  
Downloads/CaptureFiles

Save to Link-Live

Comment  
P-082


Job Comment  
North Office

CANCEL SAVE AS SAVE

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 LinkRunner file system, but you can also save them to a Micro SD card or 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.



## Discovery App

The LinkRunner 10G 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. Devices are discovered in the local broadcast domains where the LinkRunner is physically connected. By default, discovery processes run out of both **test and management ports**.

Note: AllyCare is required to use this application. Your LinkRunner must be **claimed**. Please visit: [NetAlly.com/AllyCare Support and Features](https://www.netally.com/AllyCare).

# 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](#)

[Main Discovery List Screen](#)

[Discovery Details Screens](#)

[Device Types](#)

[Device Names and Authorization](#)

[Discovery Settings](#)

[Problem Settings](#)

[TCP Port Scan Settings](#)



# Introduction to Discovery

Discovery finds, classifies, and displays 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 LinkRunner'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

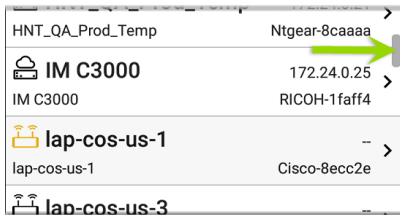
The main Discovery screen lists all the devices the LinkRunner has discovered.

Discovery (589)		🔍	⋮
🔍	↑	Name	▼
	<b>Andromeda Automati...</b>	10.250.3.224	>
	Andromeda Automation Procurve	HP-235cc0	
	<b>LinkRunner_10G_540...</b>	192.168.0.109	>
--		NetAlly-540025	
	<b>Cetus</b>	10.250.2.166	>
	Cetus	Dell-faa680	
	<b>Cisco2500WLC</b>	10.250.3.235	>
	Cisco2500WLC	Cisco-556c80	
	<b>cos-lab-ad.netally.eng</b>	--	>
	cos-lab-ad.netally.eng	VMware-678cc2	
	<b>cos_dev_sw27_huawei</b>	10.250.0.12	>

Like in AutoTest and other LinkRunner 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, support 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.

Total number of discovered devices

Discovery (589) Refresh Discovery

Discovery Settings

Filter

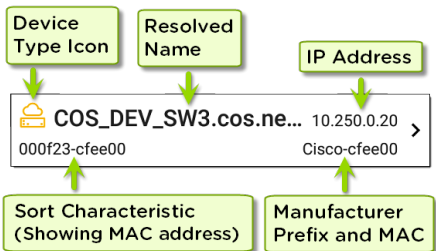
Sort

Touch a card to view device details.

Name	IP Address	MAC Address
AndroLinkSysWav	10.250.2.147	kin-454655
Andromeda Automati...	10.250.3.224	HP-235cc0
Angela's EtherScope ...	10.250.2.139	NetAlly-530000
Cetus	10.250.2.166	Dell-faa680
Cisco2500WLC	10.250.3.235	Cisco-556c80
cos-lab-ad.netally.eng	-	VMware-678cc2
COS_DEV_SW4	10.250.0.4	Dell-b63fb6
cos_dev_sw27_huawei	10.250.0.12	


## Discovery List Cards

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

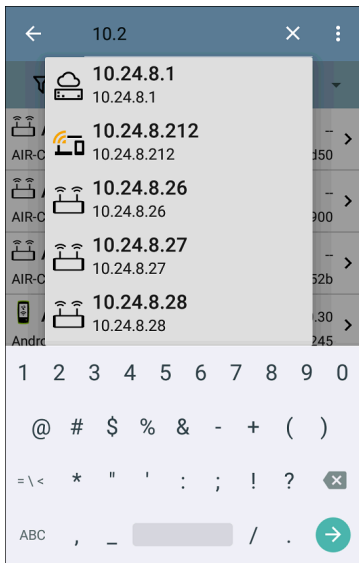


The lower left field displays the characteristic by which the Discovery list is currently sorted. In the image above, the list is sorted by MAC address. See [Discovery Sorts](#) in this topic for more about sorting.

## Searching the Discovery List


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

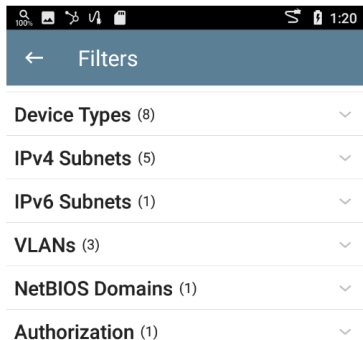
screen to search discovered devices.





## Filtering the Discovery List

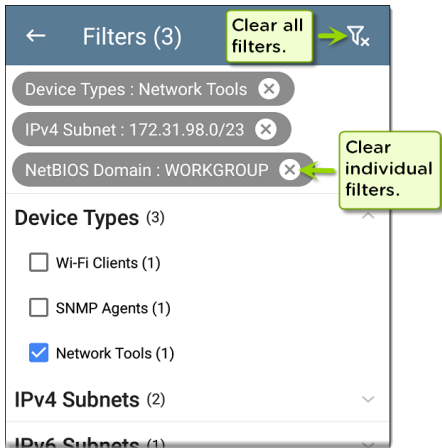
Tap the filter button  near the top left of the main Discovery screen to set filters that control which devices are displayed in the list.



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.

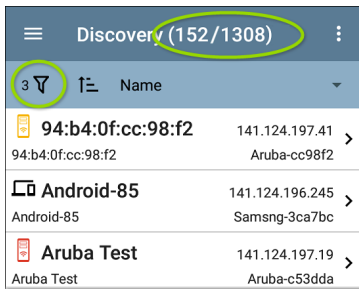


When filters are selected, those active filters are displayed at the top of the Filters screen.



- Tap the **x** 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).

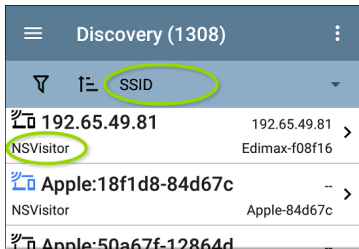
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

## 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 the devices associated with the "NSVisitor" SSID are sorted together. Individual devices on the same SSID are sorted numerically and alphabetically.

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.

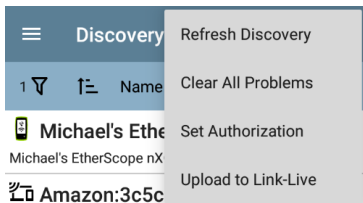
## Security Auditing – Batch Authorization

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 SSIDs 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.

## Set Authorization

1077 of 1077 clients selected

- Authorized (5)
- Neighbor (0)
- Flagged (0)
- Unknown (0)
- Unauthorized (17)
- Unspecified (1055)

CANCEL

OK

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

Select the appropriate security category. As in the example, if these devices belong to other offices, select **Neighbor**, and then tap the **OK** button.

### Set Authorization

13 of 96 devices selected

Authorized (0)

Neighbor (0)

Flagged (0)

Unknown (0)

Unauthorized (0)

Unspecified (13)

**CANCEL** **OK**

You can now sort the list of discovered devices and clearly identify the security category of the




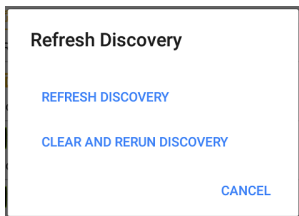
devices. Devices from other offices are identified as: Neighbor

Discovery (32)		🔍	⋮
🔼	⏮	Authorization	▾
-		localAdmin-4bd5aa	
📶	<b>localAdmin:6623ae-7b6756</b>	-	>
-		localAdmin-7b6756	
📶	<b>localAdmin:7223ae-7b6757</b>	-	>
-		localAdmin-7b6757	
📶	<b>localAdmin:86da88-a8d0d6</b>	-	>
-		localAdmin-a8d0d6	
📶	<b>localAdmin:d663fc-5b4f38</b>	-	>
-		localAdmin-5b4f38	
📶	<b>MXCHIP:c89346-87b4c4</b>	-	>
-		MXCHIP-87b4c4	
📶	<b>Netgear:803773-e4e2d3</b>	-	>
-		Netgear-e4e2d3	
📶	<b>Netgear:dcef09-a63460</b>	-	>
-		Netgear-a63460	

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.

**Link-Live**

by NetAlly



Discovery Snapshot Name

20190802\_131842

Comment

1st Floor

Job Comment

Psych Building

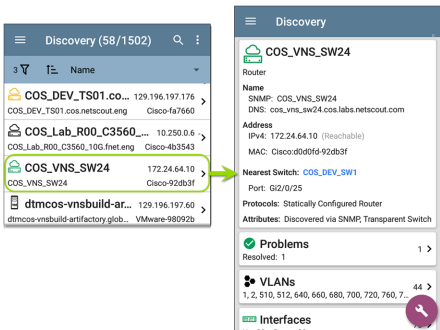
SAVE TO ANALYSIS FILES

See the [Link-Live chapter](#) for more information.


# 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 LinkRunner was able to discover. In other words, only the discoverable information for each device is shown on the Details screen.


 **Discovery**


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

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

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

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

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



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

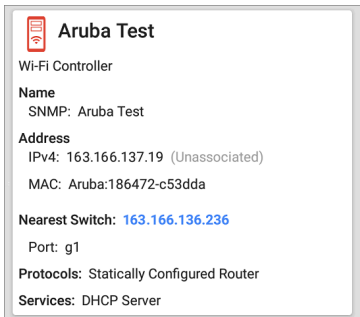
Each Details screen shows additional information about the selected device, any Problems detected by the LinkRunner, and counts for other connected or corresponding network elements.


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 LinkRunner can discover.

## Top Details Card

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



 **Aruba Test**

Wi-Fi Controller

**Name**  
SNMP: Aruba Test

**Address**  
IPv4: 163.166.137.19 (Unassociated)  
MAC: Aruba:186472-c53dda

**Nearest Switch:** [163.166.136.236](#)

Port: g1

**Protocols:** Statically Configured Router

**Services:** DHCP Server

The top of the card shows the device type(s) and icon (a Wi-Fi Controller with a **Failure or Error** 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 LinkRunner 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 .

 **Discovery**

 **Cisco3702**

Lightweight AP

**Name**  
AP: Cisco3702  
SNMP: Cisco3702

**Address**  
IPv4: 10.250.3.69 (Reachable)  
IPv6: 2001:c001:c0de:500:ba38:61ff:fe6e:1ae0  
MAC: [Cisco:b83861-6e1ae0](#)

**802.11**  
Channels: 1, 64  
Type: 802.11ac

**Nearest Switch:** [~ Unknown Switch 3 ~](#)

**Wi-Fi Controller:** [Cisco2500WLC](#)  
10.250.3.235

**Last Seen:** 5:23:20 PM

The Nearest Switch and Wi-Fi Controller links open a Discovery app Details screen for those devices.

## Data Fields on the Top Details Card

The following fields may appear on the top card on a Device Details screen, depending on the device type and the information LinkRunner was able to discover:

**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, BSSID, 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

**Wi-Fi Controller:** Name and address of the Wi-Fi Controller for a Lightweight AP

**AP:** Access Point to which the device is connected

**SSID:** Name of the network on which the device is operating

**Security:** AP's security type

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

**Virtual Machine:** Name of the virtual machine

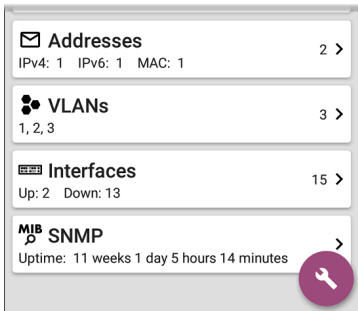
**Guest OS:** Operating system running on the virtual machine

**Memory Reservation:** Amount of memory reserved for the virtual machine

**Last Seen:** Time at which LinkRunner 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.

Addresses (3)	
↑	Address
IPv4 10.250.0.1	BSSID /22
10.250.0.120	549 >
IPv6 2001:c001:c0de	IP Address ...
2001:c001:c0de	549 >
IPv6 fe80::16	IPv6 Address
fe80::1618:77ff::	Mfg-MAC Address 549 >
	MAC Address

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

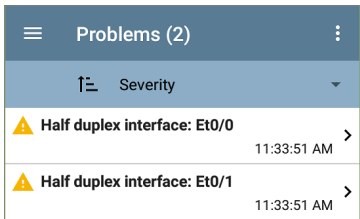
Remember, you can tap any card with a right pointing arrow ➤ to open a new screen with more information about the device or characteristic.

## 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.

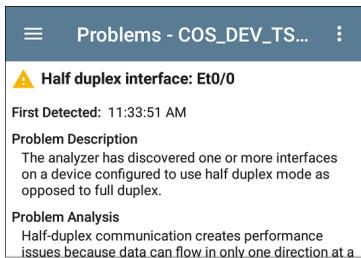


Tap the Problems card to view the Problems list screen (unless only 1 Problem is detected, in which case, the detailed Problem description opens, skipping the list screen).




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.

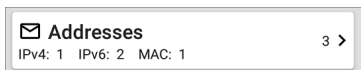


The screenshot shows a mobile application interface for 'Problems - COS\_DEV\_TS...'. At the top left is a hamburger menu icon, and at the top right is a vertical ellipsis (three dots) icon. Below the header, there is a yellow warning triangle icon followed by the text 'Half duplex interface: Et0/0'. Underneath this, it says 'First Detected: 11:33:51 AM'. The section is titled 'Problem Description' and contains the text: 'The analyzer has discovered one or more interfaces on a device configured to use half duplex mode as opposed to full duplex.' Below that is the 'Problem Analysis' section with the text: 'Half-duplex communication creates performance issues because data can flow in only one direction at a'.

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 screenshot shows a mobile application interface for 'Addresses'. At the top left is an envelope icon, followed by the text 'Addresses'. At the top right is the text '3 >'. Below this, it says 'IPv4: 1 IPv6: 2 MAC: 1'.



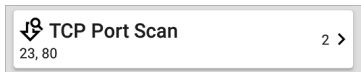
The Addresses card displays the number of each type of address discovered: IPv4, IPv6, MAC, and/or BSSID. Tap to view the addresses and related information.

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

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

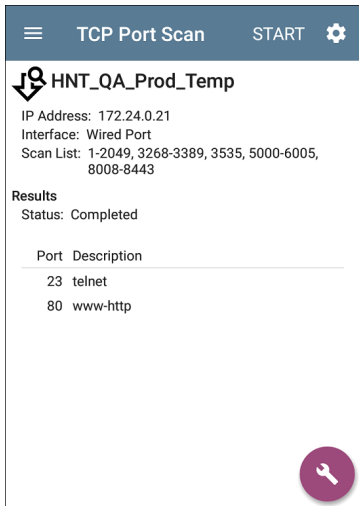
## TCP Port Scan

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 screenshot shows the 'TCP Port Scan' results screen. At the top, there is a dark blue header with a hamburger menu icon on the left, the title 'TCP Port Scan' in the center, and the word 'START' and a gear icon on the right. Below the header, the device name 'HNT\_QA\_Prod\_Temp' is displayed with a downward-pointing arrow icon to its left. Underneath, the scan details are listed: 'IP Address: 172.24.0.21', 'Interface: Wired Port', and 'Scan List: 1-2049, 3268-3389, 3535, 5000-6005, 8008-8443'. A section titled 'Results' follows, with the status 'Status: Completed'. Below this is a table with two columns: 'Port' and 'Description'. The table contains two entries: port 23 for 'telnet' and port 80 for 'www-http'. In the bottom right corner of the screen, there is a circular purple button with a white wrench icon.

☰ TCP Port Scan START ⚙️

↓ HNT\_QA\_Prod\_Temp

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

**Results**  
Status: Completed

Port	Description
23	telnet
80	www-http

🔧

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

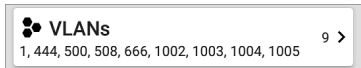
**Status:** Current status of the port scan

**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.

COS_DEV_SW33	
 <b>VLANs</b>	
VLAN	Description
1	default
444	VLAN0444
500	VLAN0500
508	LabWiFi
666	VLAN0666
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

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

## Interfaces

Interface are discovered using SNMP.

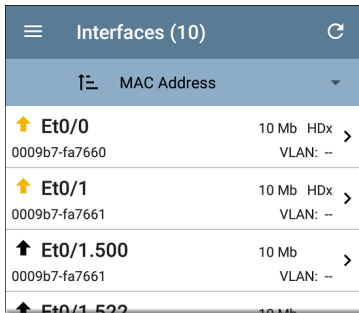
 <b>Interfaces</b>	171 >
Up: 20   Down: 151	

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.

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

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.



The screenshot shows a mobile application interface for network discovery. At the top, there is a header bar with a hamburger menu icon on the left, the text "Interfaces (10)" in the center, and a refresh icon on the right. Below the header is a filter bar with a list icon and the text "MAC Address" followed by a dropdown arrow. The main content is a list of network interfaces, each with a status icon (upward arrow), name, MAC address, speed, type, and VLAN information, along with a right-pointing chevron for more details.

MAC Address	Speed	Type	VLAN
0009b7-fa7660	10 Mb	HDx	--
0009b7-fa7661	10 Mb	HDx	--
0009b7-fa7661	10 Mb		--
0009b7-fa7661	10 Mb		--

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

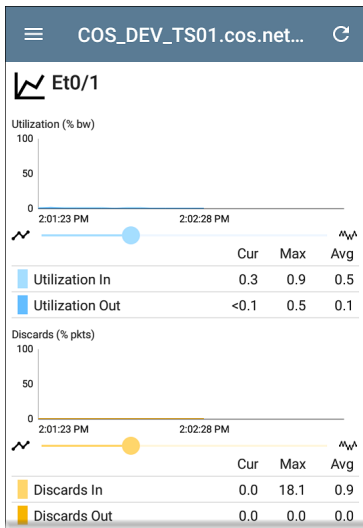
The screenshot shows a mobile application interface for network discovery. At the top, there is a blue header bar with a hamburger menu icon on the left, the text 'COS\_DEV\_TS01.cos.net...' in the center, and a refresh icon on the right. Below the header, the main content area is divided into three sections. The first section is titled 'Et0/1' with an upward-pointing arrow icon. It contains the text 'DOT1Q Trunk to CISCO\_3750\_PoE COS\_DEV\_SW2 f...', 'Status: up', 'Speed: 10 Mb', 'Duplex: HDx', 'MTU: 1500', 'Connected Device: COS\_DEV\_SW1', 'Port: Gi2/0/30', and 'Address' with 'MAC: Cisco:0009b7-fa7661'. The second section is titled 'Devices' with a square icon and shows '0' devices with a right-pointing arrow. The third section is titled 'Statistics' with a line graph icon and shows 'Util: 0.3 %', 'Discards: 0.0 %', and 'Errors: 0.0 %' with a right-pointing arrow.

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

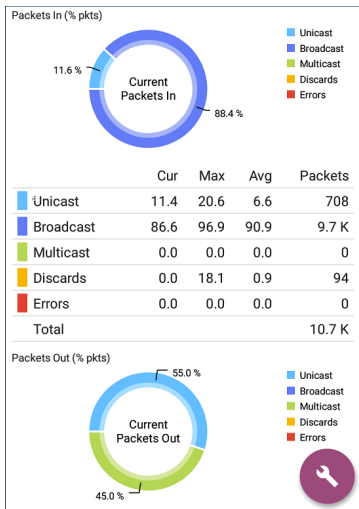


From this screen, you can tap the lower cards to review any discovery **VLANs** and **Devices** for the Interface as well as graphs of the Interface **Statistics**.



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

 **MIB SNMP**

Uptime: 5 weeks 6 days 2 hours 57 minutes



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



COS\_DEV\_SW34

 **MIB SNMP**
**SNMP System Group**

Uptime: 5 weeks 6 days 2 hours 58 minutes

Manufacturer: Cisco

Model: cat4500e

Serial Number: FOX1407GRJA

HW Version: V02

SW Version: 15.2(2)E7

**Description:**

Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICES-M), Version 15.2(2)E7, RELEASE SOFTWARE (fc3)

**Technical Support:**

<http://www.cisco.com/techsupport>

Copyright (c) 1986-2017 by Cisco Systems, Inc.

Compiled Wed 12-Jul-17 14:36 by

**SNMP**

Type: SNMP v1/v2/v3

Engine ID: 80000009030068efbd6f4b80

Communication: SNMP v2

Using: Default Community String: public

**SNMP 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 LinkRunner 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 LinkRunner may be unable to directly identify the connected switch, the devices connected to it provide clues about where the switch is operating.




 **Connected Devices**

8 >

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.


Connected Devices (8)		
	IP Address	
 <b>COS_DEV_SW1</b> 10.250.0.1	Gi1/0/38 Cisco-07ac01	>
 <b>10.250.2.143</b> 10.250.2.143	-- NetAlly-02506e	>
 <b>10.250.2.177</b> 10.250.2.177	-- TRENDn-af1e30	>
 <b>10.250.3.32</b> 10.250.3.32	-- NetAlly-02506e	>

## Resources

 **Resources** >  
 CPU: 28% Memory: 35%

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.

COS_DEV_SW34		
 Resources		
	Cur	Max
CPU %	12	12
Memory %	60	60
Last Update: 1:44:22 PM		

By default, LinkRunner 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](#).

## SSIDs

The SSIDs card appears in the Details for [Wi-Fi Controllers](#). This information is gathered via SNMP.



This card shows the number of SSIDs gathered from SNMP. Tap the card to view the list of SSIDs.

Cisco2500WLC		
SSIDs		
SSID	Security	VLAN
✓ CiscoQATest-maana	WPA2-P, WPA-P	--
✓ Cisco WEP64 OA	WEP	--
✓ aa-Cisco-Wep	WEP	--
✓ aonly	WPA2-P, WPA-P	--
✓ Cisco ISE	WPA2-E	--
✓ RF Chamber	WPA2-P, WPA-P	--
✓ Lobo	WPA2-P, WPA-P	--
✓ COS Cisco Captive Portal	Web	--
✗ Portal Test	Web	--
✓ [Cisco Hidden]	WPA2-P	--
✓ Cisco 2.4G	WPA2-P	--

On the SSIDs screen, each SSID is shown with its Security type(s) and any VLANs. SSIDs with a checkmark to the left are enabled, and those with an ✗ are disabled.



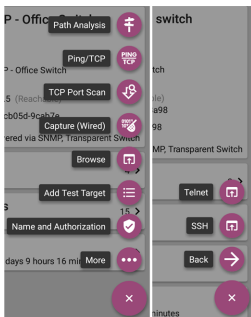
## Discovery App Floating Action Menu

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 [Path Analysis](#), [Ping/TCP](#), or [Capture](#)

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 **Browse** to open the Chromium browser.







- 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 or BSSID, 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).

 **Discovery**

 **Rack5SW1.fnet.eng**  
Router


**Name**  
SNMP: Rack5SW1.fnet.eng


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



**Nearest Switch:** [COS\\_DEV\\_SW1](#)  
Port: Gi2/0/39

**Protocols:** Statically Configured Router

**Attributes:** Discovered via SNMP, Transparent Switch

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

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

 **Interfaces**   
Up: 12    Down: 30

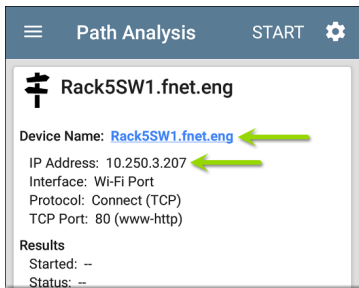
When you open the FAB and select a different app, such as Path Analysis, only the address and name listed at the top of the Details screen are populated in the Path Analysis app.




 **Rack5SW1.fnet.eng**  
Router

**Name**  
SNMP: Rack5SW1.fnet.eng ←

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



☰ **Path Analysis** START ⚙️

 **Rack5SW1.fnet.eng**

**Device Name:** [Rack5SW1.fnet.eng](#) ←

IP Address: 10.250.3.207 ←

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

**Results**  
Started: --  
Status: --

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

## Device Types

The Discovery app lists and analyzes the types of devices explained in this section. Different data may be available to the LinkRunner 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 represent an example of the data Discovery that may display for each device type.

# Routers

LinkRunner discovers IP routers by monitoring traffic and querying hosts.

 **Discovery**

---

 **COS\_DEV\_SW34**  
Router

**Name**  
SNMP: COS\_DEV\_SW34


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

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


**Protocols:** Statically Configured Router

**Attributes:** Discovered via SNMP, Transparent Switch


---


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

---

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


---


 **SNMP** >



# Switches

Switches are also discovered by monitoring traffic and querying hosts.

 **Discovery**


 **cos-dev-sw18-poe**


Switch


**Name**  
SNMP: cos-dev-sw18-poe



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

**Attributes:** Discovered via SNMP, Transparent Switch

 **Addresses** 2 >  
IPv4: 2 MAC: 2

 **VLANs** 37 >  
1, 11, 196, 500, 502, 504, 508, 510, 511, 518, ...

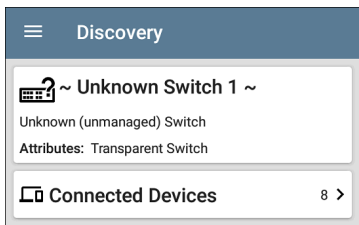
 **Interfaces** 38 >  
Up: 9 Down: 29

 **SNMP**   
Uptime: 27 weeks 2 days 7 hours 25 minutes

## Unknown Switches

Unknown switches are detected indirectly by analyzing traffic going through surrounding switches. The LinkRunner 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 LinkRunner 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.

☰ Discovery

 **Compass.netally.eng**

Network Server

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

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

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

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

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


**Services:** DNS, Virtual Machine


 **Addresses**



# Hypervisors

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

 **Discovery**

 **COS-PNT-VM.fnet.eng**

Hypervisor

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



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

**Nearest Switch:** ~ **Unknown Switch 4** ~

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

**Services:** Hypervisor


**Attributes:** Port Aggregation


 **Addresses** 

IPv4: 1 IPv6: 1 MAC: 1

# 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.

 **Discovery**

 **Cisco ACS 5.8 Linux**

Virtual Machine

**Name**  
Virtual Machine: Cisco ACS 5.8 Linux


**Address**  
IPv4: 10.250.0.59 (Reachable)  
IPv6: 2001:c001:c0de:500:20c:29ff:fe0b:e61c  
MAC: VMware:000c29-0be61c


**Nearest Switch:** ~ Unknown Switch 4 ~

**Hypervisor:** COS-PNT-VM.fnet.eng  
10.250.3.251

**Virtual Machine**  
Guest OS: Linux 2.6.32-431.20.3.el6.x86\_64 Red Hat Enterprise Linux Server release 6.4 (Santiago)  
Memory Reservation: 4,096MB


**Services:** Virtual Machine


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



# Wi-Fi Controllers

LinkRunner can discover SNMP enabled Wi-Fi controllers, including Cisco and Aruba Wi-Fi Controllers.


 **Discovery**


 **Cisco2500WLC**  
Wi-Fi Controller


**Name**  
SNMP: Cisco2500WLC



**Address**  
IPv4: 10.250.3.235 (Reachable)  
"MAC: Cisco:ece1a9-556c80

**Attributes:** Discovered via SNMP, Transparent Switch  
**AP Capacity:** 75

 **APs** 2 >

 **SSIDs** 16 >


 **VLANs** 1 >  
1

 **Interfaces**   
Up: 2 Down: 3

## Access Points (APs)

The LinkRunner discovers APs through SNMP queries with a linked connection through a management or test port.

☰ Discovery

 **Ntgear:3c3786-719307**

AP

Address


BSSID: [Ntgear:3c3786-719307](#)

802.11

Channels: 6, 36 (bonded)

Type: 802.11ax

Last Seen: 11:20:17 AM


 **Addresses** 2 >

BSSID: 2

## Wi-Fi Clients

Wireless clients are discovered through SNMP queries with a linked connection through a management or test port.

☰ Discovery

 **Samsng:4c6641-701864**

Wi-Fi Client

**Address**

MAC: [Samsng:4c6641-701864](#)


**802.11**

Channels: 60  
Type: 802.11ac

**AP:** [lap-cos-us-1](#)

SSID: NSVisitor  
Security: WPA2-P

Last Seen: 11:15:45 AM

 **Problems** 1 >

Warnings: 1

## VoIP Phones

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



## Discovery

**INET:0220c4-04c206**

VoIP Phone

**Address**

MAC: INET:0220c4-04c206

**Nearest Switch:** [RoboCop](#)

Port: g6

VLAN ID: 1


**VLANs**


1 &gt;


1


# Printers


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


 **Discovery**


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

 **Problems** 1 >  
Warnings: 1

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

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

 **SNMP**

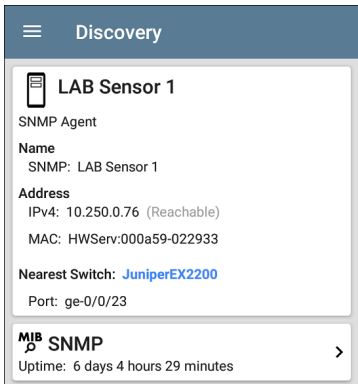




## SNMP Agents


SNMP agents are discovered using SNMP queries. See [SNMP Configuration](#).

NOTE: If LinkRunner 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](#).



The screenshot shows the 'Discovery' section of the app. It features a blue header with a hamburger menu icon and the word 'Discovery'. Below the header is a card for 'LAB Sensor 1', which is identified as an 'SNMP Agent'. The card lists the following details: Name (SNMP: LAB Sensor 1), Address (IPv4: 10.250.0.76 (Reachable) and MAC: HWServ:000a59-022933), Nearest Switch (JuniperEX2200), and Port (ge-0/0/23). At the bottom of the card is a section for 'MIB SNMP' with an uptime of '6 days 4 hours 29 minutes' and a right-pointing chevron icon.

Discovery

 **LAB Sensor 1**

SNMP Agent

**Name**  
SNMP: LAB Sensor 1

**Address**  
IPv4: 10.250.0.76 (Reachable)  
MAC: HWServ:000a59-022933

**Nearest Switch:** [JuniperEX2200](#)

Port: ge-0/0/23







**MIB SNMP** >

Uptime: 6 days 4 hours 29 minutes

See also [SNMP Details](#).

## Network Tools

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


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

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

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

The screenshot shows the 'Discovery' screen of an application. At the top, there is a blue header with a hamburger menu icon on the left and the word 'Discovery' in white. Below the header is a white card with a grey border. The card contains the following information: a small icon of a LinkRunner device, the IP address '10.250.2.240', the device name 'LinkRunner G2', and a section titled 'Address' containing 'IPv4: 10.250.2.240 (Reachable)', 'IPv6: fe80::2c0:17ff:fec5:88', and 'MAC: NetAlly:00c017-c50088'. Below this is a section for 'Nearest Switch: PV\_Mike\_NetgearGS110TP' with 'Port: g6' and 'VLAN ID: 500'. At the bottom of the card are two expandable sections: 'Addresses' with 'IPv4: 1 IPv6: 1 MAC: 1' and '2 >' to its right, and 'VLANs' with '500' and '1 >' to its right.

Discovery

 **10.250.2.240**


LinkRunner G2

**Address**


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

**Nearest Switch:** [PV\\_Mike\\_NetgearGS110TP](#)

Port: g6  
VLAN ID: 500

 **Addresses** 2 >


IPv4: 1 IPv6: 1 MAC: 1


 **VLANs** 1 >

500

## 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.

 **Discovery**

 **ubuntu**

Host/Client


**Name**  
mDNS: ubuntu

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

**Nearest Switch:** [PV\\_Mike\\_NetgearGS110TP](#)


Port: g3  
VLAN ID: 500

---

 **Addresses** 4 >

IPv4: 1 IPv6: 3 MAC: 1

---

 **VLANs** 1 >

500

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



## Discovery

**localAdm:227367-a99246**

Wi-Fi Client

**Address**MAC: [localAdm:227367-a99246](#)**802.11**

Channels: 48

Type: --

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

SSID: ngenius&amp;sniffer

Security: WPA2-E

# Device Names and Authorization

## Assigning a Name and Authorization to a Device

The Discovery app provides 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 LinkRunner 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:

Wi-Fi - BSSIDs (150)		
Filter	Sort	Authorization
	<b>Ntgear:3c3786-719306</b>	-33 dBm >
Unauthorized	Nighthawk 802.11ax 5GHz	CH: 36
	<b>Cisco:b83861-84aaf0</b>	-82 dBm >
Neighbor	Cisco WEP64 SA	CH: 36
	<b>Cisco:b83861-84aaf0</b>	-67 dBm >
Neighbor	CiscoQATest-mañana	CH: 1
	<b>Cisco:78bc1a-0fd908</b>	-64 dBm >
Authorized	[NGP-004]	CH: 36

## Applying a Name and/or Authorization

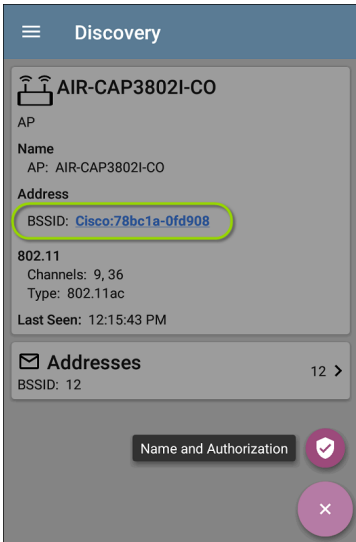
Access the **Name and Authorization** function from the floating action menu  on a [Discovery Details screen](#).

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.

**Name and Authorization**

MAC Address: Cisco:78bc1a-0fd908

User Name: Conference Room AP

Authorization

Authorized

Neighbor

Flagged

Unknown

Unauthorized

Unspecified

CANCEL OK


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.

 **Discovery**


 **Conference Room AP**

AP

**Name**  
User: Conference Room AP  
AP: AIR-CAP3802I-CO

**Address**  
BSSID: [Cisco:78bc1a-0fd908](#)  
Authorization: Authorized

802.11  
Channels: 9, 36  
Type: 802.11ac  
Last Seen: 12:17:22 PM





 **Addresses** 12 >  
BSSID: 12

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.

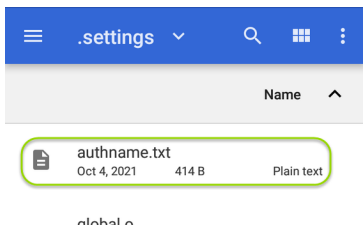
To view all assigned Authorizations for a device, open the Discovery screen for the device and view the Addresses screen. Then, sort by Authorization.

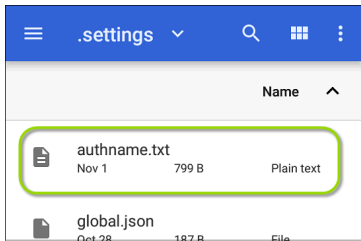
Addresses (14)	
Authorization	
 <b>Cisco:b83861-84aaf3</b> Flagged	CH: 36 > Cisco WEP128 OA
 <b>Cisco:b83861-84aaf1</b> Neighbor	CH: 1 > Cisco WEP64 OA
 <b>Cisco:b83861-84aafc</b> Authorized	CH: 1 > Cisco WEP128 OA
 <b>Cisco:b83861-84aaf0</b> Neighbor	CH: 1 > Cisco WEP64 OA


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 LinkRunner's internal storage **.settings** folder, accessible from the [Files](#) app.





NOTE: In the Files app, you may need to tap the action overflow icon  at the top right and select **Show Internal Storage** to navigate to the **LinkRunner-10G** folder and sub-folders.

If desired, you can manually edit this file on the LinkRunner 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 authname.txt files from [Link-Live](#) to your test unit.)

NOTE: Your LinkRunner 10G 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 LinkRunner, third-party apps, such as QuickEdit Text Editor, are available from the NetAlly [App Store](#)  .

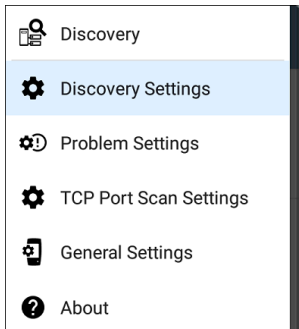
For help importing a file, see the [Managing Files](#) topic.

NOTE: After importing and overriding the authname.txt file, NetAlly recommends [Refreshing Discovery](#) in the Discovery app or restarting your unit.

# 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](#).)

**Discovery Settings**

Active Discovery Ports  
All


Extended Ranges  
0 Extended Ranges


ARP Sweep Rate  
100/second


Refresh Interval  
90 minutes

SNMP  
SNMPv1/v2: Enabled, SNMPv3: Enabled

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](#).

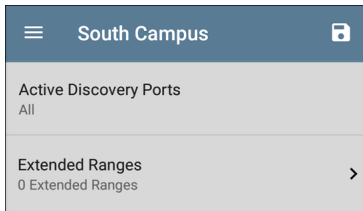
3. Then, [Refresh Discovery](#) from the action overflow menu  to apply the new configuration.

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 LinkRunner 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 LinkRunner always discovers management subnets, regardless of your network port connections.


Tap the field to open the Extended Ranges list screen.

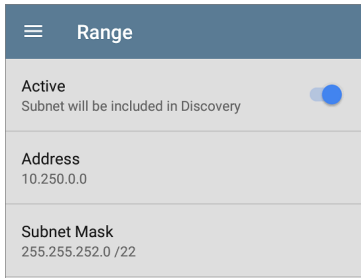
Extended Ranges

<input checked="" type="checkbox"/>	10.250.0.0 - 10.250.3.255 Extended Ranges	▼	⋮	>
<input checked="" type="checkbox"/>	10.6.0.0 - 10.6.63.255 (Restricted) Extended Ranges	▲	⋮	>
<input type="checkbox"/>	192.0.0.0 - 192.255.255.255 Extended Ranges		⋮	>

+

- 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.

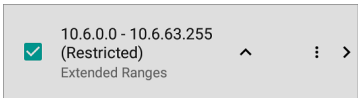


Range	
Active	<input checked="" type="checkbox"/>
Subnet will be included in Discovery	
Address	10.250.0.0
Subnet Mask	255.255.252.0 /22

## 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 LinkRunner will *not* communicate with devices within the restricted range.

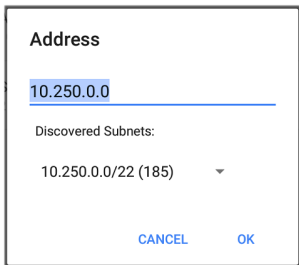




- Restricted Ranges take precedence regardless of the order in which they are listed on the Extended Ranges screen.
- You can Restrict a part of a configured Active Extended Range.
- You can also restrict a single device, whether it is part of an Active Range or not. To enter a single device that you 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.



**Address**

10.250.0.0

Discovered Subnets:

10.250.0.0/22 (185) ▼

CANCEL OK

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 LinkRunner 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 LinkRunner interrogates MIBs to determine the device type, ports, connected subnets, and other data.

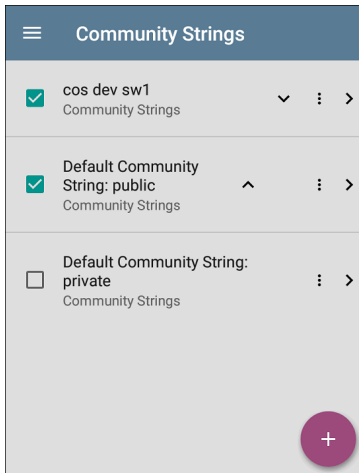
SNMP credentials are required to communicate with the SNMP agents on your interconnect devices, such as switches and routers. The Discovery Settings allow you to enter the SNMP community strings and credential sets the LinkRunner uses to communicate with those devices.

## 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 LinkRunner 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 LinkRunner 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.

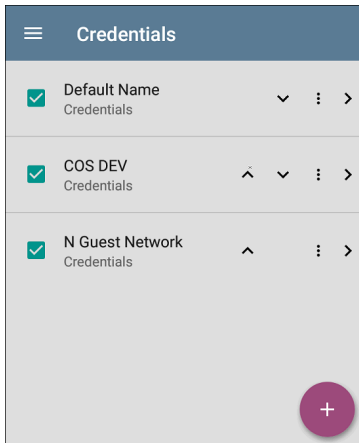
## SNMPv3

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 LinkRunner 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. LinkRunner 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.

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

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

LinkRunner Discovery supports two SNMPv3 Authorization types: HMAC-SHA and HMAC-MD5. If Authorization is required, enter the appropriate password.

## Privacy Type and Password

LinkRunner 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 LinkRunner 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 LinkRunner asks for more data as soon as a response has

been received. You can select a 1 or 5 second delay if needed.

## Devices Discovered Through Other Devices

By default, LinkRunner 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.

**Devices Discovered Through Other Devices**

- Routers and Subnets
- Switches
- VoIP Devices
- Wi-Fi Clients
- Virtual Machines

**CANCEL**      **OK**

## 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 LinkRunner is reading the CDP and LLDP caches of one switch, it contains other switches. If this option is enabled, the LinkRunner 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.

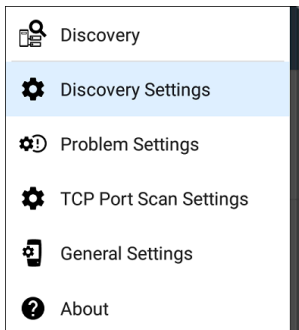
Disabling the Device Health testing affects the types of Problems that Discovery can detect.

See also [Problem Settings](#).

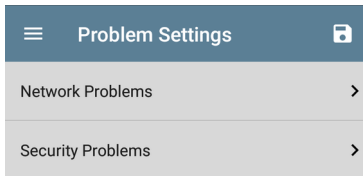
# Problem Settings

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**.



(Tap here to go to [Discovery Settings](#) or back to [General Settings](#).)

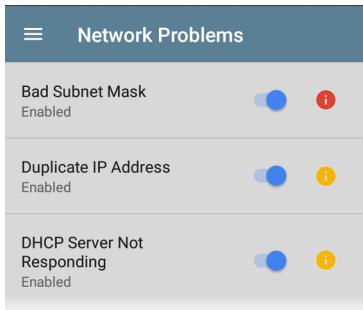


Problems are categorized as Network or Security.



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.

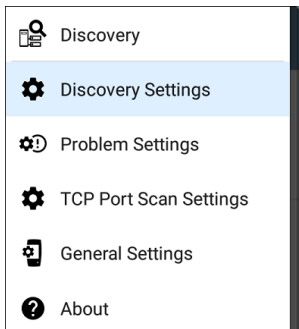
Tap the red  or yellow  information icons to the right of each Problem to read a detailed description and recommended actions. **Red** icons indicate Failure conditions and **yellow** indicate Warning conditions.

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. (Run the scan by tapping the **FAB** on a [Discovery Details](#) screen and then tapping **TCP Port Scan**.) The LinkRunner 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.

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

**Interface:** Tap the field to select the LinkRunner 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 LinkRunner 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 LinkRunner 10G 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, LinkRunner shows the number of hops to the destination device. A maximum of 30 hops can be reported.

Note: AllyCare is required to use this application. Your LinkRunner must be [claimed](#). Please visit: [NetAlly.com/AllyCare Support and Features](https://www.netally.com/AllyCare/Support-and-Features).

# 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 10G. The default destination is [www.google.com](http://www.google.com).

## Populating Path Analysis from Another App

Like other LinkRunner 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**.

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

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 LinkRunner port from which the port scan runs. Tap the field to select a port. (See [Selecting Ports](#) for explanations of the different ports.)

LinkRunner 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 dialog above.

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.)



# Running Path Analysis


Tap the **START** button at the top of the app screen to begin a Path Analysis.



NOTE: LinkRunner must be linked on the Interface (Port) selected in the app's settings. See [Test and Management Ports](#) for help.

 **Path Analysis** START 

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

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

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


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

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

LinkRunner 10G), 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 LinkRunner Cards

 **google.com**  
10 ms, 6 ms, 11 ms  
Device Name: [google.com](#)  
IP Address: 172.217.1.206  
Interface: Any Port  
Protocol: Connect (TCP)  
TCP Port: 80 (www-http)  
**Results**  
Started: 2:26:58 PM  
Status: Destination reached in 11 hops  
[UPLOAD TO LINK-LIVE](#)

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 LinkRunner Card

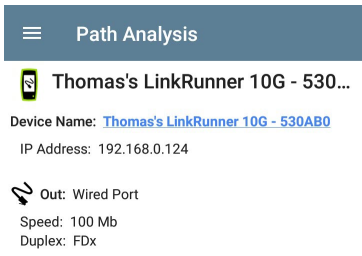


This LinkRunner card displays the port from which the Path Analysis ran.

NOTE: This card and screen only display a custom name for your LinkRunner if you have [claimed it to Link-Live](#).

Tap the card to view more details.

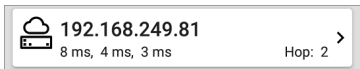
The image below shows the source LinkRunner card from a Wired Path Analysis, which displays the link speed and duplex.



Beneath the LinkRunner source card, the Hop cards show Layer 2 and Layer 3 devices determined to be in the Path.

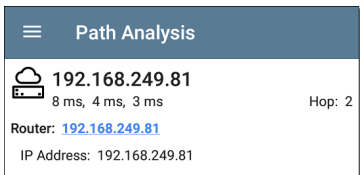
## Layer 3 Hops

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.



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


## 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.

☰
Path Analysis



### Split Route

41 ms, 25 ms, 34 ms

Hop: 8

Response 1: [et-0-0-0.msr1.ne1.yahoo.com](https://et-0-0-0.msr1.ne1.yahoo.com)

IP Address: 216.115.105.25

Response 2: [et-0-0-0.msr2.ne1.yahoo.com](https://et-0-0-0.msr2.ne1.yahoo.com)


IP Address: 216.115.105.179

Response 3: [et-19-1-0.msr2.ne1.yahoo.com](https://et-19-1-0.msr2.ne1.yahoo.com)

IP Address: 216.115.105.181

## Layer 3 Interfaces and Statistics

Statistics for Interfaces on Layer 3 devices may be identified and measured if the LinkRunner has SNMP access.



### COS\_DEV\_SW1

13 ms, 12 ms, 13 ms

Hop: 3 >

In: Gi1/0/47

1 Gb FDx

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.

☰ Path Analysis

 **COS\_DEV\_SW1**  
13 ms, 12 ms, 13 ms Hop: 3

Router: [COS\\_DEV\\_SW1](#)

IP Address: 192.168.249.82

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

Speed: 1 Gb  
Duplex: FDx

**Statistics**  
Util: 0.3 % Discards: 0.0 % Errors: 0.0 %



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.


 **Path Analysis** START 

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


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

[UPLOAD TO LINK-LIVE](#)


---

 **LinkRunner 10G** >  
Out: Wired Port 1 Gb FDx


---

 **COS\_DEV\_SW1** >  
In: Gi1/0/13 VLAN: 500 1 Gb FDx  
Out: Gi2/0/24 VLAN: 500 1 Gb FDx

---

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

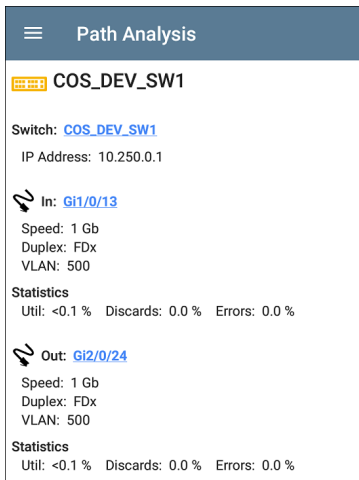
---

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

The LinkRunner 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.




The screenshot shows the Path Analysis app interface. At the top, there is a blue header with a hamburger menu icon and the text "Path Analysis". Below the header, the device name "COS\_DEV\_SW1" is displayed with a yellow keyboard icon to its left. Underneath, the switch name "Switch: COS\_DEV\_SW1" is shown in blue, followed by the IP address "IP Address: 10.250.0.1". There are two interface sections, each starting with a black lightning bolt icon. The first section is for the "In" interface "Gi1/0/13", showing "Speed: 1 Gb", "Duplex: FDx", and "VLAN: 500". Below it, the "Statistics" section shows "Util: <0.1 %", "Discards: 0.0 %", and "Errors: 0.0 %". The second section is for the "Out" interface "Gi2/0/24", showing the same speed, duplex, and VLAN information, and identical statistics.


**Path Analysis**

 **COS\_DEV\_SW1**

Switch: [COS\\_DEV\\_SW1](#)  
IP Address: 10.250.0.1

 In: [Gi1/0/13](#)  
Speed: 1 Gb  
Duplex: FDx  
VLAN: 500

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

 Out: [Gi2/0/24](#)  
Speed: 1 Gb  
Duplex: FDx  
VLAN: 500

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

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 LinkRunner 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

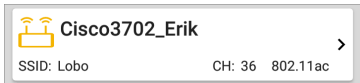
**Discards:** Percentage of total packets that have been dropped

**Errors:** Percentage of packets containing errors

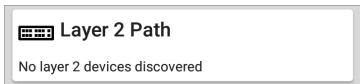
## Layer 2 APs

If the Layer 2 path starts or ends with a Wi-Fi device, its AP is shown as a Layer 2 device in the path.

A Layer 2 AP card indicates the connected network SSID, channel, and 802.11 type in use.



## No layer 2 devices discovered



In some cases, the LinkRunner does not discover Layer 2 devices between Layer 3 devices. There may not be any Layer 2 devices, or LinkRunner 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:

**Link-Live**

by NetAlly



Path Analysis Name

20190419\_131047

Comment


Conference Room B

Job Comment

Union Hall



SAVE TO ANALYSIS FILES

Path Analysis results are uploaded to the **Analysis** page  on Link-Live.

[Back to Title and Contents](#)



# Performance Test App

The LinkRunner 10G's line rate Performance Test provides point-to-point performance testing of a traffic stream across wired IPv4 network infrastructure. This test quantifies network performance in terms of target rate, throughput, loss, latency, and jitter.

The Performance test exchanges a stream of traffic with Peers or Reflectors and measures the performance of the traffic stream. You can simulate real-world traffic by configuring traffic flow, frame size, VLAN, and QoS options. Run the test at a full line rate of up to 10 Gbps for performance validation, or run at lower speeds to minimize disruption when troubleshooting operational networks.

The Performance Test runs from the [Wired Test Port](#) (top RJ-45 or Fiber port), and an [AutoTest Wired Profile](#) must connect successfully to establish link on the port. When you start up the LinkRunner, the last Wired Profile in the list of active AutoTest profiles runs automatically if an active Ethernet connection is detected on the top RJ-45 port. Otherwise, you may need to manually run a Wired AutoTest to link. See [Wired AutoTest Profiles](#) to review.

# Introduction to Performance Testing

Network performance is measured between a *Source* device, on which the test is configured and controlled, and up to four *Endpoint* devices that exchange traffic with the source. There are two endpoint types: Peers and Reflectors.

When using a Peer endpoint, separate upstream and downstream measurements can be shown for Throughput, Loss, Latency, and Jitter.

When using a Reflector, the LinkRunner reports round-trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

The LinkRunner 10G can act as the controlling Source for the performance test or as a Peer for a test conducted by different source device, such as another LinkRunner 10G or a OneTouch AT 10G.

Other NetAlly testers work with the LinkRunner to perform network performance testing:

- **OneTouch AT 10G** can act as the Source or a Peer for Performance tests.  
([NetAlly.com/products/OneTap](http://NetAlly.com/products/OneTap))
- **LinkRunner AT** and **LinkRunner G2** each have a Reflector feature for exchanging Performance test traffic.  
([NetAlly.com/products/LinkRunner G2](http://NetAlly.com/products/LinkRunner G2))
- NetAlly's **Network Performance Test (NPT) Reflector** PC application can also act as the reflector for a Performance test. Download the free NPT Reflector software from [NetAlly.com/support/downloads](http://NetAlly.com/support/downloads). Select LinkRunner 10G from the drop-down menu to view the list of downloads.

## In this Chapter

Performance Test Settings



Configuring Performance Endpoints

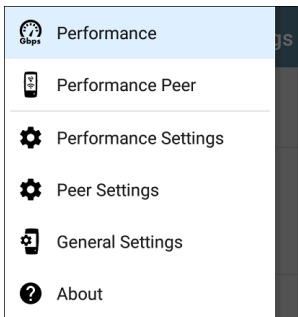
Running a Performance Test

Running LinkRunner as a Performance Peer

# Performance Test Settings

The Performance app has both **Performance** settings that apply when the LinkRunner is acting as the test source, and **Peer** settings that control the unit when it is acting as the test Peer.

Access the settings by tapping the settings button  on the Performance Test screen or the [Performance Peer](#) screen, or open the left-side [navigation drawer](#)  in the Performance app.



**Performance** goes to the main Performance test results screen.

**Performance Peer** opens the Peer results screen.

**Performance Settings** control the performance test settings when the LinkRunner is the source.

**Peer Settings** control the LinkRunner Performance Peer when another device is the source. See [Running LinkRunner 10G as a Performance Peer](#).

## Saving Custom Performance Tests



The Performance app allows you to save two levels of test configurations: individual **Services** and complete **Performance Tests** with *up to eight* enabled Services.

- **Services** include the Endpoint, Frame Size, Bandwidth, grading Thresholds, and Layer 2 and 3 Options. Services can be used in any number of saved Performance Tests.
- Saved **Performance Tests** contain a test Duration setting and the included Services.



For example, you can configure Services for multiple endpoints at different locations and with different bandwidths. A user can also create multiple Services with different QoS priorities (using the Layer 3 options) to verify that loss does not occur over the higher priority stream.

Saved Performance Tests and their Services work much like AutoTest Profile Groups, Profiles, and Test Targets. See the [AutoTest Overview](#) to review.

Open the Performance Settings screen  from the main Performance results screen or the left-side [navigation drawer](#) .


**Performance Settings**

Duration  
30 minutes

Services

- LinkRunner G2 Reflector  
192.168.65.20, Reflector
- EtherScope Peer  
10.250.5.68, Peer, Asymmetrical
- PC NPT Reflector  
10.250.7.10, Reflector

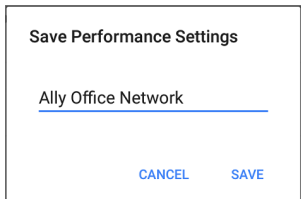
+

Tap the save icon  to load, save, import, or export a settings configuration.

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

- **Save As:** Save the current settings with an existing name or 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.

See [Saving App Settings Configurations](#) for more instructions.



In the example images here, the user has saved a custom Performance Test called "Ally Office Network."



The screenshot shows the 'Performance Settings' screen for a configuration named 'Ally Office Network'. At the top, there is a blue header with a hamburger menu icon on the left, the title 'Ally Office Network' in the center, and a save icon on the right. Below the header, the 'Duration' is set to '30 minutes'. Underneath, there is a section titled 'Services' in blue. A single service, 'LinkRunner G2 Reflector', is listed with a green checkmark on the left, the IP address '192.168.65.20, Reflector' below it, and a vertical ellipsis and a right-pointing arrow on the right.

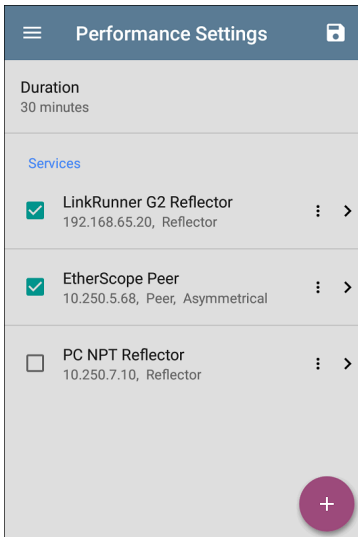
Once you save a Performance Test configuration, the custom name you entered appears at the top of the Performance Settings screen (above) and main Performance Test screen (below).



The screenshot shows the main 'Performance Test' screen for the 'Ally Office Network' configuration. The blue header contains a hamburger menu icon, the title 'Performance', and a 'STOP' button. The main content area has a white background with a grey border. At the top left is a speedometer icon with 'Gbps' below it. To its right is the title 'Ally Office Network'. Below this, the test details are listed: 'Duration: 1 minute', 'Started: 3:27:07 PM', and 'Status: Next update in 26 seconds'. A table with four columns is shown: 'Loss', 'Latency', and 'Jitter'. Below the table, the service 'LinkRunner G2 Reflector' is listed with a refresh icon on the left and a right-pointing arrow on the right. The table rows below the service name contain dashes ('--').

	Loss	Latency	Jitter
LinkRunner G2 Reflector	--	--	--

## Configuring the Source LinkRunner 10G







Open the Performance Settings screen from the main Performance results screen  or the left-side [navigation drawer](#) .





 Performance Settings 

Duration  
30 minutes

Services

- LinkRunner G2 Reflector    
192.168.65.20, Reflector
- EtherScope Peer    
10.250.5.68, Peer, Asymmetrical
- PC NPT Reflector    
10.250.7.10, Reflector



Changed settings are automatically applied. When you finish configuring, tap the back button  to return to the Performance test screen.

**Duration:** This setting is the length of time the Performance test runs. Tap the field to select a new duration. The default is 1 minute.

## Services

A Service is a configured traffic flow that simulates application traffic. You can run up to four unidirectional or bidirectional services simultaneously to emulate and test the QoS levels on your network.


The Services configurations include the Endpoints, Frame Size, Bandwidth, Thresholds, and Options the LinkRunner uses to measure and grade performance.

Your collection of configured Services is available across all of your saved Performance Test configurations, and if you delete a Service, it is deleted from all Performance Tests.

On the Performance Settings screen, you can perform the following actions:


- Check or uncheck the boxes to include or exclude Services in the list of active Performance tests.

NOTE: You can run a Performance Test on up to eight Services at once. If you select more than eight Services, the Performance Test fails.

- Tap the action overflow icon  to **Duplicate**, **Move Up/Down**, or **Delete** a configured Service.

**CAUTION:** When you delete a Service, you delete it from all Performance Test configurations. To remove a Service from the current test, simply uncheck it.

NOTE: All Services are tested at the same time, so the order of Services listed on this screen does not affect how the test runs.

- Tap the **FAB** icon  to add a new Service.
- Tap any Service's name, or add a new Service, to open its settings, where you can enter a custom Service name, endpoint address, performance thresholds, and other Service characteristics.

Service	
<b>Service Name</b> LinkRunner G2 Reflector	
<b>Endpoint Device</b> 10.250.3.112, Reflector	>
<b>Frame Size</b> 512 Bytes	
<b>Bandwidth</b> Rate: 1 Mbps	>
<b>Thresholds</b> Loss: 0.3 %, Jitter: 20 ms, Latency: 100 ms	>
<b>Layer 2 Options</b> VLAN Overrides: Disabled	>
<b>Layer 3 Options</b> TOS: Default (0)	>

## Service Name

Tap the **Service Name** field to enter a custom name for the endpoint and associated settings.



This name appears on the Services screen and the Performance test screen.

## Endpoint Device

Open this screen to configure the Endpoint Address, Type, and Traffic Flow.

☰	Endpoint Device
IPv4 Address	10.250.2.187
Communication UDP Port	3842 (netally-perf)
Endpoint Type	Peer
Traffic Flow	Asymmetrical

**IPv4 Address:** Tap the field to enter the IPv4 address of your endpoint device.

**Communication UDP Port:** If needed, tap to enter a different UDP Port number. The default NetAlly performance test port is 3842.

NOTE: The UDP port number entered here must match the port number used by your Peer endpoint device.

**Endpoint Type:** Select **Peer** or **Reflector** depending on the type of endpoint you are using for the performance test.

**Traffic Flow:** This setting only appears when **Endpoint Type** is set to **Peer**.

- Select **Upstream only** or **Downstream only** to test only the single traffic flow direction specified.
- Select **Asymmetrical** to test each direction using a different **Target Rate** (set under **Bandwidth** below). Asymmetrical is the default traffic flow for a Peer endpoint.
- Select **Symmetrical** to test both directions using the same Target Rate.

## Frame Size

Tap the **Frame Size** field to select a new single frame size, the Frame Size Mix option, or to enter a Custom Value. The default is 512 bytes.

**Frame Size**

128 Bytes


256 Bytes


512 Bytes

1024 Bytes


1518 Bytes

9600 Bytes

Frame Size Mix  
abceg 

Custom Value 

[CANCEL](#) [OK](#)

Selecting **Frame Size Mix** creates traffic with variable frame size patterns, generated in a repeating sequence. Tap the edit icon  to revise the frame size pattern.

### Frame Size Mix

Mix: abceg

User Size: 512 Bytes

<	⌫	>
a 64	b 128	c 256
d 512	e 1024	f 1280
g 1518	h 9600	u User

CANCEL OK

On the Frame Size Mix keyboard shown above, each letter (a through h) is associated with a frame size. The default pattern is "abceg," meaning the traffic pattern follow a repeating sequence of 64, 128, 256, 1024, and 1518 bytes. Use the letter keys along with the arrows and backspace button to edit the mix sequence as desired.

The **u** key enters a user-defined size into the mix. Select the field next to **User Size:** to enter your desired frame size, between 64 and 9600 bytes. Tap the **u** key to insert the new size where you want it in the pattern.

**NOTE:** If the Performance Test runs on a VLAN (configured in the Wired AutoTest Profile or the Performance Layer 2 options shown below), the frame sizes are four bytes longer. You do not need to account for this frame size increase in the settings.

## Bandwidth

Tap to open the **Bandwidth** screen and select or enter a **Target Rate** for one or both traffic directions.

Bandwidth	
Upstream Target Rate	1 Mbps
Downstream Target Rate	10 Mbps

- If you are configuring a Reflector endpoint or you have selected Symmetrical Traffic Flow for a Peer endpoint, only one Target Rate is used.
- For a Peer with an Asymmetrical Traffic Flow configuration, you can select a different Upstream and Downstream Target Rate for each direction.

Tap the **Target Rate** field(s) to select or enter a new rate.

**Upstream Target Rate**

1 Mbps

10 Mbps

100 Mbps

999.8 Mbps

**Target Rate:** The requested rate of round-trip traffic

**Upstream Target Rate:** This is the requested rate of upstream traffic, from the source to the endpoint.

**Downstream Target Rate:** This is the requested rate of downstream traffic, from the endpoint to the source.

NOTE: The 99.98 Mbps and similar values provided in the Target Rate options are meant to test the maximum, worst case throughput on an Ethernet link. Though greater rates are possible under perfect conditions, the limitation of 99.98% of the link rate results from asynchronous clocks in Ethernet. The IEEE 802.3 Ethernet standard allows link partners to differ by up to 0.02% of their clock signals. Therefore, end-to-end throughput in the worst case may be limited to 99.98% of the source link rate when the traffic traverses a link and maximum clock differences occur between the two link partners.

## Thresholds

Thresholds define the **Pass/Fail** criteria the LinkRunner uses to grade the test. The

Performance Test thresholds are Frame Loss, Jitter, and Latency.

- If you are configuring a Reflector endpoint or you have selected Symmetrical Traffic Flow for a Peer endpoint, the same threshold values grade each traffic direction.
- For a Peer with an Asymmetrical Traffic Flow configuration, you can select different Upstream and Downstream thresholds.

**Thresholds**

**Upstream**

**Frame Loss Threshold**  
Disabled

**Jitter Threshold**  
20 ms

**Latency Threshold**  
100 ms

**Downstream**

**Frame Loss Threshold**  
0.2 %



Tap each Threshold field to select or enter the maximum value allowed. If a measured value exceeds the threshold value, the test fails.

**Frame Loss Threshold:** The Frame Loss Threshold is the percentage of frames that can be lost before the test fails. The default is 0.3%. Tap the field to select or enter a new threshold or to disable grading based on frame loss altogether.

**Jitter Threshold:** Jitter is a measure of the variation in frame-to-frame latency in milliseconds. The default threshold is 20 ms.

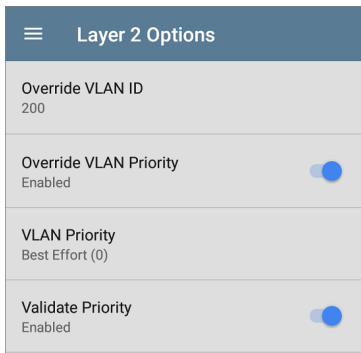
**Latency Threshold:** Latency is the amount of time it takes for a packet to go from the source to the endpoint and endpoint to source in milliseconds. The default threshold is 100 ms.

## Layer 2 Options

The Performance Test runs over the [Wired Test Port](#) link established by an [AutoTest Wired Profile](#). Therefore, by default, the Performance Test runs using the VLAN ID configured in the settings of the Wired AutoTest Profile that established the link.

To test other VLANs, for example, those that make up a trunk port, configure the Layer 2 Options in your separate Services to test the corresponding VLANs.

Open **Layer 2 Options** in the Performance app settings to override the VLAN settings from AutoTest.



**Override VLAN ID:** Tap to select or enter a VLAN ID number. The Override VLAN ID function tags frames with a particular VLAN (for example, a VLAN used for voice, video, or data). If Override

VLAN ID is not enabled, the VLAN is set to the value used for the Wired Test port.

**Override VLAN Priority:** Tap the toggle button to enable. By default, the VLAN priority is set to Best Effort (0). Use this setting to simulate a traffic stream of a certain type. If Override VLAN Priority is not enabled, the VLAN priority is set to the value used for the Wired Test port.

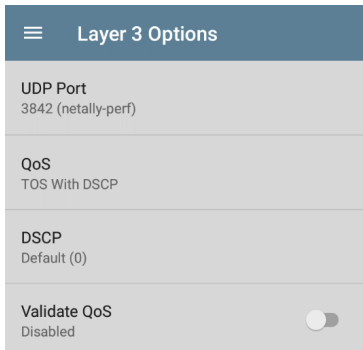
**VLAN Priority:** This setting only appears if the **Override VLAN Priority** setting above is Enabled. Tap to select a VLAN Priority.

**Validate Priority:** Tap the toggle button to enable the LinkRunner to validate the selected VLAN priority. When the Validate Priority option is enabled, LinkRunner checks the packets it receives to ensure that the priority field has been maintained from source to destination. If it has been altered, packets are counted as lost and included in the Frame Loss measurement.

### Layer 3 Options

Layer 3 options are useful when testing QoS (Quality of Service) on your network. You can create up to four Services using different DSCP

priority or IP precedence to verify that loss does not occur on the higher priority streams.



Layer 3 Options	
UDP Port	3842 (netally-perf)
QoS	TOS With DSCP
DSCP	Default (0)
Validate QoS	Disabled <input type="checkbox"/>

**UDP Port:** Tap to enter a specific UDP port number. This can help you simulate prioritized traffic on ports reserved for specific uses such as video, voice, or backup data or to match ports allowed by a firewall.

**QoS:** Select the methodology used on your network: **TOS with DSCP** (Type of Service with Differentiated Services Code Point or **TOS with IP Precedence** (legacy). Then, configure the priority using the settings below.

**DSCP:** This field is only available when **TOS with DSCP** is selected in the setting above. Using the DSCP control, you can specify a priority for the generated traffic by changing its classification. This is a six-bit field. The default value of zero specifies “Best Effort.” Tap the field to select a different DSCP.

**IP Precedence:** This field is only available when **TOS with IP Precedence** is selected. Tap the field to select an IP Precedence other than the default of Routine (0).

**IP Precedence Type:** This field is also only available when **TOS with IP Precedence** is selected. Tap the field to select an IP Precedence Type other than the default of Normal (0).

**Validate QoS:** When this setting enabled, the LinkRunner checks received packets to ensure that the QoS field has been maintained throughout the route. If the QoS field has been altered, packets are counted as lost.

# Configuring Performance Endpoints

LinkRunner 10G can run a Performance Test to any of the following Endpoints:

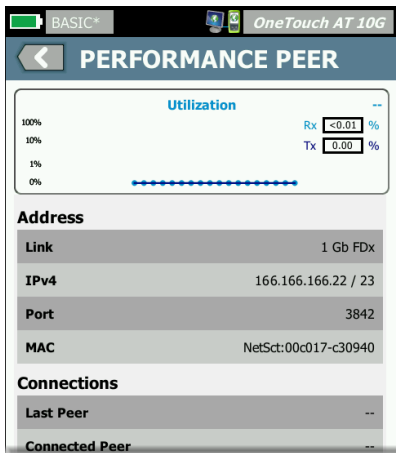
- Another LinkRunner 10G (Peer)
- A OneTouch AT 10G (Peer)
- A LinkRunner G2 or LinkRunner AT (Reflector)
- NPT Reflector Software (Reflector)

See our website [NetAlly.com](http://NetAlly.com) for more information about [OneTouch](#) and [LinkRunner](#) and to download the free NPT Reflector PC application.

## LinkRunner Performance Peer


To run an LinkRunner 10G as a Performance Peer, see the [Running as a Performance Peer](#) topic.

# OneTouch 10G Performance Peer



Follow these steps to set up a OneTouch 10G Performance Peer:

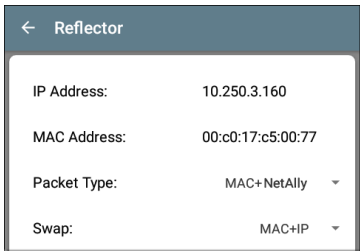
1. Ensure the OneTouch is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.

2. With the unit powered on, tap the TOOLS  icon on the Home screen.
3. In the TOOLS menu, select **Testing Tools > Performance Peer**.
4. Select the appropriate UDP **Port** number if other than the default of 3842.  
NOTE: The port number set on your endpoint must match the port number used by your source LinkRunner.
5. Turn on **Enable AutoStart** to cause the Performance Peer function to start automatically when the OneTouch is powered on.
6. Tap the **START** button.  
The PERFORMANCE PEER screen appears, and a network link is automatically established.
7. The IPv4 address of the peer is displayed on the screen. Enter this address on the [Endpoint Device](#) screen in the LinkRunner 10G's Performance test Services settings.





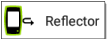

For additional details on the OneTouch Performance Peer, [see the OneTouch 10G User Manual, available online.](#)

## LinkRunner G2 Reflector






Follow these steps to set up a LinkRunner G2 Reflector:

1. Ensure the LinkRunner is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.
2. Start the LinkRunner G2 testing application by tapping the NetAlly logo  at the bottom of the screen.

3. In the testing app, open the left-side [navigation drawer](#) by tapping the menu button .
4. Select **Reflector**  .
5. Configure the **Packet Type** and **Swap** settings as required. The default settings, Packet Type: MAC + NetAlly and Swap: MAC + IP, are recommended to avoid any undesired traffic on your network.
6. Once the LinkRunner G2 Reflector has acquired an IP address, tap the floating action button (FAB)  at the lower right to start the Reflector.
7. The IP address of the Reflector is displayed at the top of the screen. Enter this address on the [Endpoint Device](#) screen in the LinkRunner 10G's Performance Test Services settings.

For additional details on the LinkRunner G2 Reflector feature, see the User Guide on the LinkRunner G2 Home screen.

# LinkRunner AT Reflector

Reflector		
IP Address:	192.168.001.090	
MAC Address:	00-C0-17-B6-86-0C	
Packet Type:	MAC+NetAlly	
Swap:	MAC+IP	
<p>Reflector Mode</p> 		
Configure	 <span>1000 FDx</span> 	Start

Follow these steps to set up a LinkRunner AT (2000) Reflector:

1. Ensure the LinkRunner is connected to an active network via the RJ-45 or Fiber test port and is plugged into AC power.
2. On the Home screen, select **Tools**.
3. In **General Configuration > Manage Power**, ensure the **Auto Shutoff Enabled** is unchecked to prevent the unit from powering down during the test. **Save** the changed setting.
4. In the Tools menu, select **Reflector**.

5. On the Reflector Screen, **Configure** the **Packet Type** and **Swap** settings as required. The default settings, **Packet Type: MAC + NetAlly** and **Swap: MAC + IP**, are recommended to avoid any undesired traffic on your network.
6. Select **Save** to apply any changed settings.
7. Select **Start** (F2) to run the Reflector.
8. The IP address of the Reflector is displayed at the top of the screen. Enter this address on the **Endpoint Device** screen in the LinkRunner 10G's Performance test Services settings.

For additional details on the LinkRunner AT Reflector feature, [see the LinkRunner AT User Manual, available online.](#)

# NPT Reflector Software



Follow these steps to set up the NPT Reflector PC application:

1. Download the software from [NetAlly.com/support/downloads](https://www.netally.com/support/downloads). Select LinkRunner 10G from the drop-down menu to view the list of downloads.
2. Install the Reflector on your PC by running the .exe file.
3. Open the Reflector application.

Once open, the application automatically detects available network interfaces and their link status.

4. Check the box next to **Enable Reflection** for each network interface you want to use as a Reflector Endpoint for your Performance Test.
5. Leave the application window open on your PC during Performance testing.
6. Enter IP addresses for the interfaces you want to test against on the [Endpoint Device](#) screen in the LinkRunner 10G's Performance Test Services settings.

Refer to the **Help** in the NPT Reflector software for additional information.

# Running a Performance Test

Note the following before running:


- The Performance Test can only run from the [Wired Test Port](#) (top RJ-45 or Fiber port), and an [AutoTest Wired Profile](#) must connect successfully to establish link on the port. If you receive a Status message such as "The wired test port is not linked" or "No IP address" but you have an active network connection, go to AutoTest and run a Wired Profile to troubleshoot your connection.
- All configured Performance Test [Services](#) are tested at the same time. If one Service fails to meet the thresholds for the test, the entire test fails.
- Only four Services can run at once. If you have selected more than four Services in the [Performance Settings](#), the test fails with the Status message, "Too many services enabled (56)."

- Newly configured Services may not display on the main Performance Test screen until you tap **START**.

To run your configured Performance Test, tap **START** on the main Performance screen.

## Performance Test Results

☰
Performance
START
⚙️
⋮




### New Performance Test

Duration: 10 minutes

Started: 11:16:22 PM

Status: Test failed, thresholds exceeded (6)


	Throughput	Loss	Latency	Jitter
--	------------	------	---------	--------



### LinkRunner G2 Reflector

>


1 Mbps	<0.001 %	60 us	<1 us
--------	----------	-------	-------



### EtherScope Peer

>

● ↑	939.4 Kbps	6.1 %	56 us	<1 us
● ↓	939.4 Kbps	6.1 %	55 us	1 us



### PC NPT Reflector

>

1 Mbps	0 %	223 us	105 us
--------	-----	--------	--------



Performance results update every five seconds if you are using only Reflector endpoints, and/or an LinkRunner 10G Peer running v1.2 or newer software, with a test Duration of 4 hours or less. If you are running a 10 second test, all results display after 10 seconds. Otherwise, results update every 30 seconds.

Performance Test results are presented on cards. The top card shows the test duration and status.

**Duration:** The test duration selected in the Performance Settings

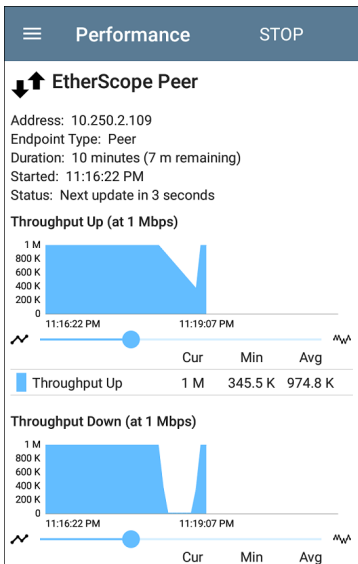
**Started:** Time at which the test began

**Status:** Current status of the test, including any error messages

Each card beneath corresponds to a configured Service and displays the Up, Down, or Round Trip measurements for Throughput, Loss, Latency, and Jitter. Remember, Peer endpoints can return Upstream and Downstream measurements, while Reflectors only provide round trip measurements.

Tap a Service card to view more details.

# Performance Service Detailed Results



The Service results screen displays detailed test characteristics and graphs of performance.

**Address:** IP address of the endpoint

**Endpoint Type:** Peer or Reflector

**Status:** Current status of the test, including any error messages

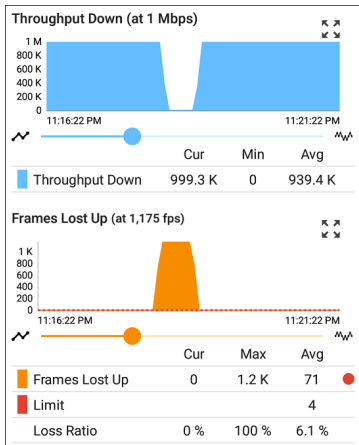
## Rerunning Tests from Detailed Results

You can rerun a Performance Test from the detailed results screen by tapping **Start** at the top of the screen. This repeats the Performance Test *only* for the Service that you are viewing.

## Throughput, Loss, Latency, and Jitter Graphs

The graphs described in this section update every 5 or 30 seconds for as long as the test is running. The graphs save and display data for the entire test duration, with a max duration of 24 hours.

Peer endpoints display separate Up and Down graphs (as shown below) for Throughput, Frames Lost, Latency, and Jitter, while Reflector endpoints display one round trip measurement for each.



Touch and drag (or swipe) left and right on each graph to move backward and forward in time, and double tap or move the slider to zoom in and out. See the [Trending Graphs](#) topic for an overview of the graph's pan and zoom controls.

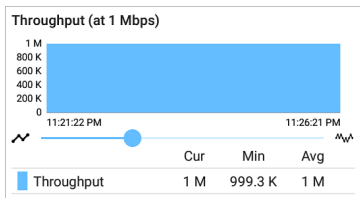
## Graph Legends

Under each graph, a legend table indicates the meanings of the colors that correspond to

different measurements. The **Limit** shown for each graph is the set Threshold from the corresponding [Service settings](#). Measurements that fall outside the Limit are indicated with a red dot next to the failing measurement. In the image above, the test has failed because Frames Lost Up was above the Limit.

The table also displays the Current, Maximum, and Average measurements. The Current columns contain measurements from the last interval (5 or 30 seconds). The Min, Max, and Avg columns show cumulative measurements gathered during the test duration.

## Throughput



**Throughput (Up/Down) (at Target Rate):**

Throughput is the measured bit rate based on the number of frames sent and frames received.

The configured Target Rate from the Performance Settings is shown in parentheses next to the Throughput heading. In the image above, the configured Target Rate is 1 Mbps.

## Loss

### Frames Lost Up (at 1,175 fps)



	Cur	Max	Avg
Frames Lost Up	0	5.9 K	279.8
Limit			18
Loss Ratio	0 %	100 %	4.8 %

### Frames Lost Down (at 2,350 fps)



	Cur	Max	Avg
Frames Lost Down	0	11.7 K	559.5
Limit			35
Loss Ratio	0 %	100 %	4.8 %

**Frames Lost (Up/Down):** Frame loss is quantified by the number of frames received subtracted from the number of frames sent.

**Limit:** This is the Frame Loss Threshold for one interval. It is computed from the Frame Loss

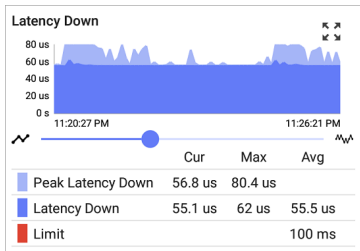
Threshold, Frame Size, and Bandwidth settings for the Service. The Limit is also displayed on the graph as a horizontal red dotted line (if the measurements are close enough to the Limit value for it to appear on the graph).

**Loss Ratio:** The percentage of total frames that were lost

NOTE (for 10G Rate Performance tests): Low-level electrostatic discharge (ESD) and low-power Electric Fast Transient (EFT) events, also called impulse noise, can interfere with newer, faster data links with less noise margin. These events could include static from a person's clothing or interference from electrical appliances and motorized equipment. When running a full 10G line rate test, ESD and EFT events can cause periodic spikes or a spike that then resolves on the Frame Loss graph.



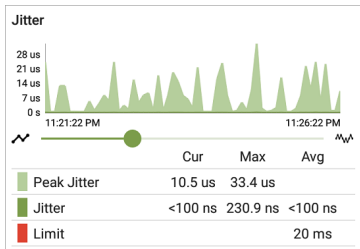
## Latency



**Latency (Up/Down):** Latency is the amount of time it takes for a packet to go from the source to the endpoint or from the endpoint to the source (in milliseconds). Latency is calculated by averaging the thousands of latencies measured during each interval. The one-way latency measurements are actually round trip measurements, divided by two.

**Peak Latency:** The highest measured latency. The Current column shows Peak Latency from the last test interval, and Max shows the highest latency measured during the entire test.

**Limit:** This is the Latency Threshold from the Performance app's setting.





**Jitter (Up/Down):** Jitter is a measure of the variation in frame-to-frame latency in milliseconds.

**Peak Jitter:** The highest measured Jitter. The Current column shows Peak Jitter from the last test interval, and Max shows the highest Jitter measured during the entire test.

**Limit:** This is the Jitter Threshold from the Performance app's settings.

## Uploading Results to Link-Live

Tap the action overflow icon  at the top right of the main Performance test screen, and select **Upload to Link-Live** to send the current latest

results to the Results page  on Link-Live.com.



**Link-Live**

by NetAlly




**Comment**

**Job Comment**



**SAVE TO LINK-LIVE**

An image file of a complete Service results screen, including all the graphs, can also be uploaded to Link-Live and attached to the main test results. From the main Performance test screen, tap a Service card to view the Service detailed results, then tap the action overflow icon  at the top right of the screen, and select **Upload graphs to Link-Live**.

**Link-Live**


by NetAlly

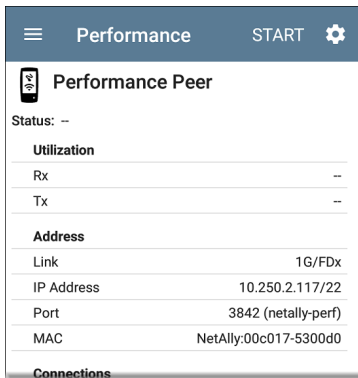
**Performance Result Filename**New Performance Test - 1 - LinkRunner**Comment**Enter Comment**Job Comment**Performance Main Offices**SAVE TO LINK-LIVE**

See the [Link-Live chapter](#) for more information.

# Running LinkRunner 10G as a Performance Peer

In addition to running a Performance Test as the controlling source device, LinkRunner 10G can also act as a Peer for another LinkRunner 10G or a OneTouch AT 10G acting as the source and controller.

To access the LinkRunner Performance Peer, tap the menu button  in the Performance app and select **Performance Peer**.



The screenshot shows the Performance app interface. At the top, there is a dark blue header with a menu icon (three horizontal lines), the word "Performance", the word "START", and a gear icon. Below the header, there is a section titled "Performance Peer" with a small icon of a device. Underneath, the status is shown as "Status: --". There are two sections: "Utilization" and "Address". The "Utilization" section has two rows: "Rx" and "Tx", both with "--" values. The "Address" section has four rows: "Link" with "1G/FDx", "IP Address" with "10.250.2.117/22", "Port" with "3842 (netally-perf)", and "MAC" with "NetAlly:00c017-5300d0". At the bottom, there is a section titled "Connections".

Utilization	
Rx	--
Tx	--

Address	
Link	1G/FDx
IP Address	10.250.2.117/22
Port	3842 (netally-perf)
MAC	NetAlly:00c017-5300d0

**Connections**

The [Wired Test Port](#) must be linked (by running an [AutoTest Wired Profile](#)) for the Performance Peer function to run. If the port is not linked, a Status message displays, "The wired test port is not linked."

## Performance Peer Setting


The only setting for the Performance Peer function is the **Communication UDP Port**.

Tap the settings button on the Performance Peer screen to change the port number. The default NetAlly performance test port is 3842.

NOTE: The UDP port number entered here must match the port number used by your source device.

## Running the Peer

Tap **START** on the Performance Peer screen to start the Peer.

Performance		STOP
	<b>Performance Peer</b>	
Status: Running		
<b>Utilization</b>		
Rx		1.02 %
Tx		1 %
<b>Address</b>		
Link		1G/FDx
IP Address		10.250.2.244/22
Port		3842 (netally-perf)
MAC		NetAlly:00c017-5300d0
<b>Connections</b>		
Last Peer		10.250.2.247
Connected Peer		10.250.2.247
Time Remaining		4 minutes 23 seconds

The screen displays real-time status, utilization, and rates for as long as the test is running.

**Status:** The current status of the peer

## Utilization

**Rx:** Receive percentage of the link speed

**Tx:** Transmit percentage of the link speed



## Address

**Link:** Link speed and duplex of the established Wired Test Port connection

**IP Address:** Address of the LinkRunner to be entered into the controlling source device

**Port:** UDP Communication port in use by the peer

**MAC:** The LinkRunner's MAC address

## Connections

**Last Peer:** Address of the previous peer that was connected to the LinkRunner

**Connected Peer:** Address of the peer that is currently connected to the LinkRunner

**Time Remaining:** Amount of time left for the current test



## 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.



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](https://netally.com/products/TestAccessory).

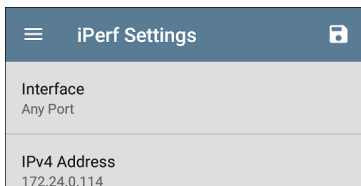
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the LinkRunner iPerf test. You can download iPerf server software from <https://iperf.fr>.


# iPerf Settings

To run an iPerf test, you must configure your LinkRunner 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

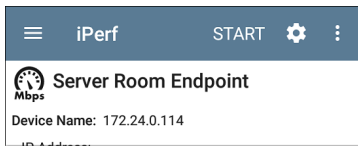
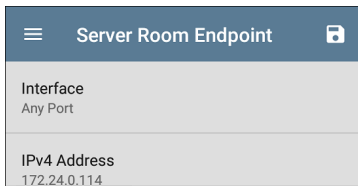
The iPerf app allows you to save a configuration of settings for running an iPerf test to the same endpoint later.



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."

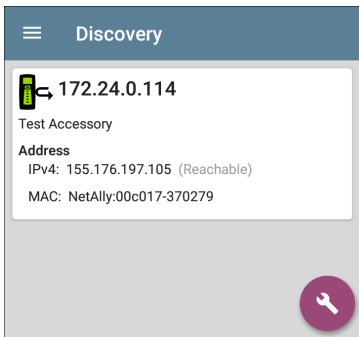



## Test Accessories in Discovery

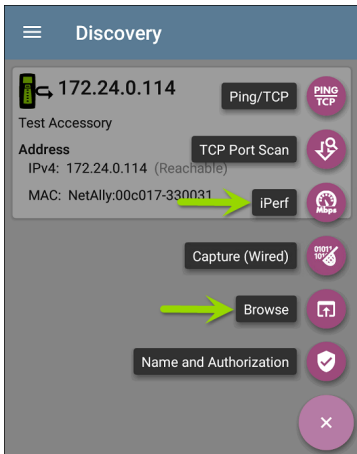
You can start an iPerf test from the Details screen for a Test Accessory in the [Discovery app](#) using the floating action button.

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.

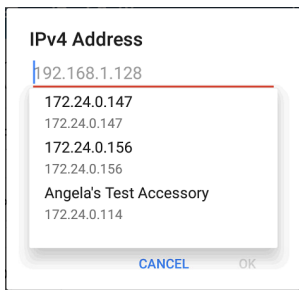
iPerf Settings 	
<b>Interface</b>	Any Port
<b>IPv4 Address</b>	172.24.0.114
<b>Port</b>	5201 (iperf3)
<b>Duration</b>	10 seconds
<b>Protocol</b>	TCP
<b>Direction</b>	Upstream/Downstream
<b>Upstream Threshold</b>	10 Mbps



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.

**Interface:** This setting specifies which LinkRunner port runs the scan. (See [Selecting Ports](#) for explanations of the different ports.)

**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 LinkRunner has discovered through the [discovery process](#), as

well as any Test Accessories that are claimed to the same [Link-Live](#) organization as your LinkRunner.

**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](http://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.

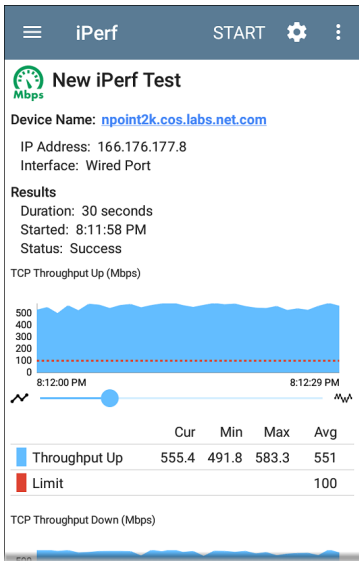
**Upstream and Downstream Bandwidth:** These fields only appear if the **UDP Protocol** is selected. They specify the desired target bandwidth for the iPerf Test using the UDP protocol.

**Upstream and Downstream Thresholds:** Thresholds are the values the LinkRunner 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.

## 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. The Management port links automatically if a connection is available.

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 LinkRunner Test Port from which the test is running.

## Results

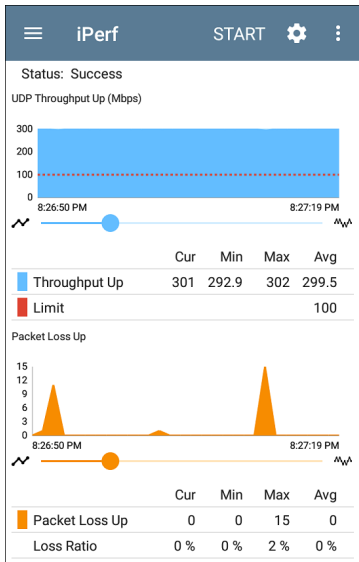
- **Duration:** Configured Duration from the iPerf settings
- **Started:** Time the test started
- **Status:** Success or failure status of the test.

### 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**.



**Link-Live**

by NetAlly

**Iperf Result Filename**

20190619\_134743

**Comment**


Room 302

**Job Comment**

Union Hall



SAVE 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](#)



# LANBERT™ Test App

LANBERT is a Bit Error Rate Testing application that transmits IEEE 802.3 data frames over LAN media and measures the number of frames sent, lost, and errored.



The LANBERT app runs a loopback test on fiber or copper media using:

- A second testing device to act as the loopback endpoint. This device can be an EtherScope nXG or a LinkRunner 10G.
- A switched port available with some Ethernet switches.
- A physical loopback device.


# LANBERT Settings

To run a test with LANBERT, you must configure the generator settings. If you are using this unit as an active loopback device, see [Configuring LANBERT Loopback Settings](#).

## Configuring LANBERT Generator Settings

To configure the LANBERT settings, open the settings  icon on the LANBERT screen or tap the Menu icon  and select **Generator Settings**.

☰ Generator Settings	
Speed	Auto
Frame Size	64 Bytes
Duration	1 minute
Grading Type	Count
Error Threshold	0 (No errors)
Loss Threshold	0 (No loss)

Tap each field to enter or revise selections as needed. Changed settings are automatically applied. When you finish configuring, tap **OK** or **Cancel** to return to the settings screen. When you finish configuring, tap the back button  to return to the LANBERT test screen.


**Speed:** This setting sets the link speed at which the Ethernet frames are sent to and received from the loopback destination.

- You can choose 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, 10 Gbps to match the capacity of the media you want to test. (All settings are full duplex.)
- **Auto** lets the generator and loopback devices auto-negotiate the speed. (The speed may vary if there are errors or impairments.)

**Frame Size:** Sets the size of the Ethernet frames to be sent during the test.

- You can choose presets of 64, 128, 256, 512, 1024, 1518 bytes.

NOTE: Because the object of your bit error rate test is often to "stress" the media path with large amounts of data, choosing the minimum frame size of 64 bytes allows the maximum number of frames to be sent in the duration of the test.


- **Random** varies the frame size at random to simulate variations in real data.
- Tap the pencil icon  to open an editing screen to enter a **Custom Value** for the frame size.

**Duration:** Sets the time for the test. Presets range from 10 seconds up to 24 hours.


**Grading Type:** Sets counts or percentages to grade error or loss thresholds. Both counts and percentages are always shown on the screen.

- **Count:** counts the total number of frames encountering errors or loss of frame and sets the Error Threshold and Loss Threshold presets to numbers.
- **Percent:** calculates the percentage of frames encountering errors or loss of frame and sets the Error Threshold and Loss Threshold presets to percentages.




**Error Threshold:** Defines what constitutes a failed test in terms of frames that were successfully sent and received but that encountered errors that changed the frame check sequences.

- Select a value from the presets:
  - For a Grading Type of Count: 0 (no errors), 1, 10, 100, or 1000.
  - For a Grading Type of Percent: 0.0% (no errors), 0.001%, 0.01%, 0.1%, or 1%.
- **Disabled** turns off grading of errors.
- Tap the pencil icon  to open an editing screen to enter a **Custom Value** for the error threshold.

**Loss Threshold:** Defines what constitutes a failed test in terms of frames that were unsuccessfully sent and received.

- Select a value from the presets:
  - For a Grading Type of Count: 0 (no errors), 1, 10, 100, or 1000.
  - For a Grading Type of Percent: 0.0% (no errors), 0.001%, 0.01%, 0.1%, or 1%.
- **Disabled** turns off grading of losses.
- Tap the pencil icon  to open an editing screen to enter a **Custom Value** for the loss threshold.

## Configuring LANBERT Loopback Settings

To configure this LinkRunner as an active loopback device, select the LANBERT icon  from the Home screen, then tap the Menu icon  and select **Loopback Settings**. When you finish configuring, tap the back button  to return to the LANBERT test screen.

The only available setting is **Speed**.

- Match the speed to the speed you selected for the transmitting test device. You can choose 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, or 10 Gbps. (All settings are full duplex.)
- **Auto** lets the LinkRunner automatically negotiate the speed.



# Running a LANBERT Test

## Before You Begin

- Identify the cable or channel path that you want to test. (Note that LANBERT uses Ethernet frames to test LAN pathways, including copper or fiber cables. It cannot function on wide-area networks or devices that use IP addresses to route traffic.)
- Plug one end of the LAN cable into the LinkRunner [Wired Test Port](#).
- Set up a loopback device at the other end of the LAN pathway to relay the received Ethernet frames back to the LANBERT generator. This device can be:
  - A physical loopback device for either copper or fiber media.
  - An Ethernet switch with a loopback feature. (Consult the manufacturer's documentation for instructions on setting up the loop.)

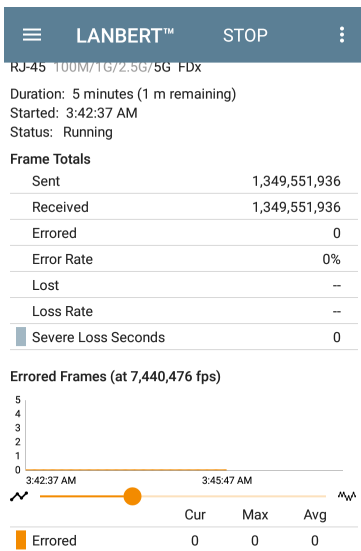
- A NetAlly EtherScope nXG or LinkRunner 10G with the LANBERT application running as the LANBERT Loopback. (Either device can function as the loopback relay and can collect data at the endpoint of the test.) See "[LANBERT Settings](#)" on page 503 for instructions on setting up the loopback settings.

NOTE: The Loopback mode is designed to stop whenever the LANBERT app is not displayed on the screen. If you plan to run a long test, make sure that the loopback unit is plugged into its AC power supply and that you have turned off the sleep function (go to system Settings, tap **Display > Sleep > Never**).

## Run the Test

You can set up and start either the LANBERT generator or the LANBERT loopback unit first. This procedure starts with the generator.

1. On the Tester unit, open the LANBERT application.

2. Tap the **START** button.

The Status shows the current activity:

- Linking: the devices are setting up a connection.
  - Waiting for loopback: the generator is waiting for a response from the loopback device.
3. On the loopback unit (if you are using an EtherScope nXG or LinkRunner 10G as the loopback device):
    - a. Open the LANBERT application.
    - b. Tap on the top left menu icon and tap on **LANBERT Loopback**.
    - c. Tap the **START** button.
    - d. The Status changes to Linking as the connection is set up with the LANBERT generator.
  4. Verify that the Status changes to Running.
    - Test status, frame information, a graph of errored frames are displayed. Multi-gigabit details are also displayed when an RJ-45 line is connected to the Wired Test Port and the link speed is 2.5G, 5G,

or 10G.

- 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.
5. Let the test run to completion. The Status shows the test result (Success or Failure) and may display additional information, such as not connecting at the fastest advertised speed.


## About LANBERT Results

- The color of the LANBERT icon indicates success or failure (green for success, red for failure).
- The first line below the icon displays information about the connection including:
  - Connector type
  - Speed (in bold). Other speeds shown as grayed out values are the ones that were advertised by the link partner but not selected. See the [Wired Link Test Results](#)

for more info about advertised speeds.

- Half versus full duplex ability.

The following example below shows a successful test for an RJ-45 connector that transmitted frames at 10 Gbps at full duplex.



**LANBERT Generator**

RJ-45 100M/1G/2.5G/5G/10G FDx


Duration: 1 minute

Started: 10:19:05 PM

Status: Success

**Frame Totals**

The following example shows an unsuccessful test for an RJ-45 connector that transmitted frames at 100 Mbps at full duplex.



**LANBERT Generator**

RJ-45 10M/100M HDx/FDx

Duration: 10 seconds

Started: 1:45:19 PM

Status: Thresholds exceeded (4)  
No frames were received (5)

**Frame Totals**

- SFP details are shown when using a fiber connection. These include:
  - Wavelength
  - Temperature
  - Voltage
  - Tx Bias Current
  - Tx Power
  - Rx Power
  - Rx Reference Power
  - Rx Power Difference
  - **SET REFERENCE** button (displayed only while test is running): Latches the Rx Reference Power value to the current Rx Power value.
  - **CLEAR REFERENCE** button (displayed only while test is running): Clears the Rx Reference Power value.

NOTE: The LANBERT generator and LANBERT Loopback both use the same reference power value. This


reference power is reset or cleared on a power cycle.

- Loss figures are not displayed until the test ends.
- Severe Loss Seconds occur when the LANBERT generator detects  $\geq 1\%$  frame loss for one second.

#### Frame Totals

Sent	128,020
Received	0
Errored	0
Error Rate	--
Lost	128,020 
Loss Rate	100%
 Severe Loss Seconds	10

## Uploading Results to Link-Live

To send your LANBERT results to the [Link-Live](#) website, tap the action overflow button  at the top right of the LANBERT screen, and then tap **Upload to Link-Live** or **Upload graphs to Link-Live** (which includes the data graphs with the upload).



**Link-Live**

by NetAlly




Comment

Job Comment



SAVE TO LINK-LIVE

The [Link-Live sharing screen](#) opens. You can enter a file name (for active surveys only) and attach comments to the LANBERT results. The

results are displayed on the Results  page on Link-Live.com.



# Link-Live Cloud Service

The screenshot displays the Link-Live Cloud Service interface. On the left, a sidebar shows a list of test results with columns for test name, time, and status. The main area shows detailed information for a specific test titled "Shared ACK-G3-E - 550078".

**Test Details:**

- Shared ACK-G3-E - 550078
- MAC: 00C817-550078
- Device: AirCheck G3
- Type: Wireless
- Profile: InOffice-PvE-Connect to LRG
- Firmware: 2.2.0.43
- Wired Management IP: 10.24.8.3.31
- WiFi Management IP: 10.24.8.101

**Test Results:**

- PHY Rate: 400 Mbps
- Retry Rate: 0%
- Signal: -94 dBm
- Noise: -90 dBm
- SAR: 56 dB
- Success

**Access Point Details:**

- 10.24.8.20
- SSID: LRG
- BSSID: 803c0a118b169-c884cf
- 802.11 Types: a, g, n
- Channel: 149
- Channel Util (%): 5
- Non-802.11 Util (%): 0.5

**DHCP Details:**

- IP: 10.24.8.247
- Server: 10.24.8.1
- Subnet: 255.255.254.0
- DHCP Total: 3417 ms
- Local IP: fe80::2c8:1791:fe55:78

**DNS Details:**

- DNS 1: 127.0.0.1

**Gateway Details:**

- 10.24.8.1

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 LinkRunner 10G is claimed.

The comprehensive LinkRunner 10G offers more features for analyzing your network in Link-Live than previous testers. Claim your LinkRunner to [Link-Live.com](https://Link-Live.com) to access these functions:

- Check for software updates and update your LinkRunner 10G software.
- Download third-party applications from the NetAlly [App Store](#) to use on your LinkRunner.
- 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](https://Link-Live.com), and sign in. You can open the Link-Live website in the LinkRunner's web browser to create and manage your account.

## Claiming the Unit

### On Link-Live.com

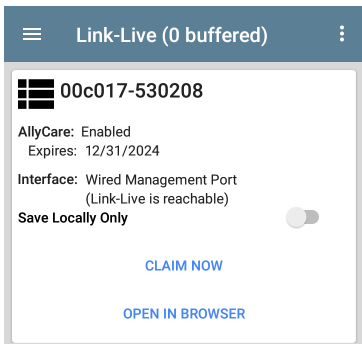
1. The first time you sign in to Link-Live.com, a pop-up window appears, prompting you to claim a device.

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 10G image, and follow the claiming instructions on the Link-Live website.

## On the LinkRunner 10G Unit

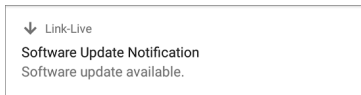
1. Open the Link-Live app. Your unit's MAC address is displayed.



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 LinkRunner 10G 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.




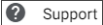
See [Updating Software](#) for more information.

## After Claiming

Once your LinkRunner 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 LinkRunner 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 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 LinkRunner from Link-Live, tap the [navigation drawer](#) icon  in the Link-Live app, tap [About](#), and then tap **UNCLAIM**.





**About**

 **LinkRunner 10G Analyzer**

Serial: 1930007

**MAC Addresses**

Wired: 00c017-5301c4  
Wired Management: 00c017-5301c5  
Wi-Fi: 00c017-5301c6  
Wi-Fi Management: 00c017-5301c7

**System Version:** 2.3.0.167

**Application Version:** 2.3.0.172

**AllyCare:** Enabled  
Expires: 6/24/2024

**SFP Details**

Type: 10GBASE-SR (850 nm)  
Vendor: AVAGO  
Version: G2.3  
Model: AFBR-703SDZ  
Rx Power: --

[UNCLAIM](#)   [EXPORT LOGS](#)

## 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.

[ALLYCARE CODE](#)   [EXPORT LOGS](#)

Tap **AllyCare Code** to open a dialog to enter an AllyCare Activation Code.

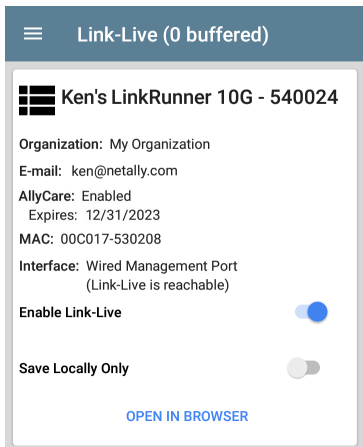
## Private Link-Live Settings

Use these settings only when your organization has deployed a private instance of Link-Live. Consult your IT organization for setting details.

# Link-Live App Features



The main Link-Live app screen on your LinkRunner 10G 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 screenshot shows the Link-Live app interface. At the top, there is a dark blue header with a hamburger menu icon on the left and the text "Link-Live (0 buffered)". Below the header is a white card with a grey border. The card contains the following information:

- Ken's LinkRunner 10G - 540024** (with a Link-Live logo icon)
- Organization: My Organization
- E-mail: ken@netally.com
- AllyCare: Enabled  
Expires: 12/31/2023
- MAC: 00C017-530208
- Interface: Wired Management Port  
(Link-Live is reachable)
- Enable Link-Live:
- Save Locally Only:
- [OPEN IN BROWSER](#)

The LinkRunner 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 LinkRunner's Link-Live app are informational.

**AllyCare** indicates the status of NetAlly's optional AllyCare services. See [NetAlly.-com/Support](https://www.netally.com/Support) for more information.


**Interface** shows which network interface is currently being used by Link-Live to post results and its status.


The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the LinkRunner 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 LinkRunner'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.

 **Link-Live (2 buffered)**

 **Ken's LinkRunner 10G - 540024**


**Organization:** My Organization  
**E-mail:** ken@netally.com  
**AllyCare:** Enabled  
Expires: 12/31/2024  
**MAC:** 00C017-530208  
**Interface:** Wired Management Port  
(Link-Live is reachable)


**Enable Link-Live**

**Save Locally Only**

[OPEN IN BROWSER](#)

---

**Discovery Snapshot**   
Apr 25, 2023 11:16:24 PM

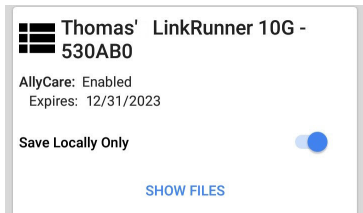
**Wired Snapshot**   
Apr 25, 2023 11:16:25 PM

The buffered files displayed automatically upload to Link-Live.com once your LinkRunner connects to an active network.

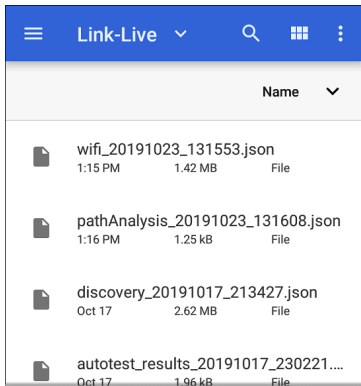
## Saving Locally Only

If you do not want to send your results to the Link-Live website, you can still save results locally to your LinkRunner 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 LinkRunner.

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 [Wired](#) AutoTest 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:

**Link-Live**  
by NetAlly

**File Name**

client1024rsa-new.pem


**Comment**

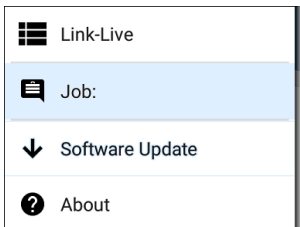
Certs

**Job Comment**

South Campus Wi-Fi

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 LinkRunner. 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
 <b>Results</b>	AutoTest, Performance, iPerf, and Cable Test results Images, connect logs, and other files when saved to a test result
 <b>Uploaded Files</b>	Captures, images, connect logs, and other file types
 <b>Analysis</b>	Discovery and Path Analysis results

If your unit is not claimed to [Link-Live.com](https://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

Save to Link-Live



UPLOAD TO LINK-LIVE

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.

**Link-Live**

by NetAlly

**Wi-Fi Snapshot Name**

20190429\_122109

**Comment**



Conference Room B

**Job Comment**

North Office



SAVE TO ANALYSIS FILES

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.



# Link-Live

by NetAlly



Comment

Conference Room B

---

Job Comment

North Office

---



SAVE TO LAST TEST RESULT



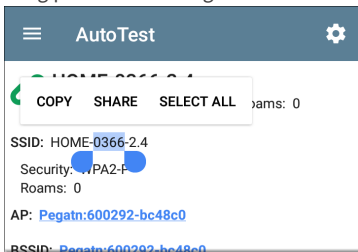
SAVE TO UPLOADED FILES

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.

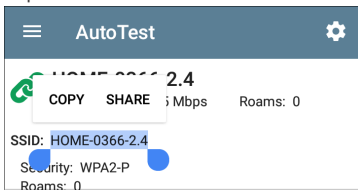
## Sharing a Text File to Link-Live

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.

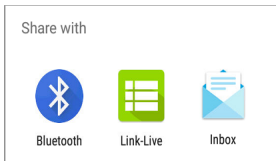


2. Tap **Select All** if needed.







3. Tap **SHARE**.



4. Select the Link-Live icon to open the [Link-Live sharing screen](#).




**Link-Live**  
by NetAlly



**File Name**  
20191106\_155804

**Comment**  
SSIDs

**Job Comment**  
/Inventory

 **SAVE TO LAST TEST RESULT**

5. Enter any **comments** as needed, and then tap **SAVE TO LAST TEST RESULT**.




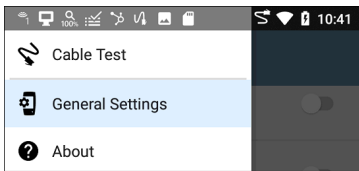
## Cable Test App

LinkRunner 10G'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 LinkRunner unit. Connect a cable to this port for testing and tracing with the tone function.

# Cable Test Settings

The only setting that affects the Cable Test app is the **Distance Unit** setting, which designates Feet or Meters. This setting is contained in the [General Settings](#) menu.

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

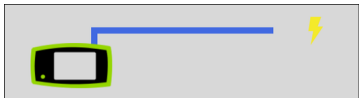


2. Scroll to the bottom of the Settings list under the **Preferences** heading.
3. Tap the **Distance Unit** field, and select either **Feet** or **Meters** as needed, then tap **OK**.

# Running Cable Test

Refer to LinkRunner 10G's [Buttons and Ports](#) as needed.

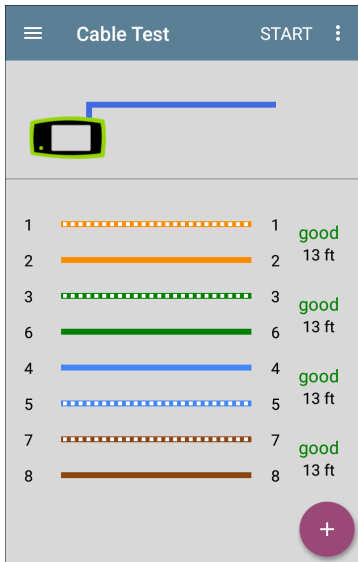
- With an [open or unterminated](#) cable connected to the RJ-45 cable test port (left side of the unit), you can measure length, identify shorts and splits, and locate opens.
- Using a cable terminated with a [WireView Cable ID accessory](#), you can measure cable length and identify shorts, opens, split pairs, crossover cables, normal or negative pair polarity, and shielded cables.
- LinkRunner 10G 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.



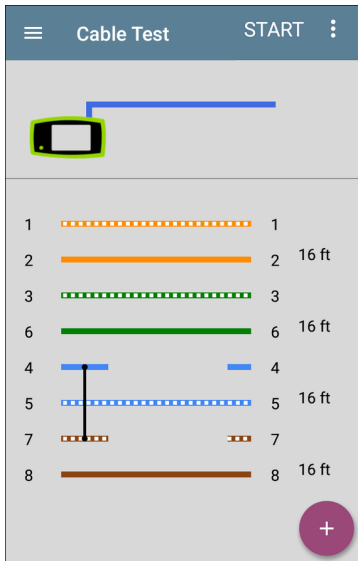
To start the cable test, tap **START** at the top right of the Cable Test app screen.

## Open Cable TDR Testing

LinkRunner 10G 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 left side of the LinkRunner 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, 5, and 7.

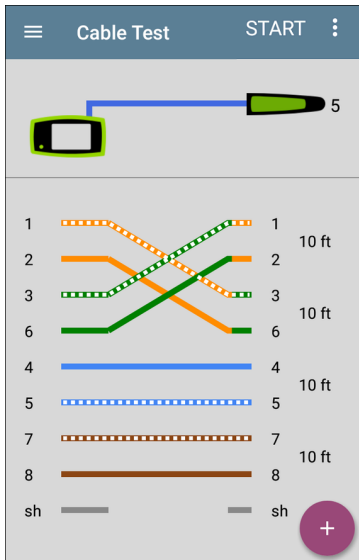


## Terminated WireView Testing

Using a WireView accessory provides more detailed, per-wire results. A WireView #1 is included with your LinkRunner 10G. Additional WireViews 2-6 are available for purchase.

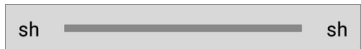
To run a terminated cable test, connect the left side RJ-45 port to a cable terminated with an external WireView Cable ID accessory.

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

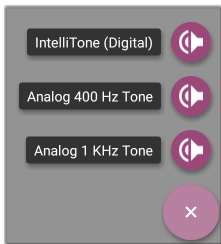


## Toning Function

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



Connect a cable into the left side RJ-45 port, and then tap the floating action button (FAB) .

 Select a Tone option from the menu. The LinkRunner 10G emits the tone through the cable, and the probe detects it, allowing you to trace the wire or locate it in the switch closet.



\* IntelliTone is a trademark of Fluke Networks.

## 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](https://link-live.com).

See the [Link-Live chapter](#) for more information.

# Specifications and Compliance

This chapter contains device specifications and required compliance information.

# LR10G-100/200

## Specifications

### General

<b>Dimensions</b>	4.05 in x 7.67 in x 2.16 in (10.3 cm x 19.5 cm x 5.5 cm)
<b>Weight</b>	1.677 lbs (0.76 kg)
<b>Battery</b>	Rechargeable lithium-ion battery pack (7.2 V, 6.4 Ah, 46 Wh)
<b>Battery Run Duration, Charge Time</b>	Typical duration: 3-4 hours Typical charge time: 2-4 hours
<b>Display</b>	5.0-inch color LCD with capacitive touchscreen (720 x 1280 pixels)
<b>Host Interfaces</b>	RJ-45 Cable Test and Management Port USB Type-A Port USB Type-C On-the-Go Port
<b>SD Card Port</b>	Supports Micro SD card storage
<b>Memory</b>	Approximately 8 GB available for storing test results and user applications

<b>Charging</b>	USB Type-C 45-W adapter: AC Input Power 100-240 V, 50-60 Hz; DC Output Power 15 V (3 A)
<b>Media Access</b>	Copper: 10M/100M/1G/2.5G/5G/10G Fiber SFP Adapters: 1G/10GBASE-X
<b>Supported IEEE Standards</b>	Wired: 802.3/ab/ae/an/bz/i/u/z Wi-Fi: 802.11a/b/g/n/ac PoE: 802.3af/at/bt, Class 0-8 and UPOE
<b>Cable Test</b>	Pair lengths, opens, shorts, splits, crossed, straight through, and WireView ID
<b>Tone Generator</b>	Digital tone: [455 KHz]; Analog tones: [400 Hz, 1 KHz]
<b>LEDs</b>	2 LEDs (Activity and Link Indic- ators)

## Environmental Specifications

<b>Operating Temperature</b>	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).
<b>Operating relative humidity (% RH without condensation)</b>	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)
<b>Storage Temperature</b>	-4°F to 140°F (-20°C to +60°C)
<b>Shock and vibration</b>	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
<b>Safety</b>	IEC 61010-1:2010: Pollution degree 2
<b>Altitude</b>	Operating: 4,000 m; Storage: 12,000 m



# Certifications and Compliance

**⚠ CAUTION:** Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.



Conforms to relevant European Union directives.



Conforms to relevant Australian Safety and EMC standards.



Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.



Listed by the Canadian Standards Association.

## 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.

---

<b>EMC</b>	IEC 61326-1:2013: 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.

Accessory Information:

Adapter Model No.: FSP045-A1BR

Input: AC 100-240 V, 50/60 Hz 1.2 A

Output: DC 15 V, 3 A

---

Battery: 3250 mAh, 7.2 V 6.4 Ah

---