netAlly

EtherScope™ nXG
User Guide

Tap a link to go directly to the app's chapter.
Search 🔍 this PDF for a specific term or phrase.
Scroll down to view the full list of Contents.

Software v1.3 Published July 21, 2020

Contents

Wi-Fi Analysis App 478

Contact Us

Online: NetAlly.com

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

NetAlly
2075 Research Parkway
Colorado Springs, CO 80920

For additional product resources, visit NetAlly.com/Products/EtherScopenXG.

For customer support, visit NetAlly.com/Support.

Register your EtherScope nXG

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

Register on the NetAlly Support Page.

Back to Title and Contents

Introduction

The EtherScope nXG Portable Network Expert is a rugged, hand-held tool for testing and analyzing copper, fiber, and Wi-Fi networks. It features applications developed by NetAlly for network discovery, measurement, and validation, which are available from the Home and Apps screens.

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

How to Use this Guide

This User Guide describes the EtherScope nXG's testing functionality and basic elements of the Android interface.

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

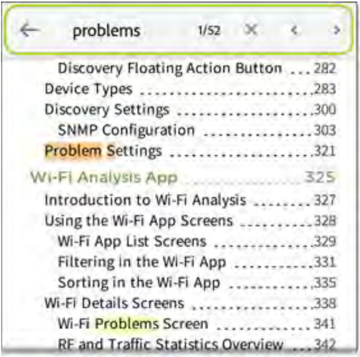
The EtherScope nXG may also be referred to as just EtherScope or the "unit" in this guide.

The PDF Reader App

A PDF reader application is pre-installed on your EtherScope to allow easy navigation of this guide:

- Tap **blue links** to go to their destinations. Underlined blue links open external websites.
- Touch headings in the **Contents** list that starts on page 2 to go to the corresponding sections.
- Use the Search function 🔍 in the upper toolbar to find specific terms in the guide.

Once you enter a term and search, the term appears at the top of the PDF reader screen. Touch the left and right arrows to search forwards and backwards in the guide for the term. In the image below, the user has searched "problems."

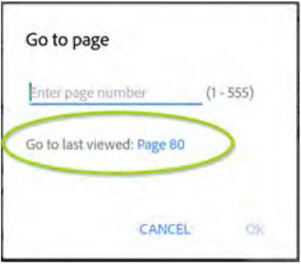


← problems 1/52 ✕ ‹ ›

Discovery Floating Action Button . . . 282
Device Types 283
Discovery Settings 300
SNMP Configuration 303
Problem Settings 321
Wi-Fi Analysis App 325
Introduction to Wi-Fi Analysis 327
Using the Wi-Fi App Screens 328
Wi-Fi App List Screens 329
Filtering in the Wi-Fi App 331
Sorting in the Wi-Fi App 335
Wi-Fi Details Screens 338
Wi-Fi Problems Screen 341
RF and Traffic Statistics Overview 342

- To scroll quickly up or down in the guide, touch and drag the page number tab 141 at the right. Drag the tab to the very top of the screen to return to the title page.

- Touch and hold the page number tab 141 to open a dialog that allows you to return to the previous page you were viewing.



Go to page

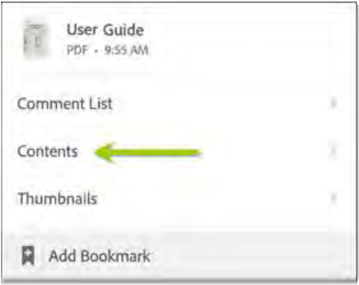
Enter page number (1 - 555)

Go to last viewed: Page 80

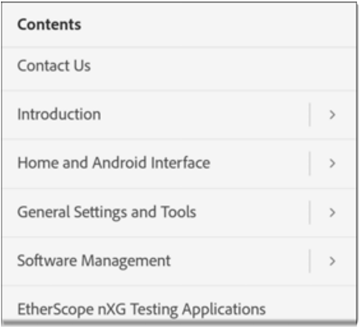
CANCEL OK

NOTE: Touching the back buttons, ◁ or ←, will not take you back to your previous place in a PDF.

- To browse the PDF **Contents** or **Bookmarks**, touch the action overflow icon ⋮ in the upper tool bar.



Select **Contents** to view the list of chapters and choose a section to read.

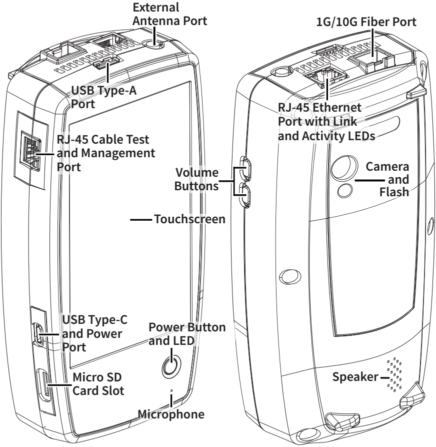

Contents
Contact Us
Introduction
Home and Android Interface
General Settings and Tools
Software Management
EtherScope nXG Testing Applications

- Tap the blue **Back to Title and Contents** link wherever it appears to return to the title page with app links.
- Scroll to show or hide the app toolbars at the top of the Adobe Reader screen and the floating action button (FAB) ✎ at the bottom right.
- Tap the screen twice to zoom in or out.

To download this guide onto another device, you can transfer the PDF file using one of the methods described in the Managing Files section, or go to NetAlly.com/Products/EtherScopenXG.

Buttons and Ports

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



Feature	Description
Fiber Port 1G/10GBASE-X	Connects to an SFP adapter and fiber cable for network testing. NOTE: 100FX SFPs are not supported.
RJ-45 LAN Port 10M/100M/1G/2.5G/5G/10G-BASE-T	Connects to a copper Ethernet cable for network testing Charges the unit if PoE Class 4 or higher is available
Transmit LEDs	Green LED lit: Linked Yellow LED flashing: Activity
USB Type-A Port	Connects to any USB device
RJ-45 Cable Test and Management Port	Connects to an Ethernet cable for patch cable testing and unit management
USB Type-C On-the-Go Port	Connects to a USB Type-C connector for file transfer and to the included AC adapter for charging the unit
Power Button and LED	Green LED: Unit is powered on Red LED: Unit is charging
Microphone	Allows voice input
Camera and Flash	Captures images and acts as a flashlight

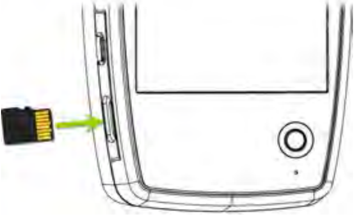
FEATURE	DESCRIPTION
Micro SD Card Slot	Used for removable storage expansion (See Inserting a Micro SD Card below.)
Volume Buttons	Increase or decrease the audio volume
Speaker	Produces audio

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

Refer to the product Specifications if needed.

Inserting a Micro SD Card

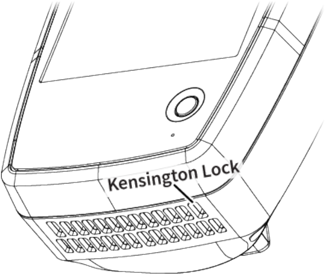
A Micro SD card must be inserted with the ***metal contacts facing the front*** (towards the touchscreen) of the unit, as shown below.



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 EtherScope nXG 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 LED button turns red when the unit is in charging mode and turns off at full charge. The unit will fully charge in 2-4 hours via AC power.

When in charging mode (meaning the unit is off but plugged into an AC power source), the unit will turn on once every 24 hours and top off the battery charge, then power off again.

Tap the power button briefly to view the battery level on the screen while the unit is in charging mode.

When on battery power only, the unit will run for 3-4 hours, depending on the type of testing being conducted.

PoE Charging

Power over Ethernet (PoE) is also convenient

To charge with PoE, connect the top RJ-45 port on the unit to a network switch with PoE or a PoE injector. The following conditions must be met for the unit to charge with PoE:

The unit must be powered on or in display sleep mode.

The **Charge Battery via PoE** setting must be enabled in General Settings.

The EtherScope must also run an AutoTest Wired Profile with a passing PoE test to detect PoE availability, meaning 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 EtherScope 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 LED remains on. Touch 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 the power button for one second until the “Power off” and "Restart" dialog box appears on the touchscreen, and then touch **Power off** or **Restart**.
- If the unit is unresponsive to a normal power off, press and hold the power button for five seconds to perform a hard shutdown.

Back to Title and Contents

Safety and Maintenance

Observe the following safety information:

Use only the Adapter provided or Power over Ethernet 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.**
✳	**Class 1 Laser Product. Do not look into the laser.**

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

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

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

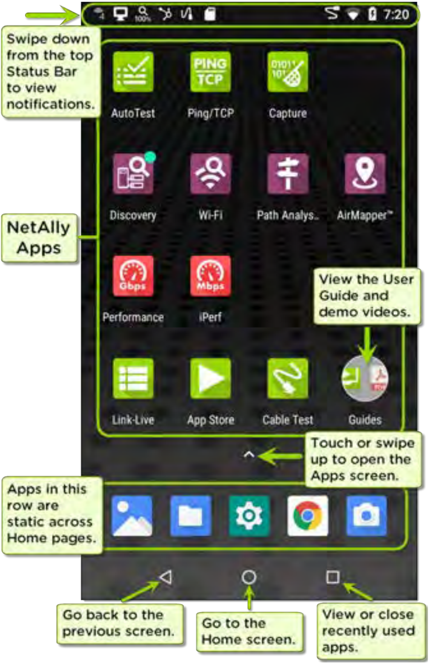
Back to Title and Contents

Home and Android Interface

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

The EtherScope nXG interface supports many of the operations typical of any Android 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


Swipe down from the top Status Bar to view notifications.
7:20
AutoTest
Ping/TCP
Capture
Discovery
Wi-Fi
Path Analys..
AirMapper™
NetAlly Apps
Performance
iPerf
View the User Guide and demo videos.
Link-Live
App Store
Cable Test
Guides
Touch or swipe up to open the Apps screen.
Apps in this row are static across Home pages.
Go back to the previous screen.
Go to the Home screen.
View or close recently used apps.

Like other Android devices, your EtherScope nXG 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 touching, 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 Android System

The navigation actions you can perform to move through screens and panels on the EtherScope nXG are the same as those you would use to navigate an Android phone or tablet.

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

◁ The back icon returns to the previous screen.

○ The circle icon opens the Home screen.

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

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

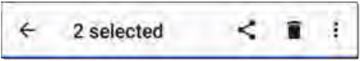
Swiping

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

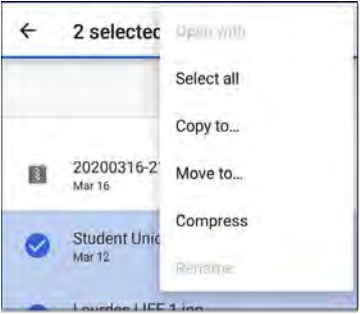
Long Pressing

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

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



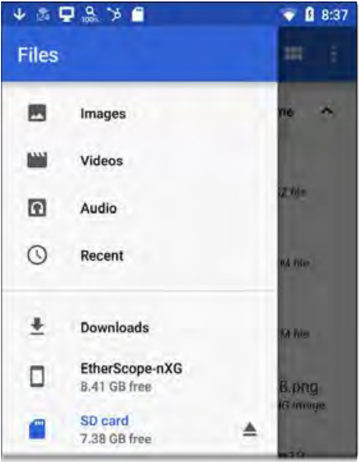
Additional options often appear in an overflow menu, designated by the action overflow icon ⋮.



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

Left-Side Navigation Drawer

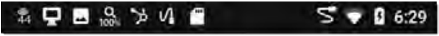
Touch the Menu icon ☰ or swipe right in the Files 📁 app to open the navigation drawer. It displays the folders in your file system.



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 **EtherScope-nXG** folder and sub-folders, as shown above.

See the Navigation Drawer topic for more.

Android Status Bar and Notifications



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

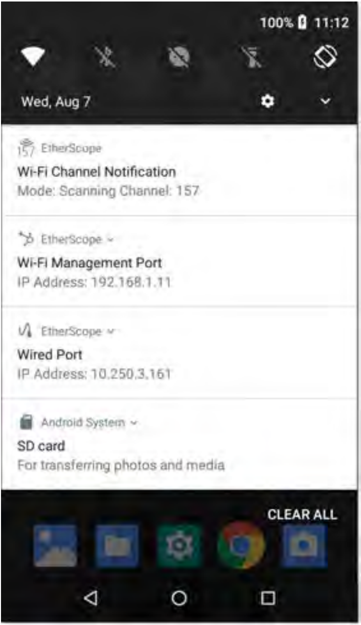
See Test and Port Status Notifications for details about the icons and notifications related to EtherScope nXG network connections, testing, and management.

Touch 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 Android 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.



100% 11:12

Wed, Aug 7

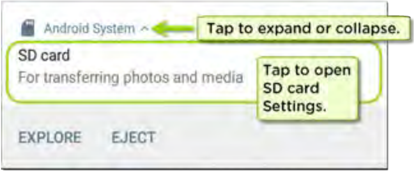
EtherScope
Wi-Fi Channel Notification
Mode: Scanning Channel: 157

EtherScope
Wi-Fi Management Port
IP Address: 192.168.1.11

EtherScope
Wired Port
IP Address: 10.250.3.161

Android System
SD card
For transferring photos and media

- Touch the title and down arrow ⌵ on a notification (or swipe down on it) to expand the box and view more details or options.


Android System ^
Tap to expand or collapse.
SD card
For transferring photos and media
Tap to open SD card Settings.
EXPLORE
EJECT

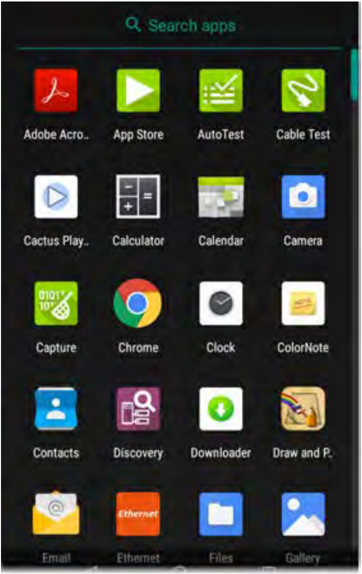
- Touch the middle of a notification to open the related app, image, or device settings or to perform other related actions.
- Swipe left on a notification to dismiss it.

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

- Touch **CLEAR ALL** at the lower right of the panel to dismiss all Android 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 touch the up arrow icon ^.



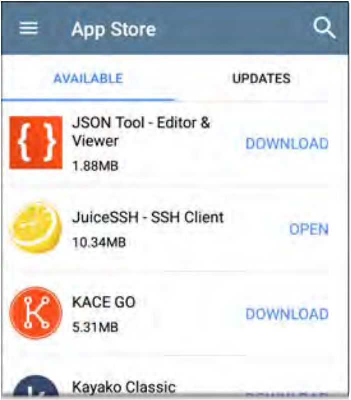
The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.

- 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 Android applications to use on your EtherScope nXG.

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

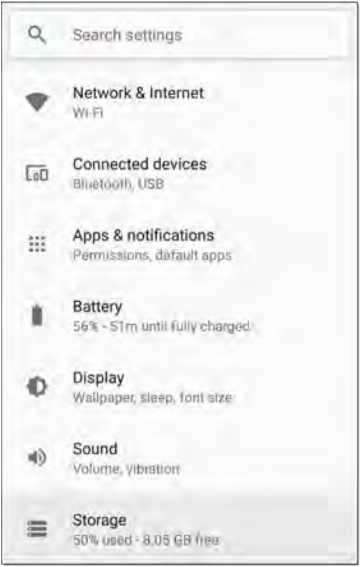


Touch the search icon to search for an App.

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

Device Settings

To access the Android system device settings, touch the Settings ⚙ icon at the bottom of the Home screen.



Search settings

Network & Internet
Wi-Fi

Connected devices
Bluetooth, USB

Apps & notifications
Permissions, default apps

Battery
56% - 51m until fully charged

Display
Wallpaper, sleep, font size

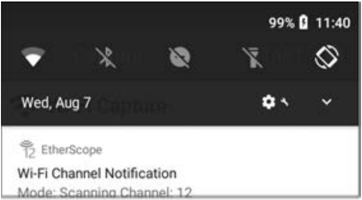
Sound
Volume, vibration

Storage
50% used - 8.05 GB free

Use the device settings screen to adjust the display, sound, and date/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.

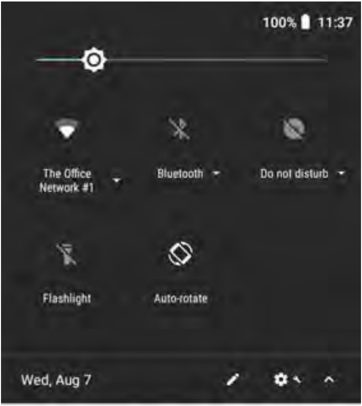


EtherScope

Wi-Fi Channel Notification

Mode: Scanning Channel: 12

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. For example, you can turn the unit's **Wi-Fi** or screen **Auto-rotate** functions on or off from the quick settings.

- Touch and hold an icon to open the relevant device setting screen, if there is one. For example, touch and hold the Wi-Fi icon to open Android's Wi-Fi settings or 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, touch **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. It will automatically power 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.

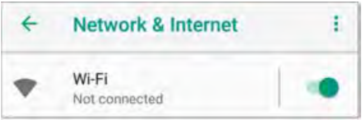
Connecting to Wi-Fi

To access the internet via Wi-Fi, set up the Android device Wi-Fi connection. The Wi-Fi Management Port connects via the main Android Wi-Fi function.

NOTE: While Wi-Fi AutoTest profiles connect to Wi-Fi networks for testing, those Wi-Fi Test Port connections do not perform the functions of the main device Wi-Fi access.

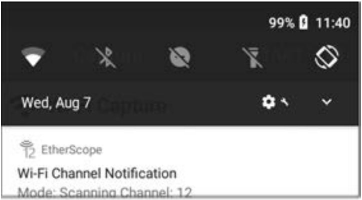
To connect your EtherScope to a Wi-Fi network, access the Android Wi-Fi Device Settings using either method below:

- Open the device Wi-Fi settings from the main Device Settings screen by touching the Settings icon ⚙ and selecting **Network & Internet > Wi-Fi**.



- Open device Wi-Fi settings from the Quick Settings panel by dragging down the top

Status Bar and touching and holding (long pressing) the Wi-Fi icon.

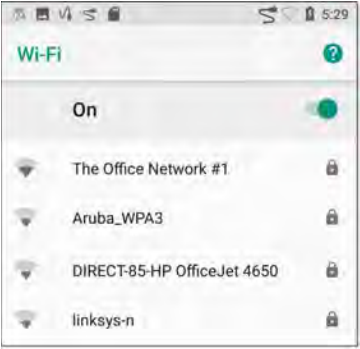


EtherScope

Wi-Fi Channel Notification

Mode: Scanning Channel: 12

Either path opens the Wi-Fi settings screen.



Wi-Fi

On

The Office Network #1

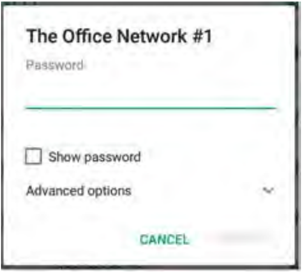
Aruba_WPA3

DIRECT-85-HP OfficeJet 4650

linksys-n

1. Ensure the Wi-Fi feature is **On**.

2. Touch an available Wi-Fi network in the list.
3. Enter the network's security credentials.



The Office Network #1

Password

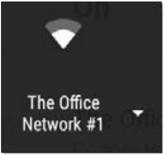
□ Show password

Advanced options

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. After entering credentials, touch 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.

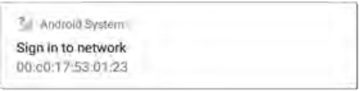


The Office Network #1

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 Android notification icon appears in the top Status Bar. Drag down from the top of the screen to open the notification.



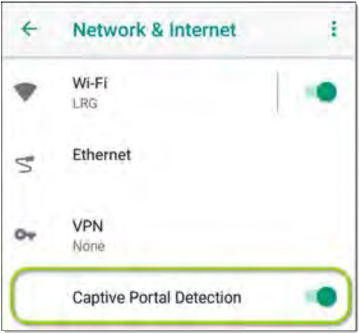
Android System

Sign in to network

00:c0:17:53:01:23

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

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



Network & Internet

Wi-Fi
LRG

Ethernet

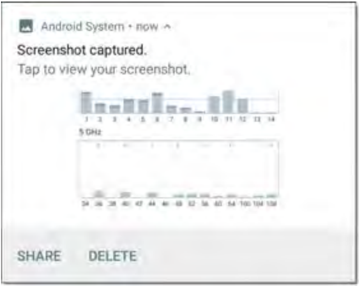
VPN
None

Captive Portal Detection

Sharing

EtherScope nXG allows you to “share” images and files like you would on any Android device. When you see the Share icon ⋖, touch it to view your configured sharing options.

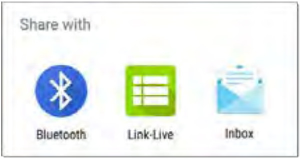
For example, the image below shows an expanded Screenshot notification from the top notification panel.



Screenshot captured.

Tap to view your screenshot.

Touch **SHARE** to open the “Share with” pop-up dialog, where you can choose a sharing method, such as email, messaging, or uploading to Link-Live Cloud Service online.

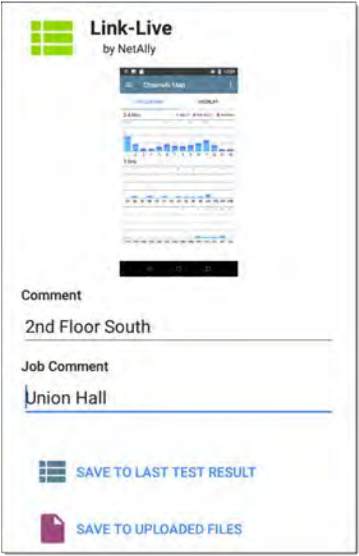


Sharing Files to Link-Live

From the “Share with” dialog box (and other screens on the EtherScope), touch the **Link-Live** option to share (upload) a file to Link-Live Cloud Service at Link-Live.com.

Files can be attached to a test result or uploaded individually to the Uploaded Files page on Link-Live.

The example below shows the Link-Live sharing screen for a screenshot image.



Link-Live
by NetAlly

Comment
2nd Floor South

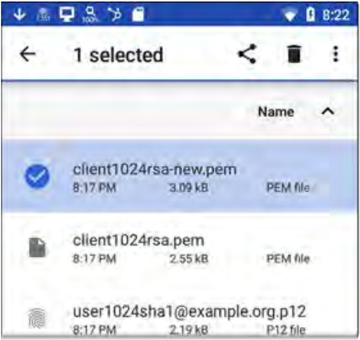
Job Comment
Union Hall

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

Sharing from the Files App

Files from internal or external storage can also be shared to Link-Live.com from the Android Files app. For most file types, you can only upload one selected file at a time, but multiple image files can be shared at once.

1. With the Files app opened, navigate to the folder containing the files you want to share using the left-side navigation drawer.
2. Long press on a file to select it.

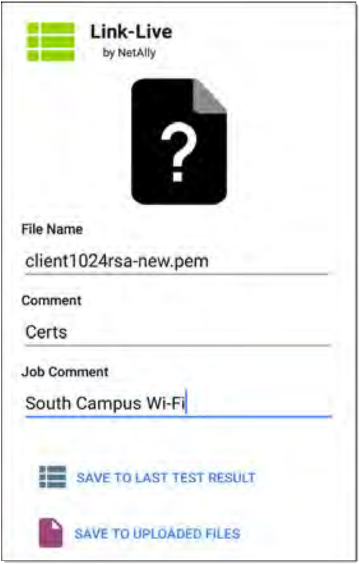


client1024rsa-new.pem
8:17 PM 3.09 kB PEM file

client1024rsa.pem
8:17 PM 2.55 kB PEM file

user1024sha1@example.org.p12
8:17 PM 2.19 kB P12 file

3. Touch the share icon in the top toolbar.
4. If needed, touch the **Link-Live** option.



File Name
client1024rsa-new.pem

Comment
Certs

Job Comment
South Campus Wi-Fi

5. Enter any **Comments** you would like attached to your file.
6. Select **SAVE TO LAST TEST RESULT** or **SAVE TO UPLOADED FILES**.

You files are uploaded and viewable on Link-Live.com.

See the Link-Live chapter for more information on using Link-Live with your EtherScope nXG.

Saving a Screenshot

On the EtherScope nXG unit, press and hold the **Power** button and the **Volume Down** button at the same time for one second to save a screenshot of the current screen. (See Buttons and Ports for button locations).

When a screenshot is taken, the unit beeps and displays the captured screenshot notification in the Notification Panel. Open the notification to share the image using Link-Live, Bluetooth, or another configured application.

EtherScope nXG Settings and Tools

The EtherScope nXG 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 EtherScope nXG*.

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

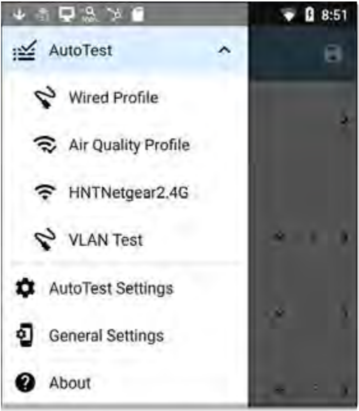
Access common settings and informational screens for the NetAlly testing apps (like AutoTest or Capture) by opening the left-side Navigation Drawers ☰ or Settings ⚙.

Navigation Drawer

Many Android 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:

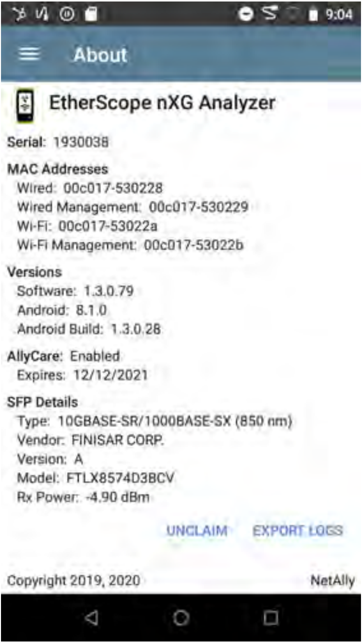
- Touch the menu icon ☰ at the top left of the testing application screens.
- Touch and drag (swipe) to the right from the very left side of the app screens.



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



EtherScope nXG Analyzer

Serial: 1930038

MAC Addresses
Wired: 00c017-530228
Wired Management: 00c017-530229
Wi-Fi: 00c017-53022a
Wi-Fi Management: 00c017-53022b

Versions
Software: 1.3.0.79
Android: 8.1.0
Android Build: 1.3.0.28

AllyCare: Enabled
Expires: 12/12/2021

SFP Details
Type: 10GBASE-SR/1000BASE-SX (850 nm)
Vendor: FINISAR CORP.
Version: A
Model: FTLX8574D3BCV
Rx Power: -4.90 dBm

Copyright 2019, 2020 NetAlly

The About screen displays the serial number, MAC addresses, software versions, SFP details and current AllyCare contract status for your EtherScope nXG.

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

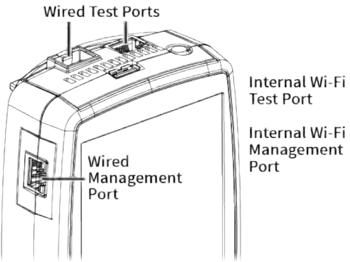
Exporting Logs

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

Touch the **EXPORT LOGS** link on the About screen 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.)

Test and Management Ports

The EtherScope nXG has two wired RJ-45 copper ports, a fiber port, and two Wi-Fi radios, each with specific test or management functions described in this section.

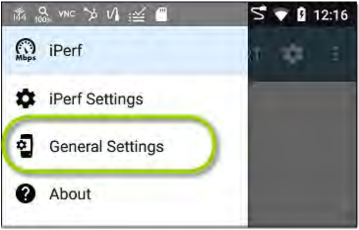


Either the top copper port or fiber port can act as the Wired Test Port, so in total, the EtherScope has *four* network interfaces:
1 Wired Test, 2 Wi-Fi Test, 3 Wired Management, and 4 Wi-Fi Management.

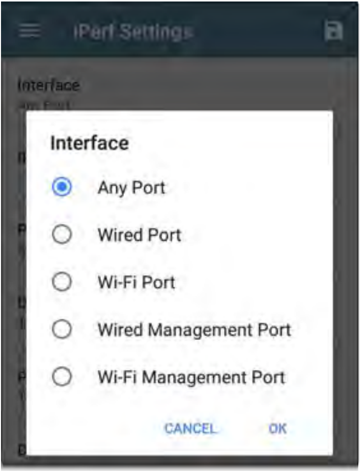
Refer to Buttons and Ports and the technical Specifications if needed.

Configuring the Ports

The NetAlly apps' General Settings control EtherScope's use of the test and management ports. The **General Settings** are accessible from the left-side navigation drawer in NetAlly's testing apps, such as AutoTest, Capture, and iPerf.



The app-specific settings ⚙ for many of the individual NetAlly testing apps (like the **iPerf Settings** above) also let you choose which ports the app uses for its test or analysis.



Interface

● Any Port

○ Wired Port

○ Wi-Fi Port

○ Wired Management Port

○ Wi-Fi Management Port

All of the ports are described below next to their corresponding status icons.

Test Ports

EtherScope runs Wired and Wi-Fi AutoTests, Captures, Discovery, and comprehensive network analyses over the test ports.

You must run an AutoTest Wired or Wi-Fi Profile in order to establish a link on the Wired or Wi-Fi 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 EtherScope detects a new copper link in the top Wired Test Port. Wired fiber connections and Wi-Fi Profiles must be started manually in the AutoTest app.

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

> **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.

Wi-Fi Test Port: The internal Wi-Fi test adapter is a 4x4 Dual-band 802.11ac wireless radio. To disable, see General Settings in the testing apps' left-side navigation drawer.

Management Ports

EtherScope can run Discovery, Ping/TCP Connect tests, Path Analysis, and iPerf tests on the management ports, but not AutoTests, packet captures, or Performance tests.

The Management Ports provide a more stable network connection than the Test Ports, as the Test Ports may frequently drop link and reconnect or resume scanning.

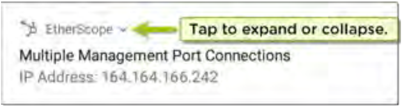
Wi-Fi Management Port: The internal Wi-Fi management port runs on the main Android system's 1x1 Dual-band 802.11ac + Bluetooth 5.0 wireless adapter, which is configured in the Android Device Settings. See Connecting to Wi-Fi to configure this connection.

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

Test and Port Status Notifications

EtherScope nXG 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 touch the title and down arrow to expand the box and view more details or options.



Multiple Management Port Connections
IP Address: 164.164.166.242

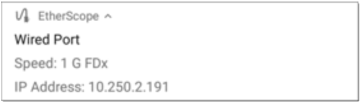
The following EtherScope icons may appear in your Status Bar with the meanings described.

> NOTE: Read Test and Management Ports for descriptions of the port functions.
>
> Also, 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.



EtherScope ^

Wired Port

Speed: 1 G FDx

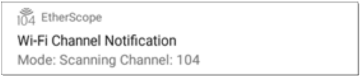
IP Address: 10.250.2.191

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

6 The **Wi-Fi Test Port** status displays with the wireless channel number under a Wi-Fi or Link icon.

6 When the EtherScope unit is dwelling on a Wi-Fi channel (in this case channel 6), the channel number is static and the Wi-Fi icon displays above it.

64 When the EtherScope is scanning wireless channels for discovery, Wi-Fi analysis, or air quality measurements, the number changes dynamically to show which channel is currently being scanned.

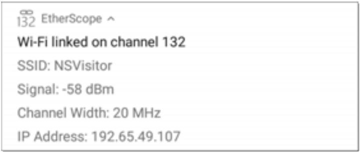


104 EtherScope

Wi-Fi Channel Notification

Mode: Scanning Channel: 104

1 When the EtherScope unit is connected to an AP on a Wi-Fi channel, the channel number is static, and the Link icon displays above it.



132 EtherScope ^

Wi-Fi linked on channel 132

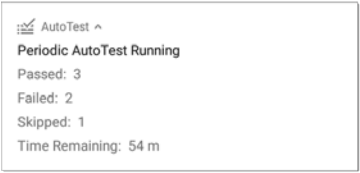
SSID: NSVisitor

Signal: -58 dBm

Channel Width: 20 MHz

IP Address: 192.65.49.107

Periodic AutoTest is running or has completed. When Periodic AutoTest is running, the Wired and/or Wi-Fi Test Ports may not be available to other testing apps.



AutoTest ^

Periodic AutoTest Running

Passed: 3

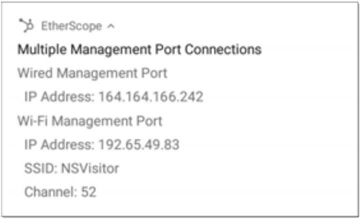
Failed: 2

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 Android Wi-Fi adapter.



EtherScope ^

Multiple Management Port Connections

Wired Management Port

IP Address: 164.164.166.242

Wi-Fi Management Port

IP Address: 192.65.49.83

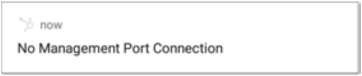
SSID: NSVisitor

Channel: 52

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).

A **Wi-Fi Management Port** connection is established via the main Android Wi-Fi adapter. Its details are displayed under the Management Port notification.

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.

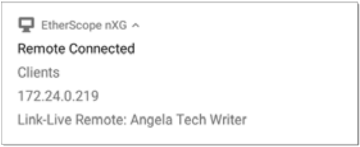
No links are currently available for active discovery, either because none of the ports enabled for discovery are connected or AutoTest is running. Discovery is temporarily disabled when AutoTest is running.

PoE

PoE 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.



EtherScope nXG ^

Remote Connected

Clients

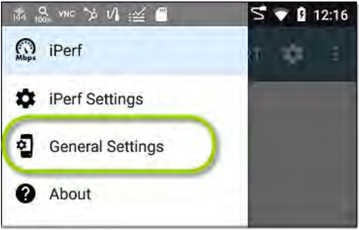
172.24.0.219

Link-Live Remote: Angela Tech Writer

EtherScope nXG General Settings

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

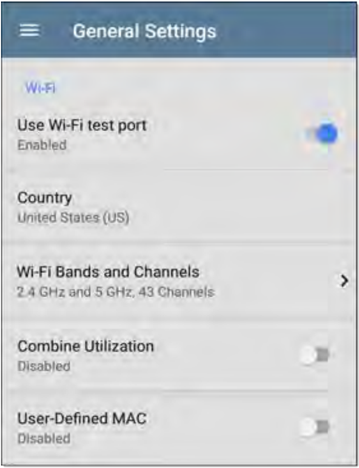
Access the General Settings from the left-side navigation drawer ☰ in the NetAlly testing apps, such as AutoTest, Discovery, Capture, iPerf, etc.



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

Wi-Fi

The Wi-Fi General Settings control functions of the Wi-Fi Test Port functions.



General Settings

Wi-Fi

Use Wi-Fi test port
Enabled

Country
United States (US)

Wi-Fi Bands and Channels
2.4 GHz and 5 GHz, 43 Channels

Combine Utilization
Disabled

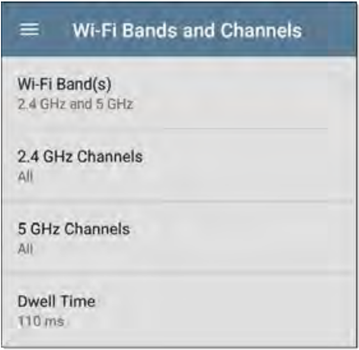
User-Defined MAC
Disabled

Use Wi-Fi test port: Enable or disable Wi-Fi tests, connections, and measurements in the testing apps, including AutoTest Wi-Fi Profiles and the Wi-Fi analysis app.

> NOTE: This setting does not disable the main Android device Wi-Fi function, which controls the Wi-Fi Management port connection. See Device Settings to disable the Android Wi-Fi.

Country: Set the unit for legal operation in your country. This setting affects the Wi-Fi bands and channels on which the unit transmits.

Wi-Fi Bands and Channels: Select the wireless frequency bands and channels the unit scans for devices and measurements such as utilization.



Wi-Fi Band(s)
2.4 GHz and 5 GHz

2.4 GHz Channels
All

5 GHz Channels
All

Dwell Time
110 ms

From this screen, you can also choose or enter a custom **Dwell Time**, meaning the amount of time the EtherScope lingers on each channel gathering data. Tap the Dwell Time field to adjust this setting.

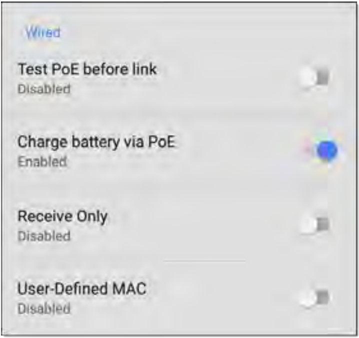
Combine Utilization: Enable this setting to combine 802.11 and non-802.11 channel utilization into one total utilization measurement. In environments with 802.11ax traffic, turn this setting on to accurately measure channel utilization. When this setting is enabled, EtherScope app screens that typically show both 802.11 and non-802.11 utilization, such as the Wi-Fi Channels Map, will instead show only total utilization.

User-Defined MAC: This setting affects the Wi-Fi 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. Touch the lower field to enter your desired MAC address for the EtherScope. 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 that 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.



Wired

Test PoE before link
Disabled

Charge battery via PoE
Enabled

Receive Only
Disabled

User-Defined MAC
Disabled

Test PoE before Link: By default, an AutoTest Wired Profile performs the Link test before the PoE test may be able to complete. Enable this setting to make your EtherScope 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: This setting is enabled by default. If you do not want your EtherScope unit to charge when connected to a switch with PoE, touch 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.

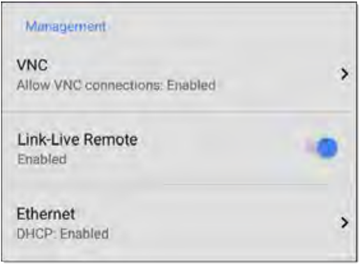
Receive Only: Enabling this setting prevents the EtherScope from transmitting packets on the Wired Test Port. You can also use the **Stop After** function in Wired AutoTest Profile Settings to hide the AutoTest cards that require transmit capability. Set the AutoTest **Stop After** setting to **Switch**. 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. Touch the lower field to enter your desired MAC address for the EtherScope. 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.

Management

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



Management

VNC
Allow VNC connections: Enabled

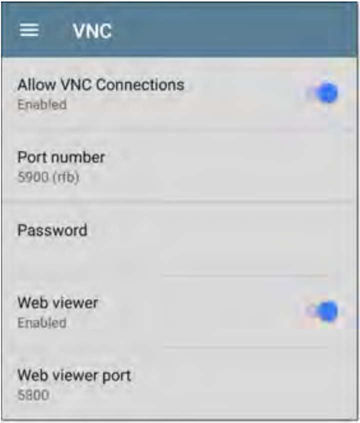
Link-Live Remote
Enabled

Ethernet
DHCP: Enabled

VNC

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

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



VNC

Allow VNC Connections
Enabled

Port number
5900 (rfb)

Password

Web viewer
Enabled

Web viewer port
5800

Allow VNC Connections: Touch the toggle button to enable or disable remote connections from VNC clients.

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

Password: Touch to enter a password, which a VNC user must enter to access the EtherScope 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: Touch the toggle to enable or disable web viewer access.

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

Link-Live Remote

This setting enables or disables the EtherScope'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. See NetAlly.com/Support for more information.

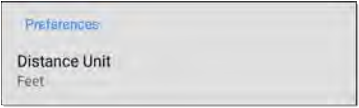
Access the Remote function on the **Units** page at Link-Live.com by selecting the claimed EtherScope nXG.

Ethernet

DHCP: This setting controls IP address assignment of the RJ-45 Wired Management

Port on the left side of the EtherScope. By default, DHCP is enabled. Touch this field and tap the toggle button to disable DHCP and enter static IP information.

Preferences



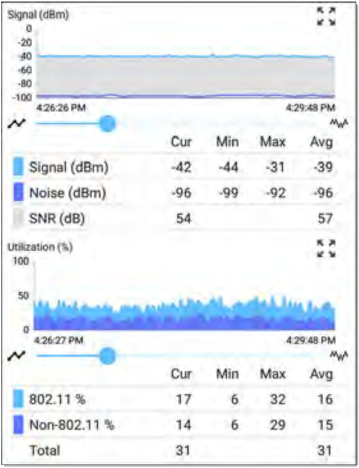
Preferences

Distance Unit
Feet

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

Trending Graphs

Many of the EtherScope nXG 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 Signal and Utilization graphs from the AutoTest Wi-Fi Link Screen.



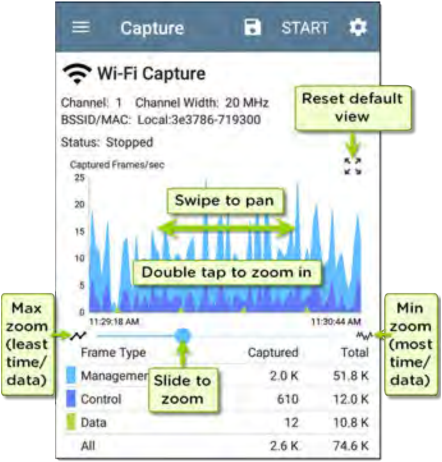
	Cur	Min	Max	Avg
🟦 Signal (dBm)	-42	-44	-31	-39
🟦 Noise (dBm)	-96	-99	-92	-96
⬜ SNR (dB)	54			57

	Cur	Min	Max	Avg
🟦 802.11 %	17	6	32	16
🟦 Non-802.11 %	14	6	29	15
Total	31			31

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

Under each graph, a legend table indicates the measurements that correspond to each plotted color.

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



Wi-Fi Capture

Channel: 1 Channel Width: 20 MHz
BSSID/MAC: Local:3e3786-719300

Status: Stopped

Frame Type	Captured	Total
🟦 Managemer	2.0 K	51.8 K
🟦 Control	610	12.0 K
🟩 Data	12	10.8 K
All	2.6 K	74.6 K

- 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 in time, 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 *once you have zoomed or panned* on the graph.
    - The default time interval varies across different apps.

The following apps and screens contain trending graphs:

- AutoTest Wi-Fi Profiles – Link and Channel
- Ping/TCP – Ping Test

- Capture
- Discovery – Interface Statistics
- Wi-Fi – RF and Traffic Statistics
- Performance
- iPerf

Common Icons

The icons below appear in multiple NetAlly test and Android 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

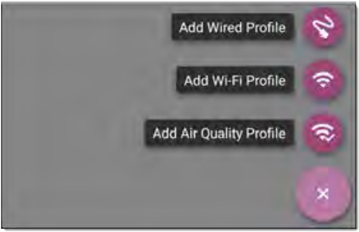
Directional Arrows (or Carets) - indicate the ability to "drill in," open a screen, or expand a panel for more detailed information, or to change the order of a list

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

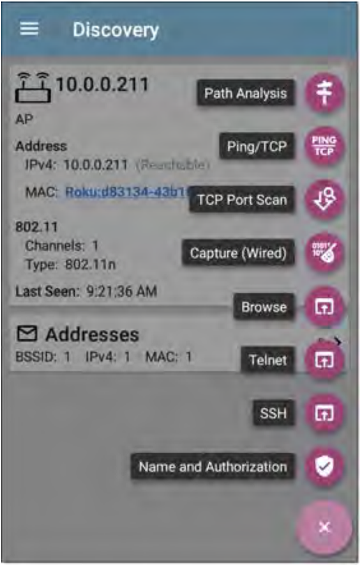
Floating Action Button (FAB) and Menu

Many Android 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 new testing Profiles.



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



10.0.0.211

AP

Address
IPv4: 10.0.0.211 (Reachable)
MAC: Roku:d83134-43b1

802.11
Channels: 1
Type: 802.11n

Last Seen: 9:21:36 AM

Addresses
BSSID: 1 IPv4: 1 MAC: 1

Floating action menus that appear in the testing applications are described more specifically in the relevant chapters. For example, see Discovery App Floating Action Menu in the Discovery app chapter for a more detailed illustration.

Common Tools

Web Browser/Chrome

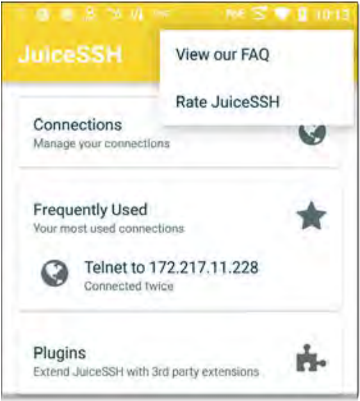
Some of the testing apps, like AutoTest, Ping/TCP, and Discovery, give you the option to **Browse** to internet addresses using a web browser application. EtherScope has Google Chrome pre-installed.

Telnet/SSH

Starting with v1.1, EtherScope 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, touch the action overflow button ⋮ at the top right of the JuiceSSH app screen, and select **View our FAQ**.



JuiceSSH

View our FAQ

Rate JuiceSSH

Connections
Manage your connections

Frequently Used
Your most used connections

Telnet to 172.217.11.228
Connected twice

Plugins
Extend JuiceSSH with 3rd party extensions

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 or Wireless 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.

Back to Title and Contents

Software Management

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

Tap a link below to skip to your desired topic:

Managing Files

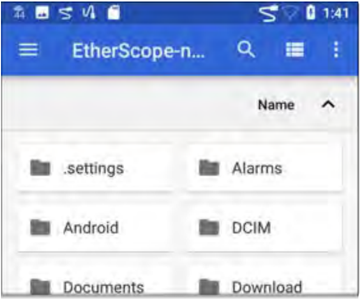
In EtherScope nXG's Android operating system, images, documents, and other files reside in a folder system, where you can copy, move, and paste them between folders or to external storage locations.

See also Navigating EtherScope nXG.

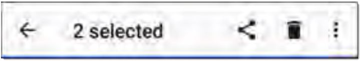
Files Application

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

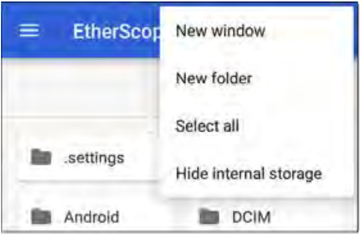
> NOTE: In the Files app, you may need to tap the action overflow icon ⋮ at the top right and select **Show Internal Storage** to navigate to the **EtherScope-nXG** folder and sub-folders, as shown below.



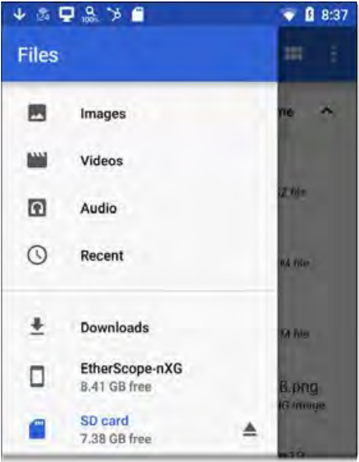
- Tap a folder or file to open it.
- Long press on folders or files to select multiple and to view additional file management operations in the top toolbar, including the Share and Delete buttons.



- 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.

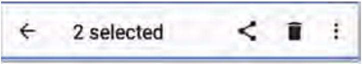


- Open the left-side navigation drawer ☰ to easily navigate through the top-level folders and attached storage devices.

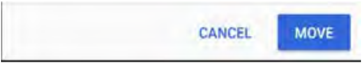


How to Move or Copy a File

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



2. Touch 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.

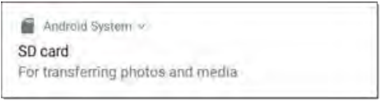


4. Navigate to the folder where you want to move or copy the file.
5. Touch the **Move** or **Copy** button at the bottom of the screen.

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 EtherScope nXG. 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.



Android System

SD card

For transferring photos and media

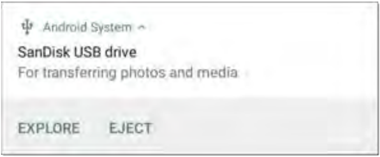
The **SD card** storage location is also available from the Files application.

⚠ **CAUTION:** As with any Android device, use the **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 EtherScope.

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.



Android System

SanDisk USB drive

For transferring photos and media

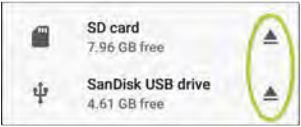
EXPLORE EJECT

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

⚠ **CAUTION:** As with any Android device, use the **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 Android notification (as shown above) in the Notification Panel or from the left-side navigation drawer in the Files app (below).



SD card

7.96 GB free

SanDisk USB drive

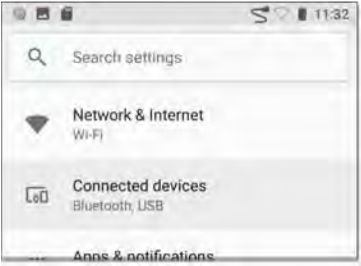
4.61 GB free

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 EtherScope, and connect to a PC or tablet.

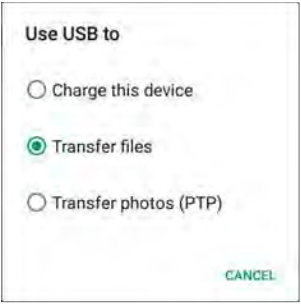
2. On the EtherScope Unit, open the Android device settings by tapping the Settings ⚙ icon at the bottom of the Home screen.

3. Select **Connected devices**.



4. On the Connected devices screen, select **USB**.

5. In the pop-up dialog, touch **Transfer files** to enable file transfer.



Use USB to

○ Charge this device

● Transfer files

○ Transfer photos (PTP)

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

6. On your PC or tablet, navigate to the EtherScope nXG folder if it does not pop up automatically. From there, you can move, copy, and paste files to and from the EtherScope nXG's file system.

⚠ **CAUTION:** As with any Android device, use the **EJECT** function before physically disconnecting the USB cable from your PC or EtherScope to avoid potential corruption of your storage device's file system. See Ejecting Storage Media above.

Back to Title and Contents

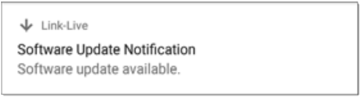
Updating Software

Your EtherScope nXG 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

You must create an account and "claim" your EtherScope nXG unit at Link-Live.com for the EtherScope to find and download software updates. See Getting Started in Link-Live.

The first time you claim your EtherScope nXG 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 select the notification to update your unit.



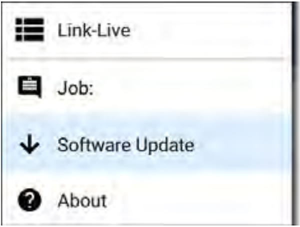
↓ Link-Live

Software Update Notification

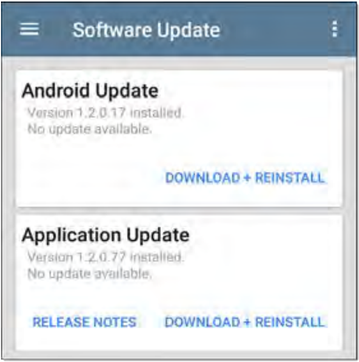
Software update available.

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, touch the menu icon ☰ or swipe right to open the left-side Navigation Drawer.



3. Touch **Software Update**.
The Software Update screen opens and displays the version number of any available updates. You can touch the blue-linked Release Notes to read descriptions of the updated features in the new version.



Android Update
Version 1.2.0.17 installed.
No update available.

Application Update
Version 1.2.0.77 installed.
No update available.

4. If both an Android and an Application Update are available, install the Android update first.

5. Touch **Download + Install** to update the Android operating system or the NetAlly Applications. Each update must be installed separately.

The files download and install. When finished, the unit will restart.

After updating Android, check the Software Update screen again in case an Application Update is still required.

Manual Updates

You can acquire the update files from Link-Live.com or by contacting NetAlly's Technical Support at NetAlly.com/Support.

To download the software update files from the Link-Live.com website, open the left-side navigation drawer by clicking the menu icon ☰, and select **Support > Software Downloads**.

1. Download the update files for the Android system (esnxg_aosp.zip) and Applications (.apk) to a PC or your EtherScope unit.
2. If you are updating both the Android OS and Applications, install the Android update first.

Updating the Android OS

Reference Buttons and Ports if needed.

1. Copy the .zip file to a **Micro SD card** inserted into your EtherScope.
2. Power off your EtherScope unit.
3. Press and hold the volume up button and press the power button to start up the EtherScope in Recovery Mode. Continue holding the volume up button until the Recovery screen appears.
4. In Recovery Mode, use the volume buttons to highlight “**apply update from SD card**,” and 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 press the power button to confirm.

The EtherScope will open the Updater, install the Android update, and then restart with the update installed.

After updating Android, be sure to check the available Applications update version to determine if an Applications update is still required.

Updating the Applications

1. Copy the .apk file to a USB flash drive or a Micro SD card inserted into your EtherScope.
2. In the Link-Live App ▤, open the left-side navigation drawer, and select **Software Update**.
3. On the Software Update screen, touch the action overflow icon ⋮ at the top right, and select **Manual Update**.
4. Navigate to the USB drive or Micro SD card where you saved the update file.
5. Tap the update file to select it.

The EtherScope will open the Updater, install the .apk files for the NetAlly apps, and then restart with the updates installed.

Back to Title and Contents

Remote Access

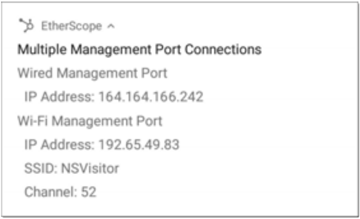
EtherScope supports remote access and control using either a standalone VNC client or the Link-Live Remote feature, which utilizes a VNC client through the Link-Live website.

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

While you can establish remote connections using the Wired or Wi-Fi Test Ports on the EtherScope, the Management Ports provide more stable links for remote control; 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 EtherScope ports. Swipe down from the Status Bar to view them.



EtherScope ^

Multiple Management Port Connections

Wired Management Port

IP Address: 164.164.166.242

Wi-Fi Management Port

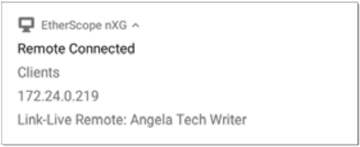
IP Address: 192.65.49.83

SSID: NSVisitor

Channel: 52

- 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.
- For a Wi-Fi Management Port connection, you must have the main Android Wi-Fi settings configured to connect to a wireless network.

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



EtherScope nXG ^

Remote Connected

Clients

172.24.0.219

Link-Live Remote: Angela Tech Writer

Using VNC

Remotely access the EtherScope nXG 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 EtherScope using a VNC client:

1. Get the IP address of a connected port (preferably a management port) by swiping down from the Status Bar at the top of the screen to view the notification panel.
2. Provide the wired or Wi-Fi 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 EtherScope.

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

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

1. If you have AllyCare, sign in to Link-Live.com to access the Link-Live Remote feature. Your EtherScope must be claimed.
2. Navigate to the **Units** 📱 page at Link-Live.com.
3. Select the EtherScope you want to remote control from the list of claimed units.
4. Click or touch the **REMOTE** icon 🖥 at the top right of the page to open an embedded window containing the EtherScope interface.
5. If necessary, at the top of the window, enter the Password set in **General Settings > Management > VNC** on the EtherScope unit.

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

Back to Title and Contents

Managing NetAlly App Settings

This chapter explains the processes for resetting, loading, saving, importing, and exporting the test settings for individual NetAlly testing apps, such as AutoTest, Discovery, and Performance.

For instructions on restoring factory defaults to the entire EtherScope unit, see Restoring EtherScope nXG Factory Defaults.

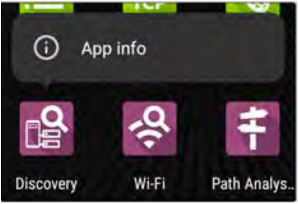
Resetting Testing App Defaults

Once you have adjusted settings in the NetAlly apps, at some point, you may need to reset an app's settings to the defaults. The following process resets all app-specific settings to the factory defaults.

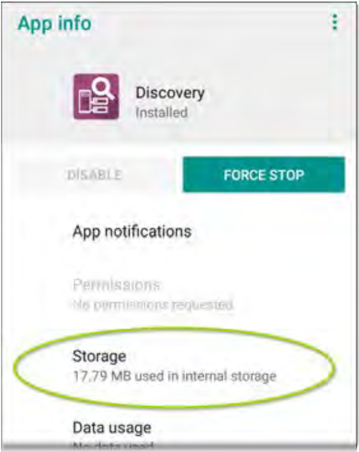
> ⚠ **CAUTION:** This operation will delete all saved settings, including testing profiles and other application data.

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 a app's icon on the Home or Apps screen.



2. Touch **App info**.



App info

Discovery
Installed

App notifications

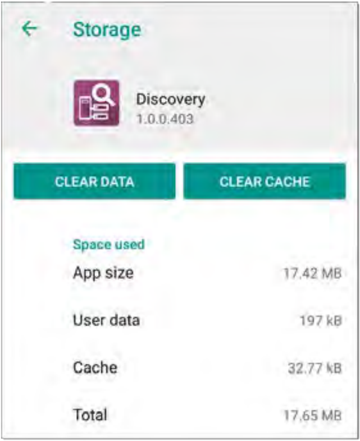
Permissions
No permissions requested

Storage
17.79 MB used in internal storage

Data usage
No data used

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, touch **CLEAR DATA**.



Storage

Discovery
1.0.0.403

Space used

App size	17.42 MB
User data	197 kB
Cache	32.77 kB
Total	17.65 MB

5. When the "Delete app data?" dialog appears, tap **OK**.

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

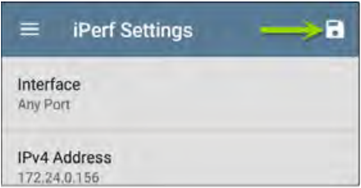
Saving App Settings Configurations

Many of the NetAlly testing applications allow you to save and load a configuration of 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 Settings, including Profile Groups
- Discovery Settings
- Discovery > Problem Settings
- Performance Settings
- iPerf Settings

The iPerf app is shown below as an example.

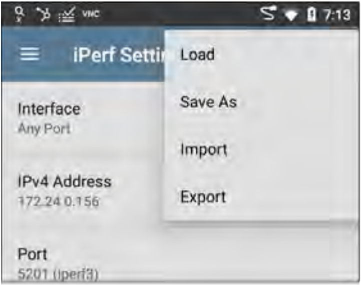


iPerf Settings

Interface
Any Port

IPv4 Address
172.24.0.156

The following options display in a drop-down menu:

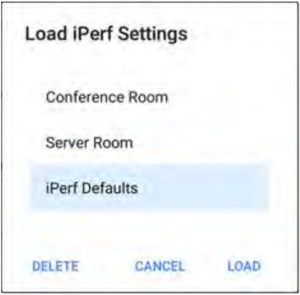


Interface
Any Port

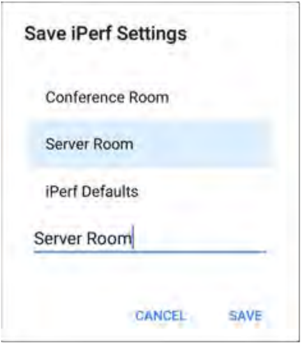
IPv4 Address
172.24.0.156

Port
5201 (iperf3)

- **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

- **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 (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.

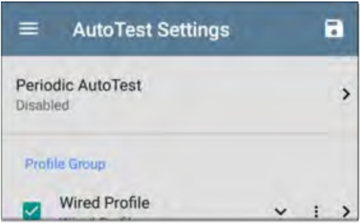
Exporting and Importing Settings

EtherScope nXG provides functionality for exporting and importing saved test app settings for transfer to additional units.

The following apps enable you to import and export settings 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.



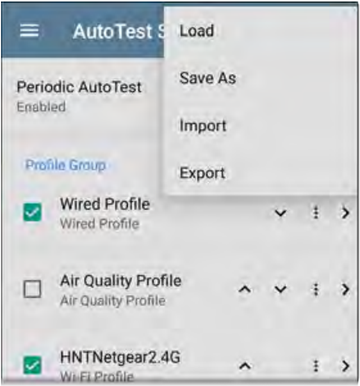
AutoTest Settings

Periodic AutoTest
Disabled

Profile Group

☑ Wired Profile

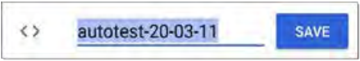
- Touch the save button 💾 to import new app settings or export the *currently active and selected* app settings.



- Unselected (unchecked) items in shared lists of configurations *are not exported*.

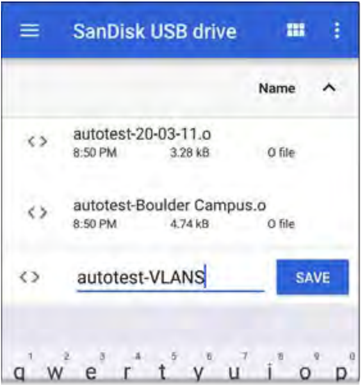
  For example, in the AutoTest Settings image above, the "Air Quality Profile" will not be exported. Likewise, any unchecked items in submenus, like AutoTest's Test Targets or Community Strings in Discovery Settings, will not be exported.

- Unsaved configurations without a custom name are auto-named with the app name and date:



autotest-20-03-11

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



SanDisk USB drive

autotest-20-03-11.o
8:50 PM 3.28 kB 0 file

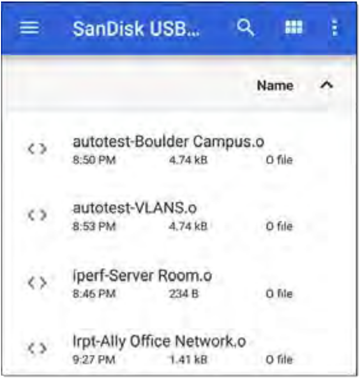
autotest-Boulder Campus.o
8:50 PM 4.74 kB 0 file

autotest-VLANS

- 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.



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

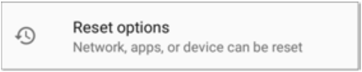
lrpt-Ally Office Network.o
9:27 PM 1.41 kB 0 file

- 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 will overwrite existing saved configurations with the same name that are already in the app.

Restoring EtherScope nXG Factory Defaults

⚠ **CAUTION:** Depending on the reset option you select, this operation can delete all test results, user-installed applications, testing app settings, and saved files, and reset device settings to the factory default state. Make sure to back up any files you desire to keep.

1. To access the Android Device Settings, touch the Settings ⚙ icon at the bottom of the Home Screen.
2. On the Settings screen, scroll down and tap the **System** section.
3. On the System screen, touch **Reset options**.



Reset options
Network, apps, or device can be reset

4. On the Reset options screen, select an option based on which defaults you want restored. Whichever option you choose,

EtherScope displays a list of the items that will be reset based on the option.

5. Touch **RESET** to initiate your chosen reset type.
6. The unit may ask you to confirm a final time before resetting. Touch the final confirmation button to reset your EtherScope's defaults.

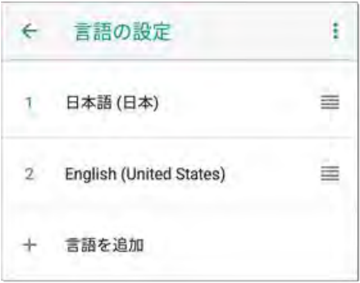
The device restarts with factory default settings.

Changing the Language

NOTE: The EtherScope nXG supports **Japanese** beginning with version 1.1.

1. To change the interface language, go to Device Settings by touching the Settings ⚙ icon at the bottom of the Home screen.
2. On the Settings screen, scroll down and select the **System** section, and then, **Languages & input**.
3. On the Languages & input screen, touch **Languages**.
4. On the Language preferences screen, select **+ Add a language**.
5. Touch to select the name of your desired language option.
6. On the Language preferences screen, touch the icon to the right of the language, and drag your desired language option to the

top (1) spot on the list.



言語の設定

1 日本語 (日本)

2 English (United States)

＋ 言語を追加

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

EtherScope nXG 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 EtherScope nXG. It allows you to 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 and Wi-Fi network connections, wireless Air Quality, and individual Test Targets.

AutoTest establishes the Wired and Wi-Fi Test Port connections used by other testing apps, like Ping/TCP, Capture, and Performance.

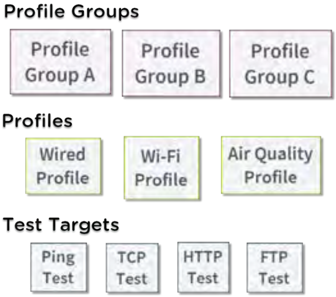
AutoTest results are automatically uploaded to Link-Live Cloud Service once you have claimed your EtherScope.

AutoTest Chapter Contents

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

AutoTest Overview

AutoTest consists of three distinct testing levels: **Test Targets**, **Profiles**, and **Profile Groups**.



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 are three different Profile types: Wired, Wi-Fi, and Air Quality. The Wired and Wi-Fi Profiles include connection tests and credentials for a Wi-Fi network or Wired VLAN. Air Quality is a passive scan of your wireless environment. 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**.

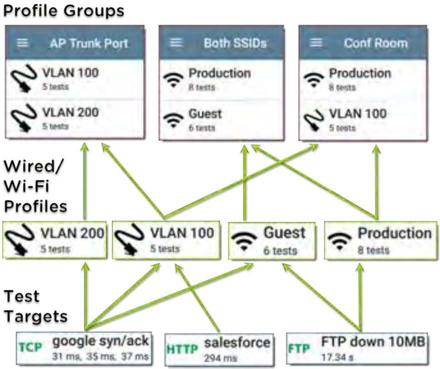
A **Profile Group** is a custom-named collection of Profiles. Profile Groups are designed to allow further automation for testing multiple networks or network elements with a single tap of the START button.

Here are some examples of useful Profile Grouping schemes:

- Testing multiple Wired VLANs on a trunk port.

- Testing multiple Wi-Fi SSIDs from a single location.
- Testing both wired and Wi-Fi access from a conference room.

The graphic below illustrates each of these scenarios. Note how Test Targets can be included in any number of Profiles, and Profiles can be included in any number of Profile Groups.



You can create as many Profile Groups, Profiles, and Test Targets as you want.

Back to Title and Contents

Managing Profiles and Profile Groups

Profiles are a series, or suite, of tests designed to analyze the different characteristics of your networks. The EtherScope nXG AutoTest app features three types of test profiles:

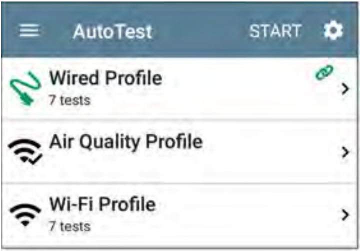
Wired Profiles test copper and fiber connections.

Wi-Fi Profiles test wireless connections.

Air Quality Profiles measure channel utilization and interference.

Factory Default Profiles

The EtherScope begins with a default version of the three AutoTest profile types—Wired, Air Quality, and Wi-Fi—which you can customize, delete, or replace for your purposes.



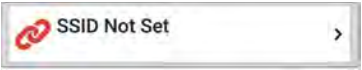
To customize each Profile with the required network settings and a custom name, touch the Profile name *first*, and then select the settings ⚙ icon.

NOTE: Touching 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 touch START in AutoTest to run a Wired Profile on a fiber connection.

- The default **Air Quality Profile** runs when you touch **START** on the main AutoTest screen or the Air Quality screen.
- For the default **Wi-Fi Profile** to run successfully, you must select an SSID and enter security credentials before the EtherScope can connect to a network.

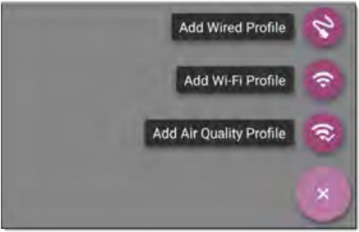


SSID Not Set

See Wi-Fi Profile Connection Settings.

Adding New Profiles

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



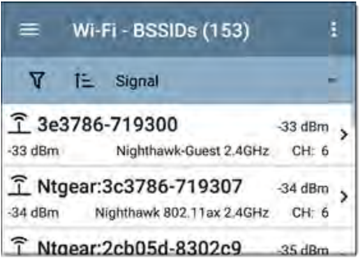
The profile's configuration screen appears after you select the type of profile you want to add. See the topic for each profile type for a description of its settings.

Once you have configured the profile's settings, tap the back button ◁ at the bottom of the screen to open and run the new test profile.

Creating a Wi-Fi Profile from the Wi-Fi Analysis App

You can also create an AutoTest Wi-Fi Profile from the Wi-Fi Analysis app's SSID or BSSID Details screen. This is a quick and easy way to add a Profile to connect to a Wi-Fi network in your vicinity.

1. Open the Wi-Fi app from the Home screen.
2. Tap the menu button ☰ to select the **SSIDs** or **BSSIDs** list screen.



Wi-Fi - BSSIDs (153)

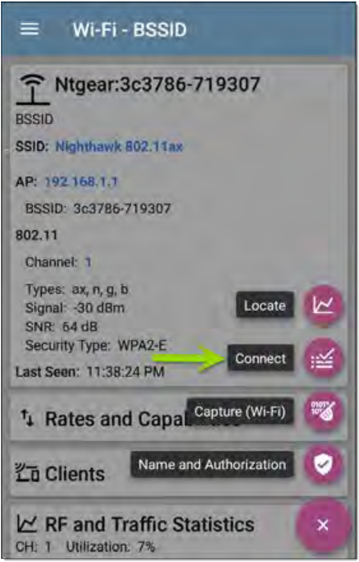
Signal

3e3786-719300 -33 dBm
-33 dBm Nighthawk-Guest 2.4GHz CH: 6

Ntgear:3c3786-719307 -34 dBm
-34 dBm Nighthawk 802.11ax 2.4GHz CH: 6

Ntgear:2cb05d-8302c9 -35 dBm

3. Touch an SSID or BSSID's card to open its Details screen.
4. Touch the FAB (floating action button) to open the floating action menu.



Wi-Fi - BSSID

Ntgear:3c3786-719307

BSSID

SSID: Nighthawk 802.11ax

AP: 192.168.1.1

BSSID: 3c3786-719307

802.11

Channel: 1

Types: ax, n, g, b
Signal: -30 dBm
SNR: 64 dB
Security Type: WPA2-E

Last Seen: 11:38:24 PM

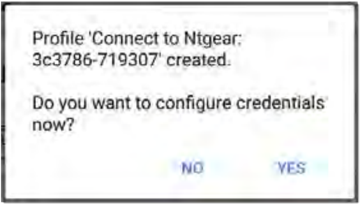
Rates and Capa

Clients

RF and Traffic Statistics
CH: 1 Utilization: 7%

5. In the floating action menu, touch **Connect**.

   A Wi-Fi Profile called "Connect to [SSID/BSSID]" is created in AutoTest.

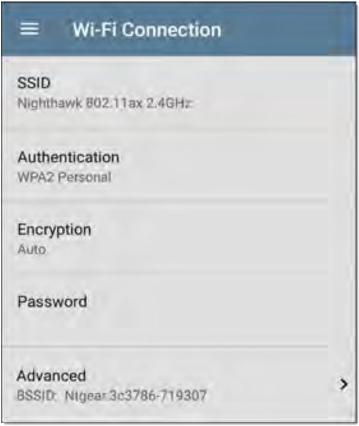


Profile 'Connect to Ntgear: 3c3786-719307' created.

Do you want to configure credentials now?

The SSID, BSSID (if applicable), and Authentication Type are auto-populated in the Wi-Fi Connection settings for the new profile.

6. Tap **YES** in the pop-up dialog to review and configure additional credentials.



Wi-Fi Connection

SSID
Nighthawk 802.11ax 2.4GHz

Authentication
WPA2 Personal

Encryption
Auto

Password

Advanced
BSSID: Ntgear 3c3786-719307

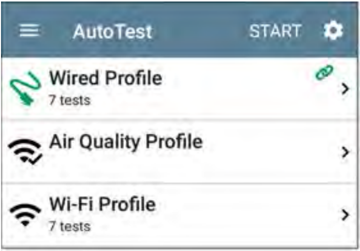
7. Enter any additional credentials, like the network Password.

8. After configuring, touch the back button ◁ to return to and run the new Profile.

Profile Groups

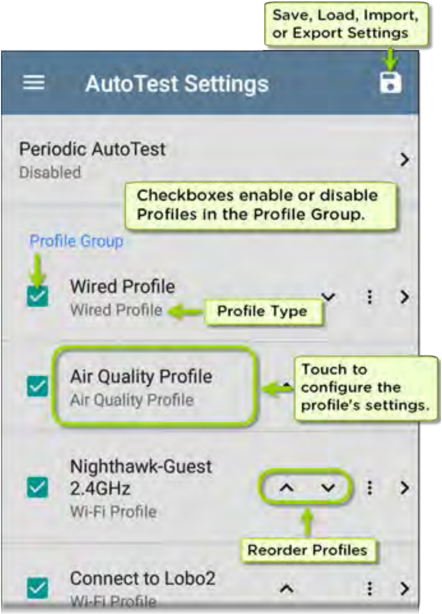
EtherScope nXG also allows you to save Profile Groups. Profile Groups are simply **the included list of test Profiles and the order in which they run** when you start an AutoTest. (See AutoTest Overview for more explanation of Profile Groups.) You can configure and select Profiles and Profile Groups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

To manage your Profiles and Profile Groups, touch 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.
- Touch 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.
- Touch any Profile's name to open the test and connection settings for the Profile.
- Touch 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.

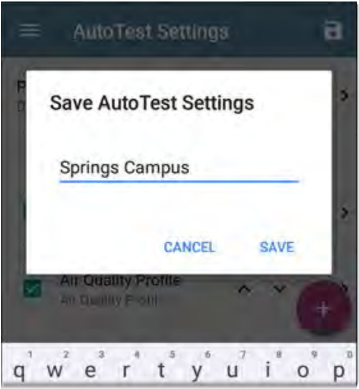
  See Exporting and Importing App Settings for more details.

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.

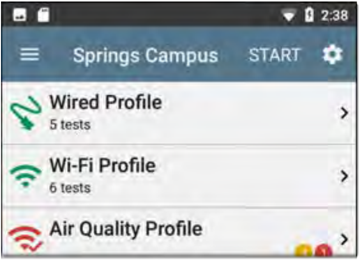
In the example below, the user saves a custom AutoTest configuration named "Springs Campus."



Save AutoTest Settings

Springs Campus

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



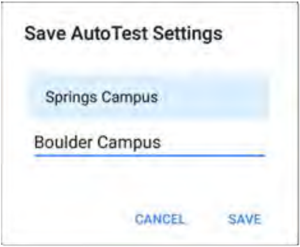
Creating New Profile Groups

To create a new Profile Group, follow these steps:

1. Go to the AutoTest Settings and Profile Group screen by touching ⚙ on the main AutoTest screen.
2. Uncheck the boxes for any Profiles you do not want included in the new Profile Group.
3. Touch 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 will run. Unchecked profiles will 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.

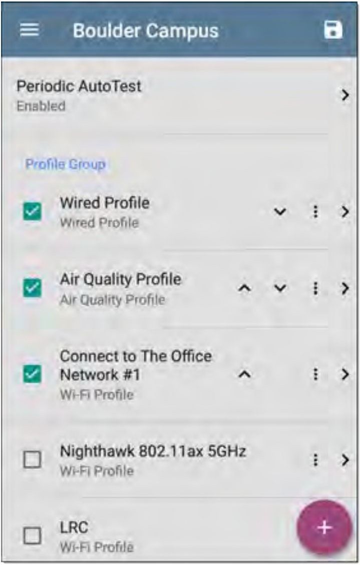


Save AutoTest Settings

Springs Campus

Boulder Campus

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



Boulder Campus

Periodic AutoTest
Enabled

Profile Group

☑ Wired Profile
Wired Profile

☑ Air Quality Profile
Air Quality Profile

☑ Connect to The Office Network #1
Wi-Fi Profile

□ Nighthawk 802.11ax 5GHz
Wi-Fi Profile

□ LRC
Wi-Fi Profile

When running the "Boulder Campus" configuration shown above, AutoTest will first run the Wired Profile over the Ethernet connection, next scan the wireless channels for Air Quality results, and then connect to "The Office

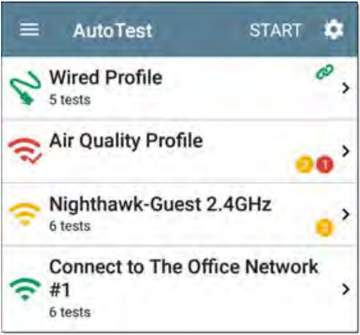
Network #1" and remain connected to that network. This Profile Group will *not* connect to or test the "Nighthawk..." or "LRC" networks.

Back to Title and Contents

Main AutoTest Screen

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

Touch 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: ②① (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. Touch a profile's or individual test's card to open and view test result details, including the causes of any Warnings or Failures.

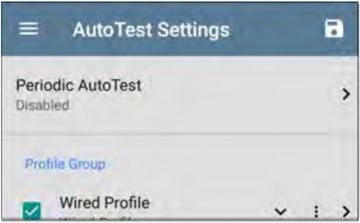
Back to Title and Contents

Periodic AutoTest

The Periodic AutoTest feature allows you to repeatedly run AutoTests for a specified amount of time.

Periodic AutoTest Settings

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



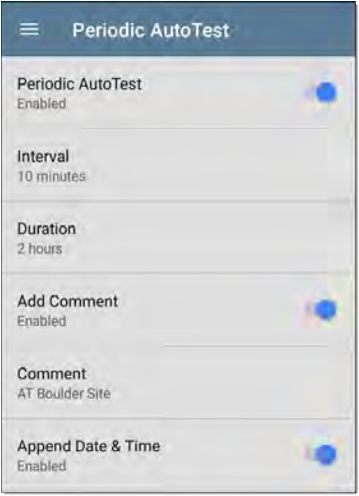
AutoTest Settings

Periodic AutoTest
Disabled

Profile Group

☑ Wired Profile

The Periodic AutoTest settings screen displays.



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

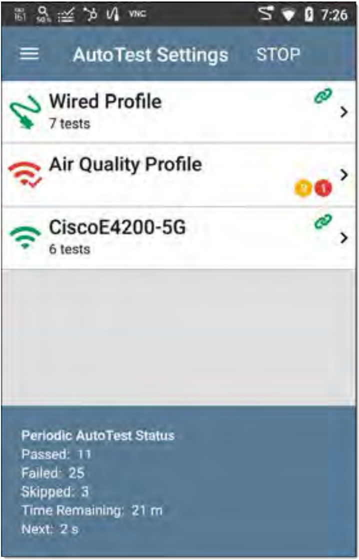
Add Comment: Enabling this setting allows you to attach a comment to the Periodic AutoTest result in Link-Live Cloud Service. The comment will appear as a label on the Link-Live.com Results page. This setting and the **Comment** setting below are enabled by default.

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

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

Running Periodic AutoTest

Touch **START** on the main AutoTest screen to begin Periodic AutoTests. AutoTests will continue to run at the set Interval for the selected Duration or until you touch **STOP** in AutoTest.



Wired Profile
7 tests

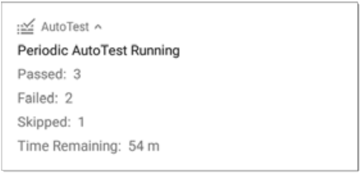
Air Quality Profile

CiscoE4200-5G
6 tests

Periodic AutoTest Status
Passed: 11
Failed: 25
Skipped: 3
Time Remaining: 21 m
Next: 2 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

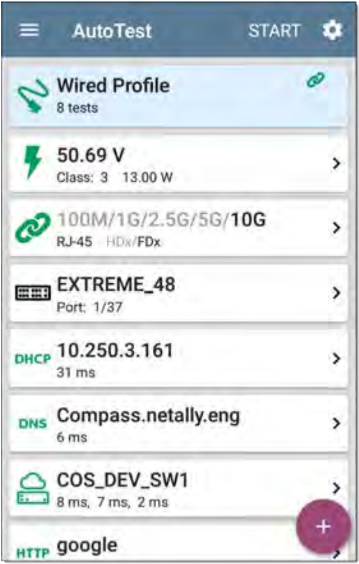
Skipped: 1

Time Remaining: 54 m

> NOTE: AutoTest has priority control of the Test Ports, so other apps, including Discovery, Wi-Fi, Wi-Fi Capture (but not Wired Capture), and AirMapper, are paused while AutoTest completes.

Wired AutoTest Profiles

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



Wired Profile
8 tests

50.69 V
Class: 3 13.00 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

Like the main AutoTest screen, Wired Profile tests are summarized on cards. Touch 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

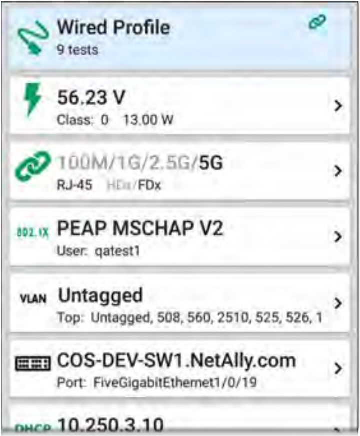
The last enabled Wired Profile in the currently active Profile Group runs automatically when a copper cable is connected or energy is detected to the top RJ-45 port, unless the AutoTest app is open in the foreground and there is more than one enabled Wired Profile. A Wired Profile does not start automatically 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 tests that are specific to a Wired Profile include the following:

- PoE
- Wired Link
- 802.1X
- VLAN
- Switch



Wired Profile
9 tests

56.23 V
Class: 0 13.00 W

100M/1G/2.5G/5G
RJ-45 HDx/FDx

802.1X PEAP MSCHAP V2
User: qatest1

VLAN Untagged
Top: Untagged, 508, 560, 2510, 525, 526, 1

COS-DEV-SW1.NetAlly.com
Port: FiveGigabitEthernet1/0/19

DHCP 10.250.3.10

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

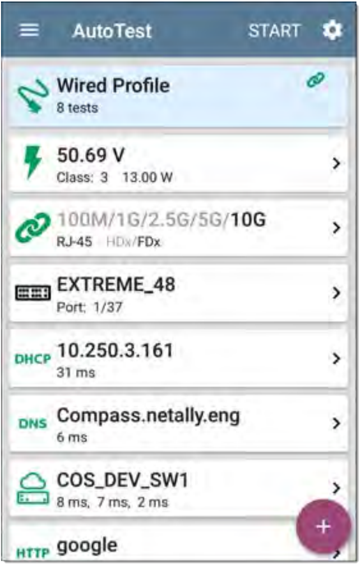
The VLAN test card appears if the **VLAN** setting is enabled or if VLAN-tagged traffic is detected during the AutoTest.

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.



Wired Profile
8 tests

50.69 V
Class: 3 13.00 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

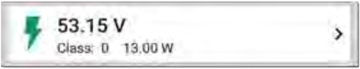
On the Wired Profile screens, you can perform these actions:

- Touch 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, touch **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.
- Touch 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



53.15 V

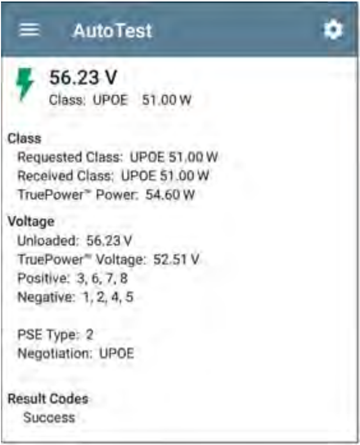
Class: 0 13.00 W

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

Refer to PoE Settings if needed.

Touch the card to open the PoE results screen.

PoE Test Results Screen



56.23 V
Class: UPOE 51.00 W

Class
Requested Class: UPOE 51.00 W
Received Class: UPOE 51.00 W
TruePower™ Power: 54.60 W

Voltage
Unloaded: 56.23 V
TruePower™ Voltage: 52.51 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

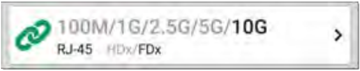
PSE Type: Switch's advertised Power Sourcing Equipment (PSE) type. Recognized types are 1 – 4, LTPoE++, Cisco UPOE, and PoE Injectors. PSE supporting UPOE are classified under Type 2. If the type cannot be determined, "1/2" is displayed.

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.

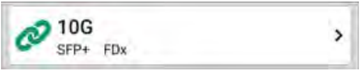


100M/1G/2.5G/5G/**10G**

RJ-45 HDx/**FDx**

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**.

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



10G

SFP+ FDx

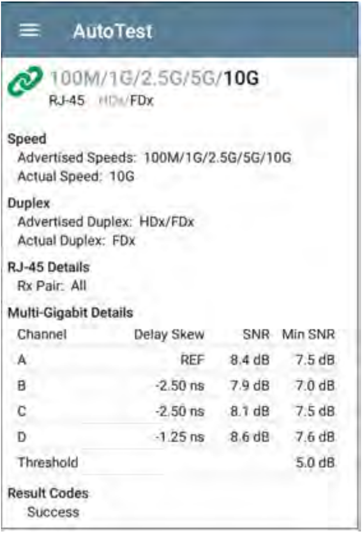
For a Fiber connection, the Link test card shows the connection speed and duplex.

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

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

Touch the card to open the Link test screen.

Wired Link Test Screen



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

RJ-45 HDx/FDx

Speed

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

Actual Speed: 10G

Duplex

Advertised Duplex: HDx/FDx

Actual Duplex: FDx

RJ-45 Details

Rx Pair: All

Multi-Gigabit Details

Channel	Delay Skew	SNR	Min SNR
A	REF	8.4 dB	7.5 dB
B	-2.50 ns	7.9 dB	7.0 dB
C	-2.50 ns	8.1 dB	7.5 dB
D	-1.25 ns	8.6 dB	7.6 dB
Threshold			5.0 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 EtherScope nXG

Duplex

Advertised Duplex: Duplex capabilities reported by the switch

Actual Duplex: Duplex in use as detected by EtherScope

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

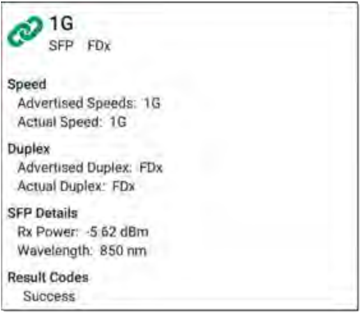
Delay Skew: Difference in propagation delay between sets of wired pairs. Channel A acts as the reference for the other channel measurements.

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

Min SNR: Lowest 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

Rx Power: -5.62 dBm

Wavelength: 850 nm

Result Codes

Success

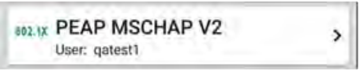
Rx Power: Link receive power

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

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.

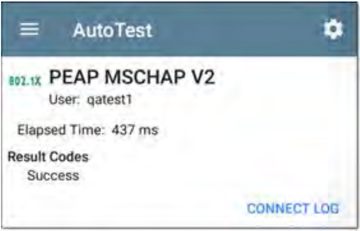


802.1X PEAP MSCHAP V2

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



PEAP MSCHAP V2

User: qatest1

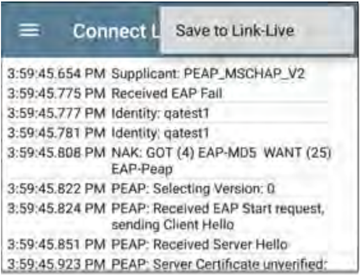
Elapsed Time: 437 ms

Result Codes

Success

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.

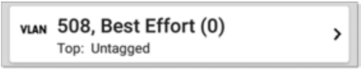


```
3:59:45.654 PM Supplicant: PEAP_MSCHAP_V2
3:59:45.775 PM Received EAP Fail
3:59:45.777 PM Identity: qatest1
3:59:45.781 PM Identity: qatest1
3:59:45.808 PM NAK: GOT (4) EAP-MD5  WANT (25)
               EAP-Peap
3:59:45.822 PM PEAP: Selecting Version: 0
3:59:45.824 PM PEAP: Received EAP Start request,
               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

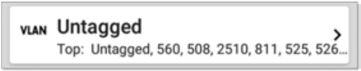
The VLAN card only displays if the VLAN setting is enabled in the Wired Profile Settings or if AutoTest detects VLAN-tagged traffic.



VLAN 508, Best Effort (0)

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.



VLAN Untagged

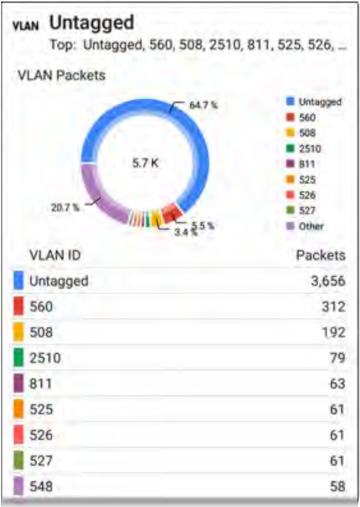
Top: Untagged, 560, 508, 2510, 811, 525, 526...

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.

Touch the card to open the full VLAN screen.

VLAN Test Screen



VLAN Untagged

Top: Untagged, 560, 508, 2510, 811, 525, 526, ...

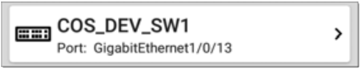
VLAN Packets

VLAN ID	Packets
🟦 Untagged	3,656
🟥 560	312
🟨 508	192
🟩 2510	79
🟪 811	63
🟧 525	61
🟥 526	61
🟩 527	61
🟪 548	58

The VLAN test screen displays the real-time traffic the EtherScope 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

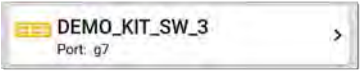
The results available for the Switch Test are based on Discovery Protocol advertisements and SNMP system group information. SNMP forwarding table data is used to determine the Nearest Switch. See Discovery Settings for SNMP configuration instructions.


COS_DEV_SW1

Port: GigabitEthernet1/0/13

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

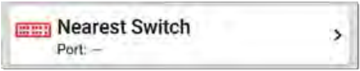
- If the EtherScope does not detect any network traffic moving through the switch after 45 seconds, the switch icon turns yellow.



DEMO_KIT_SW_3

Port: g7

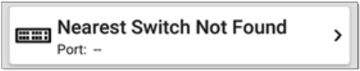
- If the connection is lost while the Wired Autotest is running, the switch icon turns red.



Nearest Switch

Port: --

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



Nearest Switch Not Found

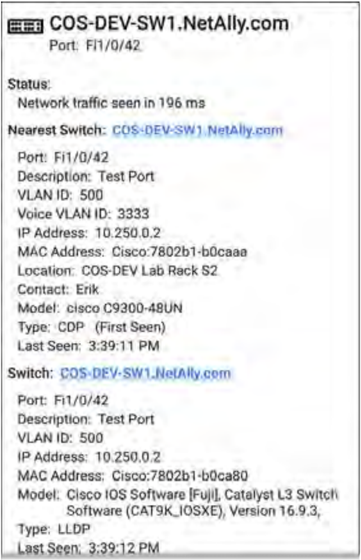
Port: --

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

Touch 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

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

Nearest Switch: Name of the switch determined to be closest to the EtherScope

> **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 EtherScope has SNMP access to the Nearest Switch.

Contact: Configured contact person reported by the switch. This field only appears if the EtherScope has SNMP access to the Nearest Switch.

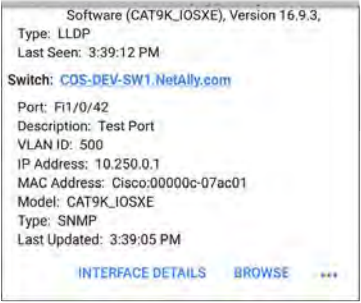
Model: Switch model name and/or number

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

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

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.



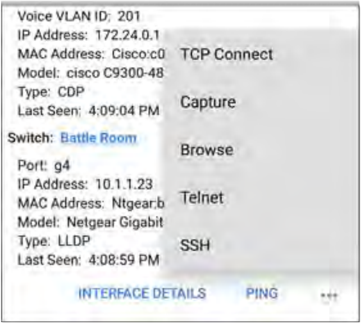
Software (CAT9K_IOSXE), Version 16.9.3,
Type: LLDP
Last Seen: 3:39:12 PM

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

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

At the bottom of the switch test screen, touch 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

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 EtherScope 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 Google Chrome, and **Telnet** or **SSH** open the JuiceSSH app.

DHCP, DNS, and Gateway Results

Results for these tests operate the same in both Wired and Wi-Fi profiles.

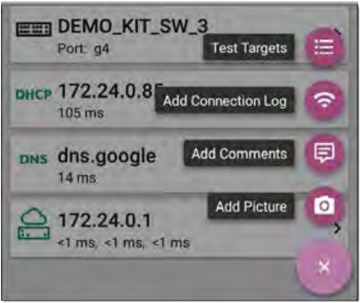
See DHCP, DNS, and Gateway Tests for Wired and Wi-Fi.

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 Connection Log to this AutoTest result on the Link-Live website.



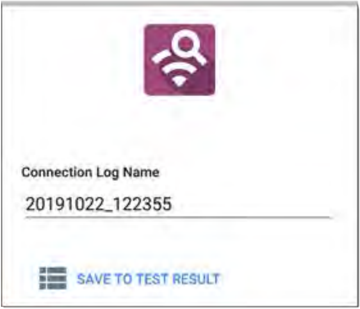
DEMO_KIT_SW_3
Port: g4

DHCP 172.24.0.8
105 ms

DNS dns.google
14 ms

172.24.0.1
<1 ms, <1 ms, <1 ms

- 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.

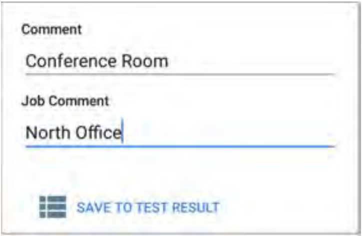


Connection Log Name

20191022_122355

Touch 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

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

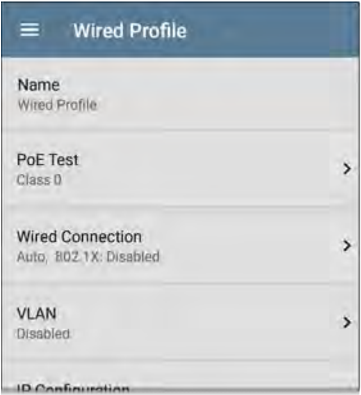
- The **Add Picture** function lets you open the **Gallery** or **Camera** app to select or take a photo that is then uploaded and attached to your test result.

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.

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



Wired Profile

Name
Wired Profile

PoE Test
Class 0

Wired Connection
Auto, 802.1X: Disabled

VLAN
Disabled

IP Configuration

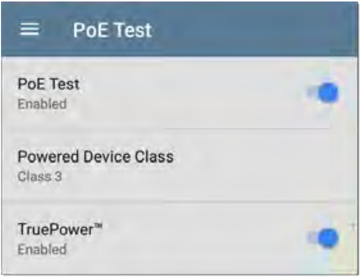
On the **Wired Profile** settings screen, touch each field described below as needed to configure the profile. Changed settings are automatically applied. When you finish configuring, tap the back button ◁ to return to the profile.

Name

Touch 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
Enabled

Powered Device Class
Class 3

TruePower™
Enabled

PoE Test

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

Powered Device Class

Touch to select a PoE class setting to match your switch's (or PoE injector's) available class. EtherScope 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 the **PoE Injector** option if you are using a non-IEEE injector.

> NOTE: EtherScope may not receive the total wattage advertised by your switch or injector because of power loss over the cable.
>
> NOTE: EtherScope automatically negotiates Cisco UPOE over LLDP, up to 51 W. LLDP must be enabled on the switch for

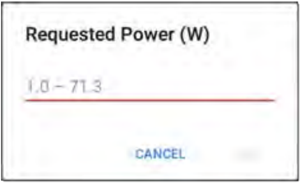
negotiation to succeed. If the UPOE Class is selected on your EtherScope but LLDP is not enabled on your Cisco switch, negotiation will fail.

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 will fail.

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 **PoE Injector** and **TruePower** is enabled. Touch to enter a Requested Power other than the default, if needed. If you touch 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.

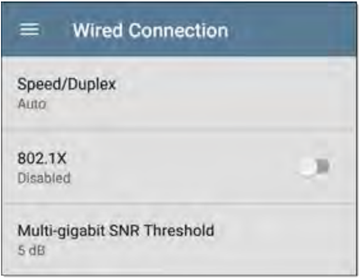
General Settings that Affect PoE

See the Wired section in General Settings for descriptions of the **Test PoE before Link** and **Charge Battery via PoE** settings, which also affect the PoE Test and function.

See also PoE Charging.

Wired Connection Settings

Open **Wired Connection** settings to configure speed and duplex.



Wired Connection

Speed/Duplex
Auto

802.1X
Disabled

Multi-gigabit SNR Threshold
5 dB

Speed/Duplex

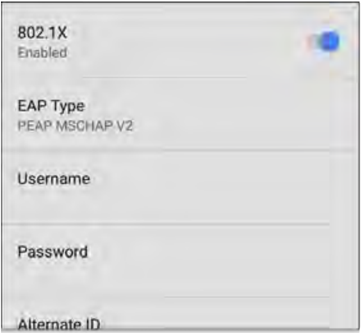
Touch to select the speed and duplex option that you want to test your network against. The default is Auto negotiation.

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

802.1X

Touch 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

EAP Type
PEAP MSCHAP V2

Username

Password

Alternate ID

EAP Type

Touch 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. Touch the **Username** field to enter your username.

Password

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

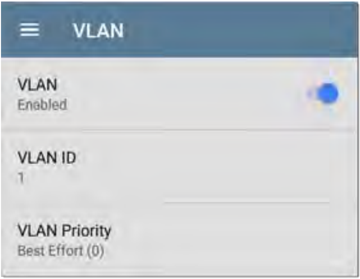
Alternate ID

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 will display a yellow warning condition. The default is 5 dB.

VLAN Settings

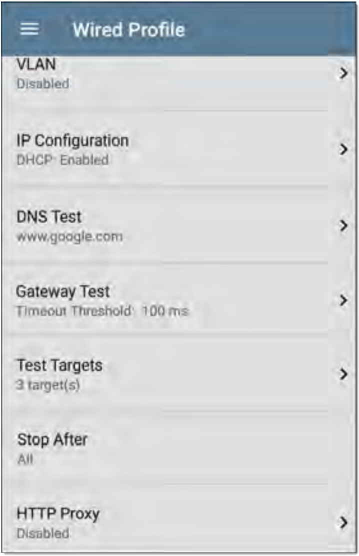


VLAN
Enabled

VLAN ID
1

VLAN Priority
Best Effort (0)

Touch 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. Touch these fields to open a pop-up number pad and enter the correct ID and priority. Touch **OK** to save them.



VLAN
Disabled

IP Configuration
DHCP: Enabled

DNS Test
www.google.com

Gateway Test
Timeout Threshold: 100 ms

Test Targets
3 target(s)

Stop After
All

HTTP Proxy
Disabled

DHCP, DNS, and Gateway Settings

Settings for these tests operate the same in both Wired and Wi-Fi profiles.

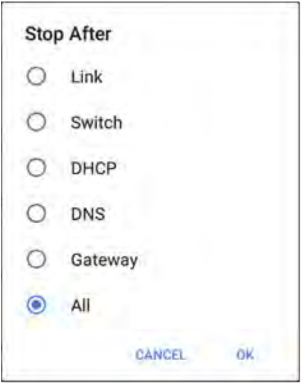
See DHCP, DNS, and Gateway Tests for Wired and Wi-Fi.

Test Targets

Touch 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 and Wi-Fi Profiles.

Stop After



Stop After

○ Link

○ Switch

○ DHCP

○ DNS

○ Gateway

● All

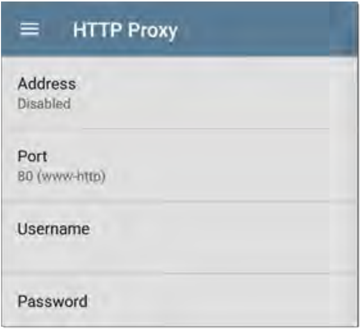
This setting directs the Wired Profile to stop testing after the selected test step. The excluded test cards will not appear on the Profile results screen.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the EtherScope 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.



Address
Disabled

Port
80 (www-http)

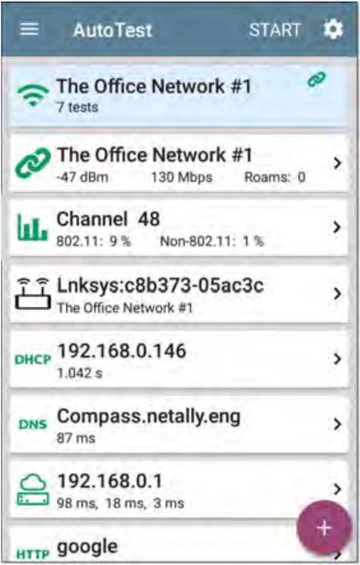
Username

Password

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

Wi-Fi AutoTest Profiles

A Wi-Fi Profile runs a series of tests by connecting to a selected wireless network.



The Office Network #1
7 tests

The Office Network #1
-47 dBm 130 Mbps Roams: 0

Channel 48
802.11: 9 % Non-802.11: 1 %

Lnksys:c8b373-05ac3c
The Office Network #1

DHCP 192.168.0.146
1.042 s

DNS Compass.netally.eng
87 ms

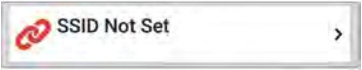
192.168.0.1
98 ms, 18 ms, 3 ms

HTTP google

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

Each test icon (except the AP) displays green, yellow, or red to indicate the status (or grade) of the completed test step: **Success**/**Warning**/**Fail**. The AP Test card shows the name and SSID of the connected AP. The AP test is not graded, so the icon stays black.

Wi-Fi Profiles do not run automatically. Unlike the Wired Profile, the factory default Wi-Fi Profile cannot run until you have configured an SSID with the proper credentials.



SSID Not Set

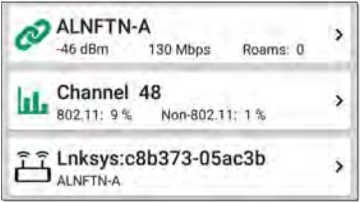
See the Wi-Fi Profile Settings topic for instructions.

After connecting to a network during a Wi-Fi connection test, EtherScope nXG remains connected until you run another Wi-Fi or Air Quality Profile or open the Wi-Fi app. Wi-Fi Test Port linkage is indicated in the top Status Bar with this notification icon, 48, which also shows the connected channel.

> NOTE: When running an AutoTest Profile that connects to a network with a Captive Portal, an Android notification icon ? appears in the top Status Bar. Open and select the notification to open a web browser window where you can enter the required information for the captive portal.

Wi-Fi-Profile-Specific AutoTests

The tests that are specific to a Wi-Fi Profile include the wireless Link, Channel, and AP tests.



ALNFTN-A
-46 dBm 130 Mbps Roams: 0

Channel 48
802.11: 9 % Non-802.11: 1 %

Lnksys:c8b373-05ac3b
ALNFTN-A

The link and channel cards update in real time to display the connection measurements for as long as EtherScope remains connected to the wireless network.

Link (Connection), Channel, and AP Results are described next.

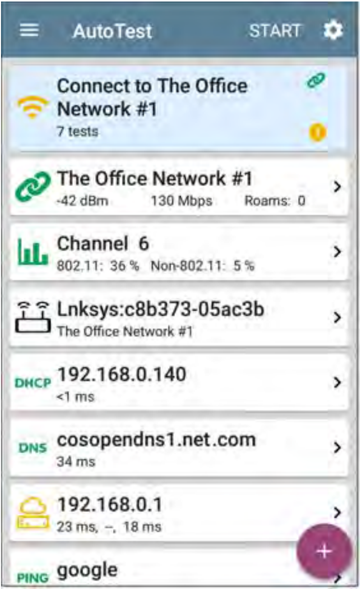
Skip to Wi-Fi Profile Settings.

Skip to DHCP, DNS, and Gateway Tests.

Skip to Test Targets.

Wi-Fi Profile Test Results

The image below shows a completed AutoTest Wi-Fi Profile.



Connect to The Office Network #1
7 tests

The Office Network #1
-42 dBm 130 Mbps Roams: 0

Channel 6
802.11: 36 % Non-802.11: 5 %

Lnksys:c8b373-05ac3b
The Office Network #1

DHCP 192.168.0.140
<1 ms

DNS cosopendns1.net.com
34 ms

192.168.0.1
23 ms, --, 18 ms

PING google

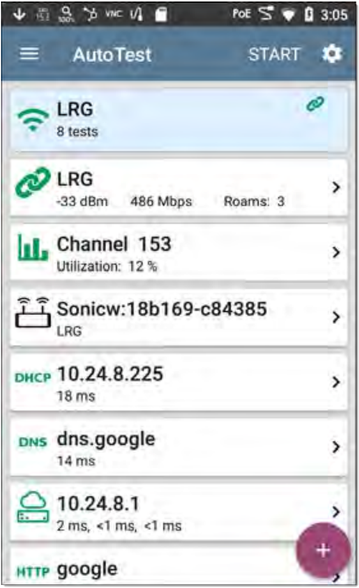
This Profile connects to SSID "The Office Network #1." The Profile is displaying one **Warning** condition from a timeout of the second Gateway ping.

On the Wi-Fi Profile screens, you can perform these actions:

- Touch any of the test result cards, like 🔗 Link , 📊 Channel, or 📡 AP, 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 individual test screens, touch **blue underlined links** to open a Wi-Fi app Details screen showing the selected device or ID.
- Touch other **BLUE LINKS** or the action overflow icon ••• at the bottom of test results screens for additional actions.

  NOTE: Blue links and action icons do not appear on every test screen, and if the network connection is dropped, you may need to rerun the Profile to re-establish link and enable additional actions.

The rest of this topic describes the individual test cards and screens using the Wi-Fi Profile results for the "LRG" SSID shown below.



LRG
8 tests

LRG
-33 dBm 486 Mbps Roams: 3

Channel 153
Utilization: 12 %

Sonicw:18b169-c84385
LRG

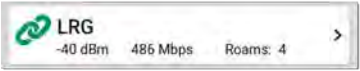
DHCP 10.24.8.225
18 ms

DNS dns.google
14 ms

10.24.8.1
2 ms, <1 ms, <1 ms

HTTP google

Wi-Fi Link Test Results



LRG

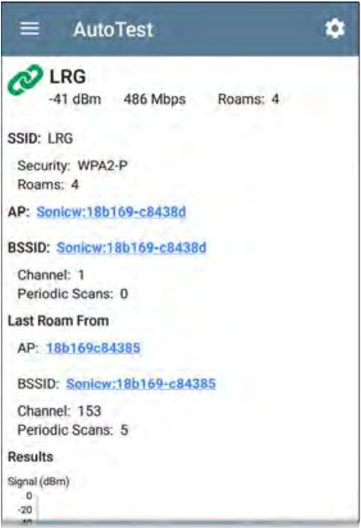
-40 dBm 486 Mbps Roams: 4

The Wi-Fi link test card indicates whether you can connect to the configured network at your current location. The Wi-Fi Link card displays the SSID, current signal strength (dBm), link speed (Mbps), and number of roams.

Refer to Wi-Fi Connection Settings if needed.

Touch the card to open the Link test screen.

Wi-Fi Link Test Screen



LRG
-41 dBm 486 Mbps Roams: 4

SSID: LRG

Security: WPA2-P
Roams: 4

AP: Sonicw:18b169-c8438d

BSSID: Sonicw:18b169-c8438d

Channel: 1
Periodic Scans: 0

Last Roam From

AP: 18b169c84385

BSSID: Sonicw:18b169-c84385

Channel: 153
Periodic Scans: 5

Results

The Wi-Fi Link test screen shows these results:

SSID

Security: Security protocol in use on the network

Roams: Number of times the unit has disconnected from the previous AP and connected to a different AP with a better signal strength. This behavior is partly controlled by the **Roam Threshold** in the Wi-Fi Connection settings.

AP: Name, IP, or MAC address of the AP to which the Tester is connected, depending on the information EtherScope can see about the AP. This field shows the custom User Name if one has been entered. See Assigning a Name and Authorization to a Device in the Wi-Fi app chapter.

BSSID: BSSID of the access point

Channel: Channel number on which the AP is operating

Periodic Scans: Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause

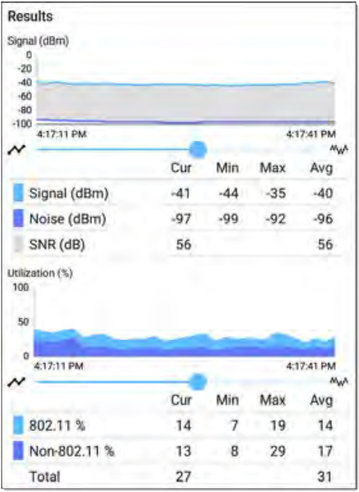
EtherScope to scan for another AP, such as low signal strength or high retry rate.

Last Roam From: If the EtherScope has roamed to a new AP, the previous AP's name, BSSID, and Channel display.

Periodic Scans: Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause EtherScope to scan for another AP, such as low signal strength or high retry rate.

Wi-Fi Link Trending Graphs

EtherScope's trending graphs operate similarly across different testing apps, allowing you to pan and zoom to view different time intervals. Swipe, double tap, and move the slider to adjust the graph views. See the Trending Graphs topic for an overview of the controls.



Results

	Cur	Min	Max	Avg
🟦 Signal (dBm)	-41	-44	-35	-40
🟪 Noise (dBm)	-97	-99	-92	-96
⬜ SNR (dB)	56			56

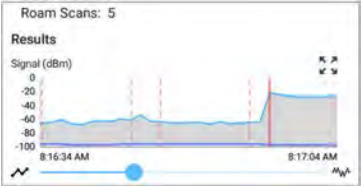
	Cur	Min	Max	Avg
🟦 802.11 %	14	7	19	14
🟪 Non-802.11 %	13	8	29	17
Total	27			31

The Wi-Fi Link Test graphs save and display data for up to 24 hours in the past if the unit stays linked. The default time interval shown is 30 seconds.

Under each graph, a legend table displays the Current, Minimum, Maximum, and Average measurements. The Current column contains measurements from the last second. Min, Max, and Avg columns show cumulative measurements.

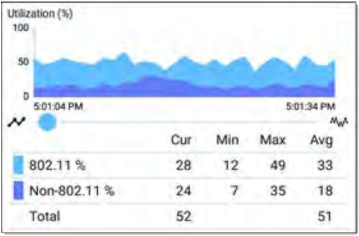
Signal (dBm) graph: Plots the signal strength in dBm of the connected AP

- Signal - The AP's signal strength in dBm
- Noise - The noise level in dBm on the channel used
- SNR - The network's signal-to-noise ratio, a measure of signal strength relative to noise, measured in decibels (dB)


Roam Scans: 5

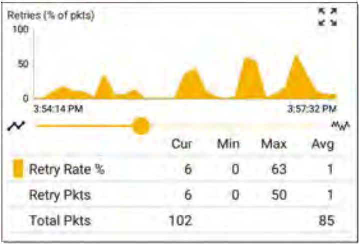
Results

When the EtherScope roams to a new AP, each graph shows a **red** vertical line at the time the tester connected to the new AP, as shown in the image above. Roam scans are indicated by a **red** dashed vertical line.



	Cur	Min	Max	Avg
🟦 802.11 %	28	12	49	33
🟦 Non-802.11 %	24	7	35	18
Total	52			51

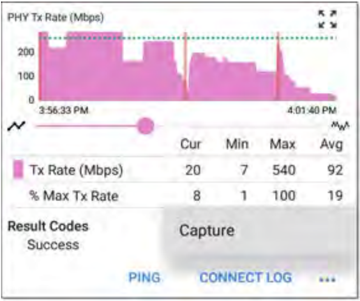
Utilization (%) graph: Plots percentage of the connected channel's capacity being used by 802.11 devices and by non-802.11 interference. If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows only combined 802.11 and non-802.11 channel utilization. See the General Settings topic for more information.



	Cur	Min	Max	Avg
🟨 Retry Rate %	6	0	63	1
Retry Pkts	6	0	50	1
Total Pkts	102			85

Retries (% of packets) graph: Plots percentage of transmitted packets that are retry packets

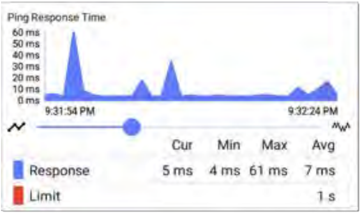
- Retry Rate % - The percentage of total packets that are retry packets
- Retry Pkts - The number of retry packets seen in the current sample cycle
- Total Pkts - The total number of packets transmitted in the current sample cycle



	Cur	Min	Max	Avg
🟪 Tx Rate (Mbps)	20	7	540	92
% Max Tx Rate	8	1	100	19

Result Codes
Success

PHY TX Rate (Mbps) graph: Plots the physical transmission rate. The green horizontal dotted line indicates the AP's maximum TX rate.



	Cur	Min	Max	Avg
🟦 Response	5 ms	4 ms	61 ms	7 ms
🟥 Limit				1 s

Ping or TCP Connect Response Time graph: This graph appears on the Link test screen if you run a Ping or TCP Connect test, using the Ping/TCP app, over the Wi-Fi test port connection while the Profile is linked.

Follow these steps to view the Response Time graph:

1. To navigate easily to the Ping/TCP app, touch the blue **PING** hyperlink at the bottom of the Link test screen.

   The Ping/TCP app opens with the **Interface** set to Wi-Fi Port and **Protocol** set to Ping.

2. Access and adjust the Ping/TCP settings as desired.

3. **START** the Ping or TCP Connect test.

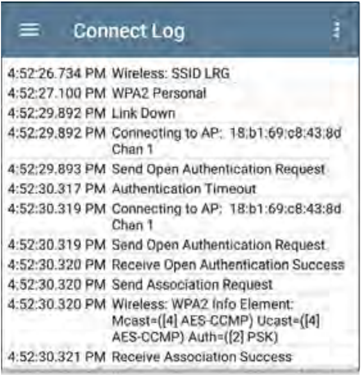
4. Touch back ◁ to go back to the AutoTest Wi-Fi Link screen.

   The Response Time graph appears near the bottom of the screen and updates in real time along with the other graphs for the duration of the Ping/TCP test.

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

Tap the blue links at the bottom of the link test screen to open the Ping/TCP app, view the **CONNECT LOG**, or run a Wi-Fi packet **CAPTURE** on the connected channel and AP.

Connect Log

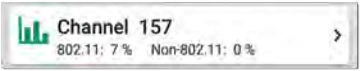


```
4:52:26.734 PM Wireless: SSID LRG
4:52:27.100 PM WPA2 Personal
4:52:29.892 PM Link Down
4:52:29.892 PM Connecting to AP: 18:b1:69:c8:43:8d
               Chan 1
4:52:29.893 PM Send Open Authentication Request
4:52:30.317 PM Authentication Timeout
4:52:30.319 PM Connecting to AP: 18:b1:69:c8:43:8d
               Chan 1
4:52:30.319 PM Send Open Authentication Request
4:52:30.320 PM Receive Open Authentication Success
4:52:30.320 PM Send Association Request
4:52:30.320 PM Wireless: WPA2 Info Element:
               Mcast=([4] AES-CCMP) Ucast=([4]
               AES-CCMP) Auth=([2] PSK)
4:52:30.321 PM Receive Association Success
```

The Connect Log shows the connection log, including driver activity, supplicant, and the DHCP process. The Connect Log can be especially helpful for identifying linking or roaming problems.

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, or attach the Connect Log from the floating action menu ⊕ on the main Profile screen. See Wi-Fi Profile FAB below.

Channel Test Results



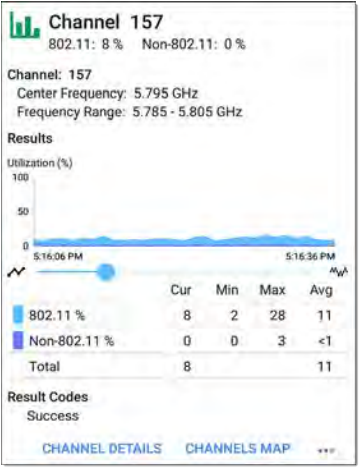
Channel 157

802.11: 7 % Non-802.11: 0 %

The Channel card shows the channel on which the AP is operating and the current 802.11 and Non-802.11 utilization. If the **Combine Utilization** setting is enabled in General Settings, the card shows only combined 802.11 and non-802.11 channel utilization. See the General Settings topic for more information.

Refer to Channel Test Settings if needed.

Channel Test Screen



Channel 157

802.11: 8 % Non-802.11: 0 %

Channel: 157

Center Frequency: 5.795 GHz

Frequency Range: 5.785 - 5.805 GHz

Results

	Cur	Min	Max	Avg
🟦 802.11 %	8	2	28	11
🟪 Non-802.11 %	0	0	3	<1
Total	8			11

Result Codes

Success

The Channel Test results screen indicates the **Center Frequency** and **Frequency Range** of the connected channel along with a real-time Utilization graph.

Results: The channel Utilization (%) graph updates in real time for as long as the unit is still connected to the network. The graph saves and displays data for up to 24 hours if the unit stays linked.

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.

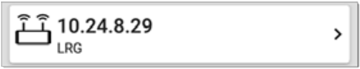
Utilization (%) graph: Plots percentage of the connected channel's capacity being used by 802.11 devices and by non-802.11 interference

- **802.11 %**: Percentage of channel capacity being used by 802.11 devices
- **Non-802.11 %**: Percentage of channel capacity being used by non-802.11 interference
- **Utilization**: If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows only combined 802.11 and non-802.11 channel utilization.
- **Total**: Total percentage of both 802.11 and non-802.11 channel utilization

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

Tap the blue links at the bottom of the channel test results to open the Wi-Fi app's **CHANNEL DETAILS** or **CHANNELS MAP** screens, or to run a Wi-Fi packet **CAPTURE** on the connected channel.

AP (Access Point) Test

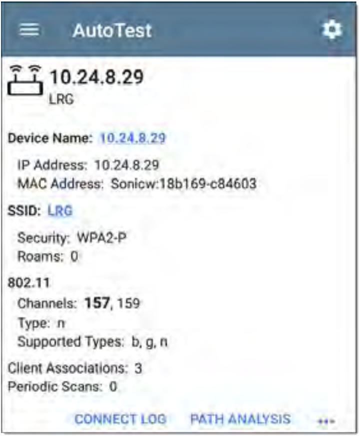


10.24.8.29
LRG

The AP card shows the AP's name and the SSID of the network it is supporting. The AP name or address shown is based on what the EtherScope is able to gather from the device and network. If the AP has a custom user name, that name is shown on the card and test screen.

The AP test is not graded, so the icon remains black.

AP Test Screen



10.24.8.29
LRG

Device Name: 10.24.8.29
IP Address: 10.24.8.29
MAC Address: Sonicw:18b169-c84603

SSID: LRG
Security: WPA2-P
Roams: 0

802.11
Channels: **157**, 159
Type: n
Supported Types: b, g, n

Client Associations: 3
Periodic Scans: 0

In addition to the AP name and SSID, the AP test screen shows the following:

Device Name: AP's name or address

> **IP Address**: The AP's assigned IP address. If none could be determined, the field displays dashes --.
>
> **MAC Address**: The AP's MAC address

SSID: Name of the network on which the AP is operating

Security: Security protocol in use on the network

Roams: Number of times the unit has roamed and connected to a different AP

802.11

Channel(s): Channel or channels the AP is operating on. If the BSSID is on multiple channels, the **bold** channel number indicates the primary channel.

Type: 802.11 type in use on the current link

Supported Types: 802.11 types that the BSSID supports. If none could be determined, the field displays dashes --.

Client Associations: The number of client devices connected to the AP

Periodic Scans: Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause EtherScope to scan for another AP, such as low signal strength or high retry rate.

Tap the blue links at the bottom of the link test screen to view the **CONNECT LOG** or run a **PATH ANALYSIS** to the AP.

Open the overflow menu ••• for additional actions, such as to run a Wi-Fi packet **CAPTURE** on the connected channel and AP, or start a Telnet or SSH session using the AP's IP address.

DHCP, DNS, and Gateway Results

Results for these tests operate the same in both Wired and Wi-Fi profiles.

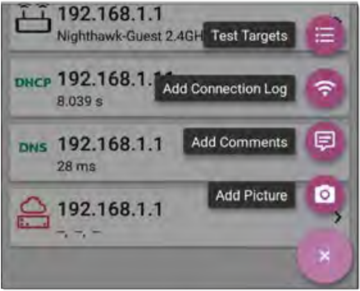
See DHCP, DNS, and Gateway Tests for Wired and Wi-Fi.

PING FTP TCP HTTP Target Tests

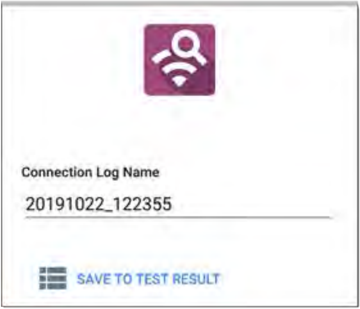
See the Test Targets topic for information on target test results.

Wi-Fi Profile FAB

The floating action button (FAB) on the Wi-Fi Profile AutoTest Profile screens allows you to attach comments, an image, and the Connection 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.

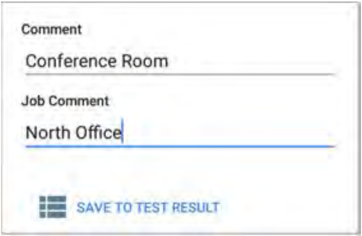


Connection Log Name

20191022_122355

Touch 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

Touch 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.

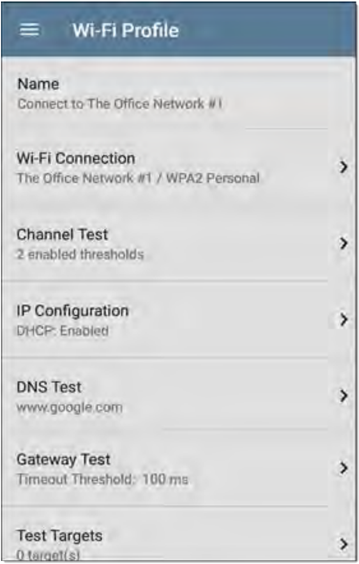
Wi-Fi Profile Settings

These settings control which network is tested, how the EtherScope nXG connects, thresholds for **Success**/**Warning**/**Fail** results, and any user-added test targets.

To configure the profile settings, touch the settings icon ⚙ on the Wi-Fi Profile screen, or add a new Wi-Fi Profile to AutoTest.

Touch the links below to skip to later sections in this topic:

- Wi-Fi Connection Settings
- Certificates
- Advanced Wi-Fi Connection Settings
- Channel Test Settings



Name
Connect to The Office Network #1

Wi-Fi Connection
The Office Network #1 / WPA2 Personal

Channel Test
2 enabled thresholds

IP Configuration
DHCP: Enabled

DNS Test
www.google.com

Gateway Test
Timeout Threshold: 100 ms

Test Targets
0 target(s)

On the **Wi-Fi Profile** settings screen, touch each field described below as needed to configure the profile. Changed settings are automatically applied.

> NOTE: If you add a new Wi-Fi profile from the Wi-Fi Analysis app, the Profile Name, SSID, and Authentication type are auto-populated. See Creating a Wi-Fi Profile from the Wi-Fi Analysis App.

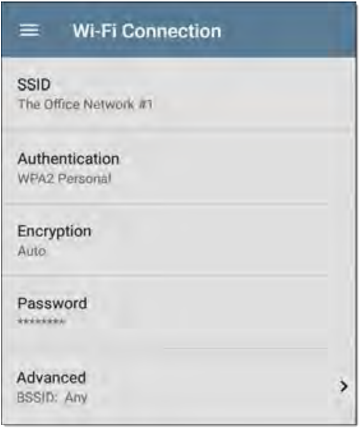
When you finish configuring, tap the back button ◁ to return to the profile.

Name

Touch the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Wi-Fi profile screen header.

🔗 Wi-Fi Connection Settings

Open **Wi-Fi Connection** settings to configure network IDs, security credentials, and test thresholds for the Link 🔗 test. These settings control the Wi-Fi Test Port connection.



SSID
The Office Network #1

Authentication
WPA2 Personal

Encryption
Auto

Password
****

Advanced
BSSID: Any

SSID

Touch to enter an **SSID** or select from the list of discovered SSIDs. If you do not enter a custom **Name** for the Profile, the SSID is displayed as the Wi-Fi Profile's name.

Authentication

If you selected an **SSID** from the drop-down list of discovered SSIDs in the setting above, or created a "Connect to [SSID]" profile from the Wi-Fi app, the Authentication type is automatically selected. If needed, touch to open the **Authentication** dialog and select the correct security type for the network.

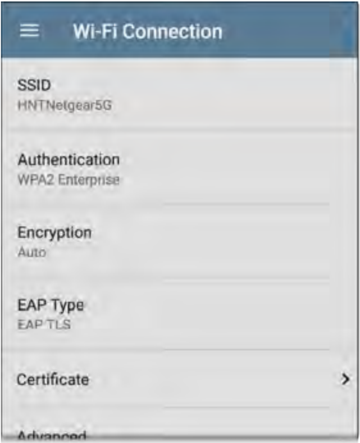
The following settings depend on the Authentication type. Enter all necessary credentials for the network security type, such as Encryption, Keys, EAP type, username, certificate, and/or password.

WEP Key

This setting appears if the Authentication type is **WEP Shared** or **WEP Auto**. Tap to select the correct key type (ASCII or Hex) and enter the key.

Encryption

Touch to select an encryption type if needed. The default is "Auto."



SSID
HNTNetgear5G

Authentication
WPA2 Enterprise

Encryption
Auto

EAP Type
EAP TLS

Certificate

Advanced

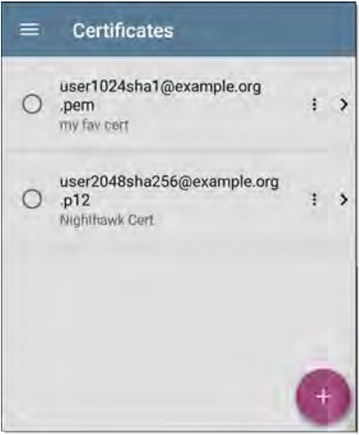
EAP Type

This setting appears if the **Authentication** type is **WPA Enterprise** or **WPA2 Enterprise**. The default is PEAP MSCHAP V2. Touch to select a different EAP type if needed.

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**.

Touch to open the Certificates screen.



Certificates

○ user1024sha1@example.org.pem
my fav cert

○ user2048sha256@example.org.p12
Nighthawk Cert

This screen displays all the certificates that have been imported to AutoTest via the Wired or Wi-Fi Profile settings.

- Touch the radio button to the left of an imported certificate to select and use it with the current Profile.
- Touch a certificate's row to edit its name and description.
- Touch the action overflow icon ⋮ to **Delete** an imported Certificate.
- Touch the floating action button (FAB) ⊕ to import a new certificate file.

EtherScope nXG supports these certificate file extensions:

- .pem
- .p12
- .cer
- .crt

The imported certificate feature is meant for client authentication and must include the private key. The EtherScope supports 1-way client authentication only; mutual authentication, Server, and CA/Root certificates are not supported. While EtherScope can perform a key exchange, it does not authenticate the server certificate.

Touch here to skip the following "How to" section and go to Advanced Wi-Fi Connection Settings.

How to Import a Certificate:

Certificate files can be imported from either an inserted storage device (USB or Micro SD) or the EtherScope's internal file system.

1. Make the certificate file available on your EtherScope unit by saving it to a USB drive or Micro SD card inserted into your unit or by transferring to the file system using a USB-C cable or email. (See Managing Files for help.)

2. To run an **AutoTest Wi-Fi Profile** using certificate authentication, set up the profile with the following **Wi-Fi Connection** settings:

    a. **Authentication**: WPA Enterprise or WPA2 Enterprise

    b. **Encryption**: Auto

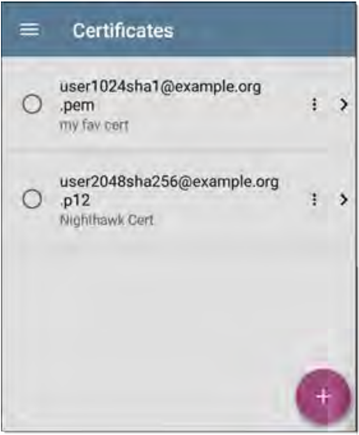
c. **EAP Type**: EAP TLS, PEAP TLS, or TTLS EAP TLS

To run an **AutoTest Wired Profile** using 802.1X with certificate authentication, set up the profile with the following 802.1X test settings:

a. **802.1X**: Enabled

b. **EAP Type**: EAP TLS, PEAP TLS, or TTLS EAP TLS

3. In **AutoTest > Wi-Fi Connection** or **Wired Connection** settings, tap the **Certificate** setting to open the Certificates screen.

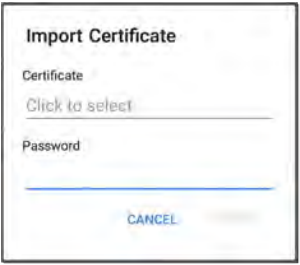


Certificates

○ user1024sha1@example.org.pem
my fav cert

○ user2048sha256@example.org.p12
Nighthawk Cert

4. Touch the floating action button (FAB) ⊕ to open the Import Certificate dialog box.



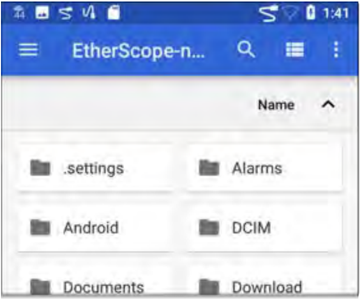
Import Certificate

Certificate

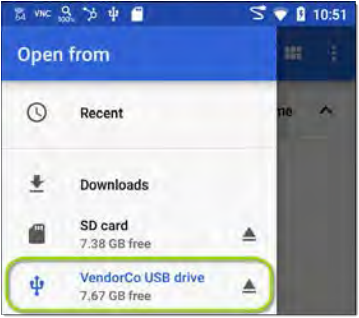
Click to select

Password

5. Touch **Click to select** beneath the Certificate field to open the Files app.

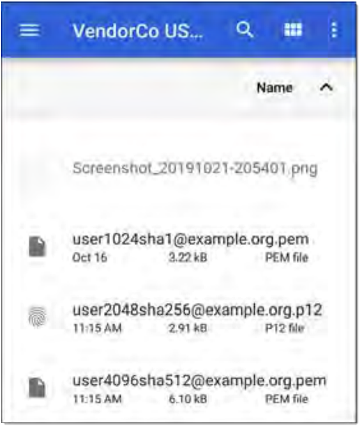


6. In the Files app, navigate to the folder or storage device where your certificate file is saved. Touch the menu button ☰ to open the left-side navigation drawer and access the storage devices.

   In the image above, the user is navigating to a USB flash drive.

7. Navigate to the required certificate file, and touch to select it.



Screenshot_20191021-205401.png

user1024sha1@example.org.pem
Oct 16 3.22 kB PEM file

user2048sha256@example.org.p12
11:15 AM 2.91 kB P12 file

user4096sha512@example.org.pem
11:15 AM 6.10 kB PEM file

After you select a file, the Files app closes, and the Import Certificate dialog displays the chosen certificate file.

8. Enter the certificate’s password if it is password protected.
9. Touch **IMPORT**.
10. If desired, touch the fields to edit the **Name** and **Description** of the certificate.

The name defaults to the certificate filename.

11. Tap the back button ◁ to return to the Certificates list screen. The newly added certificate appears selected in the list.
12. Tap the back button ◁ to return to the Connection settings.

After running the AutoTest, you can review the **Connect Log** from the Wi-Fi Link Test screen or Wired 802.1X Test screen to verify or troubleshoot certificate authentication.

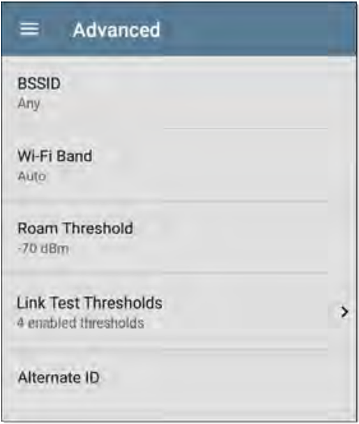
Username

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

Password

This field appears along with multiple security types. Touch the **Password** field to enter the network password.

Advanced (Wi-Fi Connection) Settings



Advanced

BSSID
Any

Wi-Fi Band
Auto

Roam Threshold
-70 dBm

Link Test Thresholds
4 enabled thresholds

Alternate ID

BSSID

Enter or select a specific BSSID for the Wi-Fi Profile to prevent the EtherScope from roaming to a new AP while linked.

Wi-Fi Band

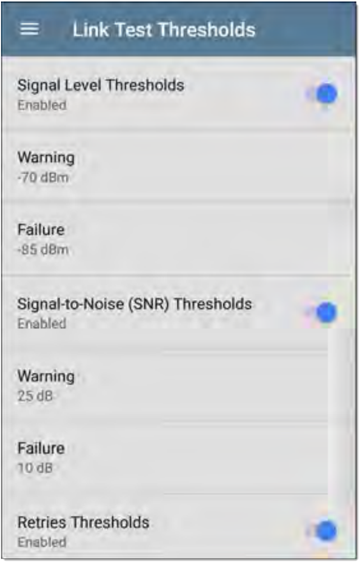
Tap this setting to specify the wireless band(s) on which the Wi-Fi Profile will attempt to connect. The default setting of Auto allows the unit to connect on either band. Note that the Profile will fail to link if this setting conflicts with the selected bands in General Settings.

Roam Threshold

This threshold controls the Signal Strength (in dBm) at which EtherScope disconnects from the linked AP and attempts to connect to another AP on the network with a stronger signal. Touch the field to select a new value or enter a custom one.

Link Test Thresholds

Open the **Link Test Thresholds** screen to adjust the values that determine **Success**/**Warning**/**Fail** results for the following measurements.



Link Test Thresholds

Signal Level Thresholds
Enabled

Warning
-70 dBm

Failure
-85 dBm

Signal-to-Noise (SNR) Thresholds
Enabled

Warning
25 dB

Failure
10 dB

Retries Thresholds
Enabled

Touch each field to select a new value or enter a custom one. Each threshold also has a toggle button that allows you to disable grading based on that measurement entirely.

Signal Level Thresholds: Measured signal from the AP

Signal-to-Noise (SNR) Thresholds: Ratio of measured AP signal to noise level detected on the channel

Retries Thresholds: Retry frames as a percentage of total transmitted frames

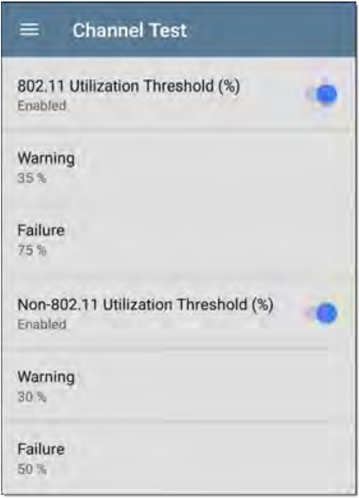
Transmit Rate (TX) Thresholds: Measured rate as a percentage of the AP's maximum throughput rate

Alternate ID

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

Channel Test Settings

Open **Channel Test** settings to configure Utilization thresholds for the channel test portion of the Wi-Fi profile.



802.11 Utilization Threshold (%)
Enabled

Warning
35 %

Failure
75 %

Non-802.11 Utilization Threshold (%)
Enabled

Warning
30 %

Failure
50 %

If the **Combine Utilization** setting is enabled in General Settings, only a single, combined **Utilization Threshold** setting appears.

802.11 Utilization Threshold (%)

This threshold controls the **Success**/**Warning**/**Fail** gradings for the percentage of the connected channel's capacity being used by 802.11 devices.

- Touch the toggle button to enable or disable test grading based on 802.11 utilization.
- Touch **Warning** or **Failure** to select or enter custom percentage values for Warning or Failure results.

Non-802.11 Utilization Threshold (%)

This threshold controls the **Success**/**Warning**/**Fail** gradings for the percentage of the connected channel's capacity being used by non-802.11 interference.

- Touch the toggle button to enable or disable test grading based on non-802.11 utilization.
- Touch **Warning** or **Failure** to select or enter custom percentage values for Warning or Failure results.

DHCP, DNS, and Gateway Settings

Settings for these tests operate the same in both Wired and Wi-Fi profiles.

See DHCP, DNS, and Gateway Tests for Wired and Wi-Fi.

PING FTP TCP HTTP Test Targets

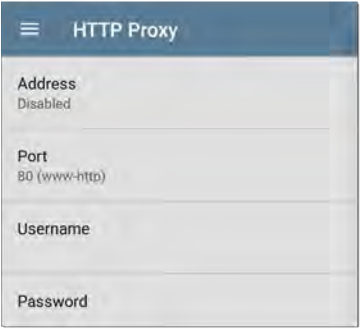
Touch the **Test Targets** field to open the Test Targets screen and add custom **Ping**, **TCP Connect**, **HTTP**, or **FTP Tests** to your AutoTest profile. See Test Targets to learn more.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the EtherScope 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. When using a web browser, the Wired Test Port takes priority over the Wi-Fi Test Port, so if you want to browse via Wi-Fi proxy connection, unplug the (top) Wired Test Port.

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



Address
Disabled

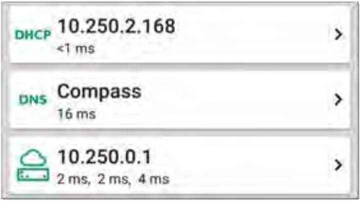
Port
80 (www-http)

Username

Password

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

DHCP, DNS, and Gateway Tests for Wired and Wi-Fi AutoTests



DHCP 10.250.2.168 ›
<1 ms

DNS Compass ›
16 ms

10.250.0.1 ›
2 ms, 2 ms, 4 ms

These tests are included in both Wired and Wi-Fi AutoTest Profiles, and the settings and results fields are the same for each Profile type. Access AutoTest's DHCP, DNS, and Gateway settings from either the Wired or Wi-Fi Profile settings screens, or by touching the settings button ⚙ from the full results screen for each test type.

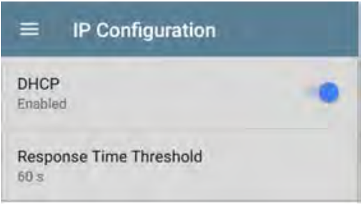
Touch blue links or the blue action overflow icon ••• on the test results screens for additional actions.

DHCP or Static IP Test

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

DHCP Settings – IP Configuration

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



DHCP
Enabled

Response Time Threshold
60 s

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

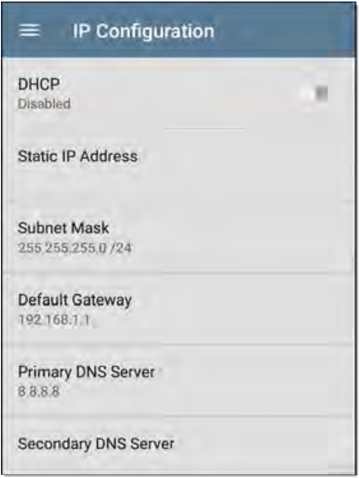
DHCP

DHCP is enabled by default. Touch 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 EtherScope waits for a DHCP server response before failing the Link and DHCP tests.

Static IP Address



DHCP
Disabled

Static IP Address

Subnet Mask
255.255.255.0 /24

Default Gateway
192.168.1.1

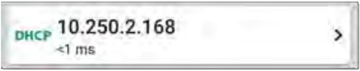
Primary DNS Server
8.8.8.8

Secondary DNS Server

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

DHCP Test Results

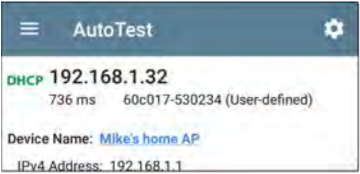
When DHCP is enabled, the DHCP test card and results screen are displayed in the Profile.



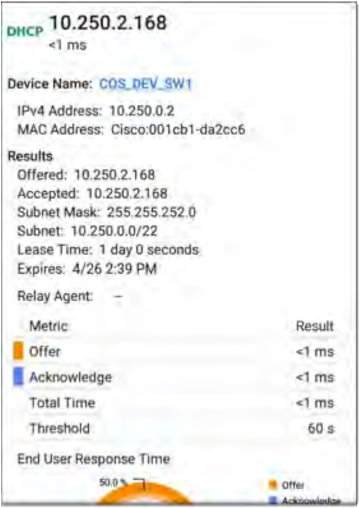
The DHCP Test card displays the DHCP server's IP address and the total time for the discover, offer, request, and acknowledgment to complete.

Touch the card to open the DHCP test screen.

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


AutoTest
DHCP
192.168.1.32
736 ms
60c017-530234 (User-defined)
Device Name: Mike's home AP
IPv4 Address: 192.168.1.1

DHCP Test Results Screen



DHCP 10.250.2.168

<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

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 Ether-Scope

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

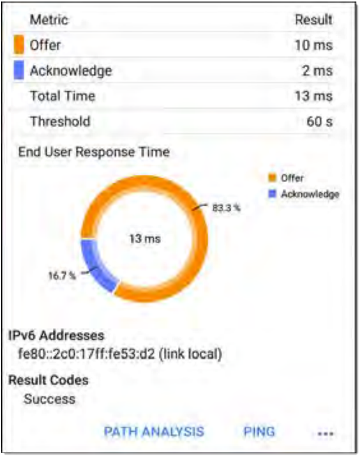
Lease Time: The amount of time the IP address is leased to the EtherScope by the DHCP server

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



	Metric	Result
🟧	Offer	10 ms
🟦	Acknowledge	2 ms
	Total Time	13 ms
	Threshold	60 s

End User Response Time

IPv6 Addresses
fe80::2c0:17ff:fe53:d2 (link local)

Result Codes
Success

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

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

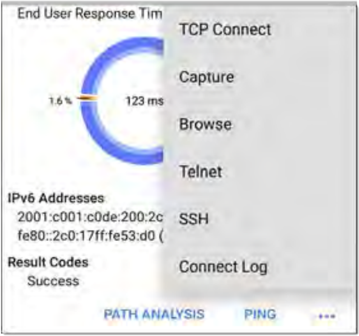
Total Time: Total amount of time consumed by the DHCP process

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



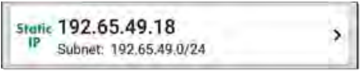
IPv6 Addresses
2001:c001:c0de:200:2c
fe80::2c0:17ff:fe53:d0 (

Result Codes
Success

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

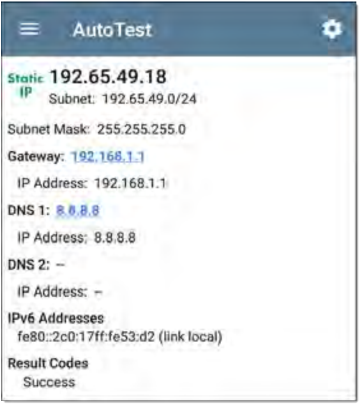
If DHCP is disabled, the DHCP test becomes a "Static IP" test and the Subnet and addresses that were entered in the DHCP test settings are displayed.



Static IP 192.65.49.18
Subnet: 192.65.49.0/24

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

Touch the card to open the test results screen.



Static IP 192.65.49.18
Subnet: 192.65.49.0/24

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IP Address: 192.168.1.1

DNS 1: 8.8.8.8

IP Address: 8.8.8.8

DNS 2: --

IP Address: --

IPv6 Addresses
fe80::2c0:17ff:fe53:d2 (link local)

Result Codes
Success

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

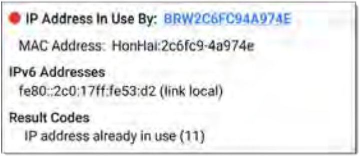
DNS (1 and 2): Names and IP addresses of Primary and Secondary DNS servers

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. Touch the blue underlined link to open a Discovery Details screen for the device.

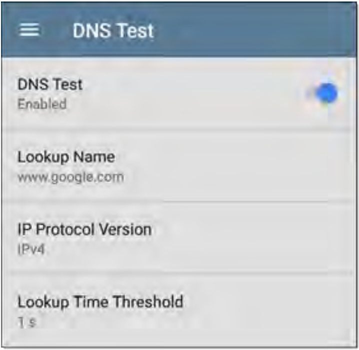
> **MAC Address**: MAC of the device using the IP address

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 EtherScope obtains DNS addresses through DHCP or static address configuration.

DNS Test Settings



DNS Test
Enabled

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) will attempt to resolve. Touch the field to enter a URL other than the default: www.google.com.

IP Protocol Version

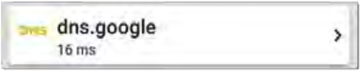
Touch the field to switch between IPv4 and IPv6.

Lookup Time Threshold

This threshold controls how long the EtherScope waits for a response from the DNS server(s) before the test is failed. The default is 1 second. Touch 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.

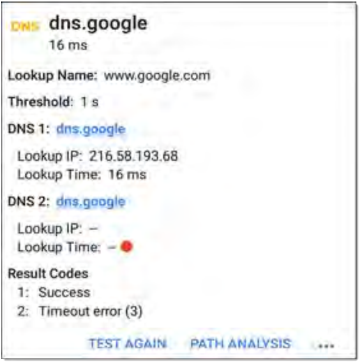


DNS dns.google

16 ms

Touch the card to open the DNS test results screen.

DNS Test Results Screen



DNS dns.google

16 ms

Lookup Name: www.google.com

Threshold: 1 s

DNS 1: dns.google

Lookup IP: 216.58.193.68
Lookup Time: 16 ms

DNS 2: dns.google

Lookup IP: –
Lookup Time: – ●

Result Codes
1: Success
2: Timeout error (3)

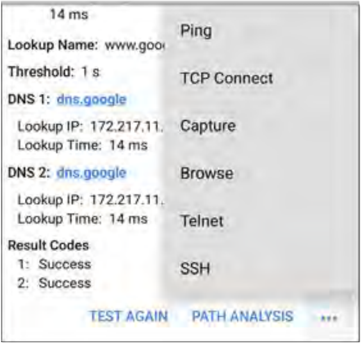
Lookup Name: Name resolved by the DNS servers

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.goo

Threshold: 1 s

DNS 1: dns.google

Lookup IP: 172.217.11.

Lookup Time: 14 ms

DNS 2: dns.google

Lookup IP: 172.217.11.

Lookup Time: 14 ms

Result Codes

1: Success

2: Success

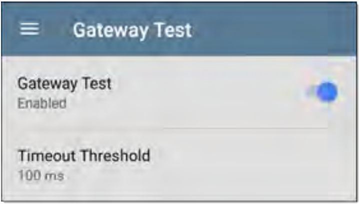
Touch blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the DNS **Test Again**, open another app populated with the name and IP address of DNS 1, or **Browse** to the Primary DNS server in your web browser.

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
Enabled

Timeout Threshold
100 ms

Gateway Test

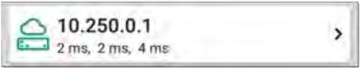
If desired, you can tap the top field on the Gateway Test screen and switch the toggle to disable the Gateway test in your current AutoTest. When this setting is disabled, the Gateway card does not appear on the main AutoTest results screen, and the following setting is hidden.

Timeout Threshold

The only other setting for the Gateway Test is the timeout threshold, which indicates how long the EtherScope will wait 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

EtherScope 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 EtherScope's subnet. See Discovery Settings for information about SNMP configuration.

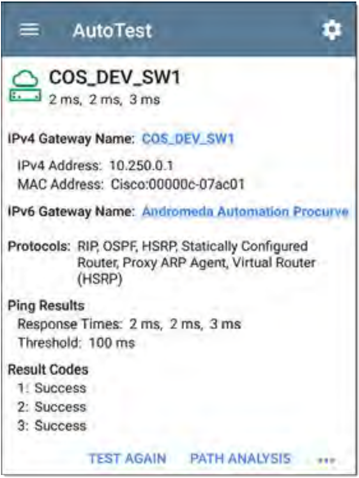


10.250.0.1

2 ms, 2 ms, 4 ms

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

Gateway Test Results Screen



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

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)

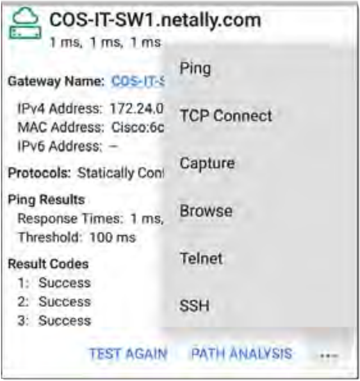
IPv6 Gateway Name: Name advertised by the IPv6 router (if available)

Protocols: Routing protocols the EtherScope 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-S

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

Protocols: Statically Con

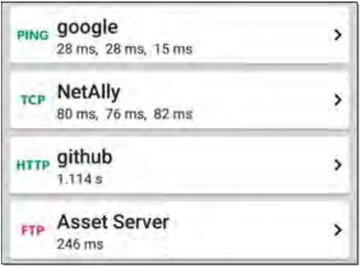
Ping Results
Response Times: 1 ms,
Threshold: 100 ms

Result Codes
1: Success
2: Success
3: Success

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

Back to Title and Contents

Test Targets for Wired and Wi-Fi AutoTests



PING google
28 ms, 28 ms, 15 ms

TCP NetAlly
80 ms, 76 ms, 82 ms

HTTP github
1.114 s

FTP Asset Server
246 ms

AutoTest Target tests are user-assignable endpoints to which EtherScope nXG 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

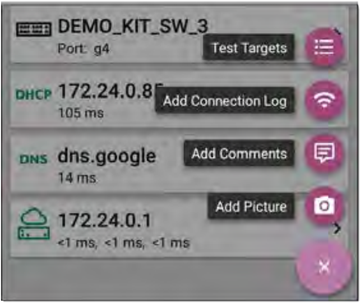
TCP Connect

HTTP

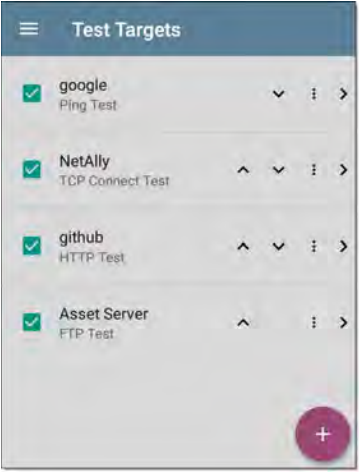
FTP

Adding and Managing Test Targets

To add test targets to AutoTest profiles and manage your saved targets, open the **Test Targets** screen from either the Wired or Wi-Fi Profile Settings ⚙ or by touching the FAB ⊕ on the Wired or Wi-Fi 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 or Wi-Fi Profiles.



☑ google
Ping Test

☑ NetAlly
TCP Connect Test

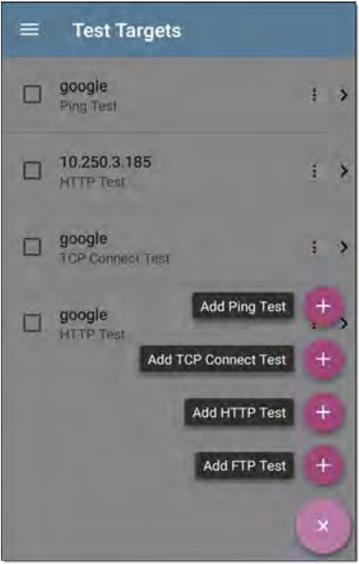
☑ github
HTTP Test

☑ Asset Server
FTP Test

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

- Select the checkboxes for each Target you want to include in the current Wired or Wi-Fi profile.

- Tap the up and down arrows ⌃ ⌄ to reorder the saved Test Targets on this screen and the main AutoTest Profile screen.
- Touch 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.
- Touch the FAB icon ⊕ to add a new target test: Ping, TCP Connect, HTTP, or FTP.

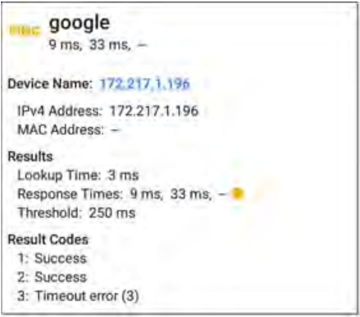


- Touch any target's name, or add a new target, to open the test's settings, where you can enter a custom test name, target address, and thresholds.

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.



google
9 ms, 33 ms, –

Device Name: 172.217.1.196

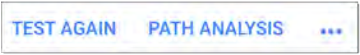
IPv4 Address: 172.217.1.196
MAC Address: –

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



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

- Touch 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.
- Touch TEST AGAIN to run just the target test again.
- Touch PATH ANALYSIS to open the Path Analysis app. The path Destination will be configured with the current target.
- Touch the action overflow icon ••• to open the listed apps or tools with the target

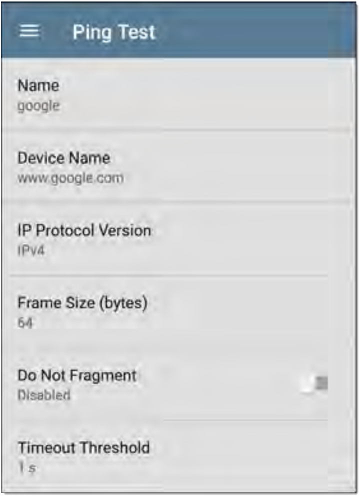
pre-populated, for example:

- 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



Name
google

Device Name
www.google.com

IP Protocol Version
IPv4

Frame Size (bytes)
64

Do Not Fragment
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.

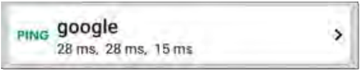
IP Protocol Version: IPv4 is used by default. Touch the field to switch between IPv4 and IPv6.

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: Touch the toggle button to enable.

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

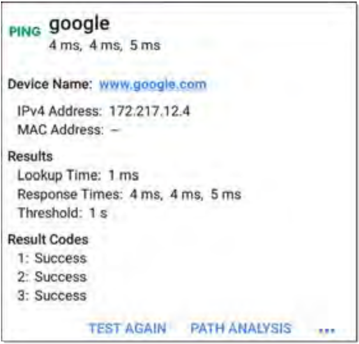
Ping Test Results


PING google
28 ms, 28 ms, 15 ms

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

Touch 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

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

Device Name: Hostname or address of the target device

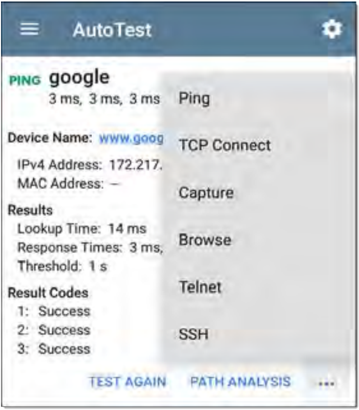
- **IPv4 or IPv6 Address**: IP address of the target device

- **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 EtherScope 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



PING google
3 ms, 3 ms, 3 ms

Device Name: www.goog
IPv4 Address: 172.217.
MAC Address: –

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

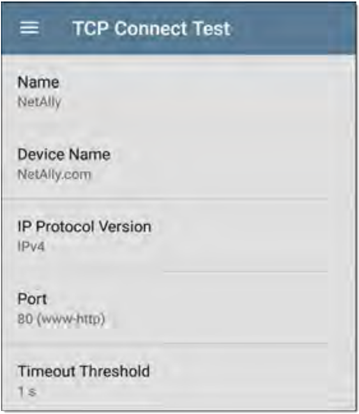
Result Codes
1: Success
2: Success
3: Success

Touch 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



Name
NetAlly

Device Name
NetAlly.com

IP Protocol Version
IPv4

Port
80 (www-http)

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.

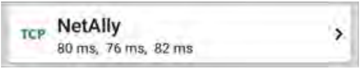
Device Name: Enter the IP address or URL of the target you want to test. If you enter an IP address, the DNS lookup portion of the test will be skipped.

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

Port: Specify the TCP port number EtherScope will use to connect to the target.

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

TCP Connect Test Results

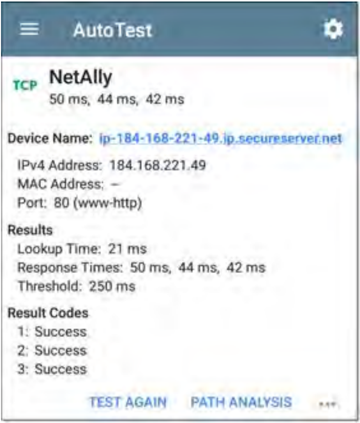


TCP NetAlly
80 ms, 76 ms, 82 ms

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

Touch the card to open the TCP results screen.

AutoTest TCP Results Screen



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

Device Name: ip-184-168-221-49.ip.secureserver.net

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

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

Result Codes
1: Success
2: Success
3: Success

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 EtherScope to receive a response from the server for each of the three connect tests

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

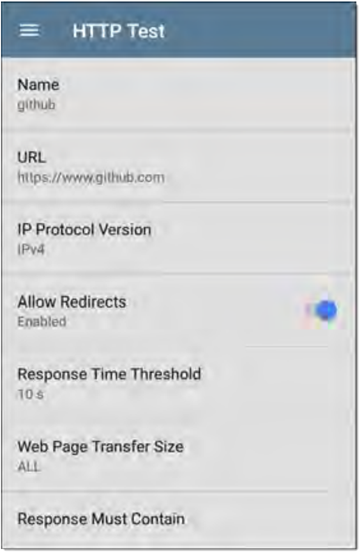
Results Codes: Final status of the test (Success or Failure) for each of the three Pings

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.



Name
github

URL
https://www.github.com

IP Protocol Version
IPv4

Allow Redirects
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. Touch the field to switch between IPv4 and IPv6.

Allow Redirects

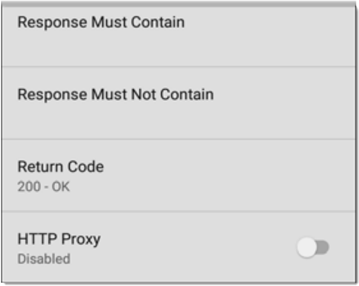
Touch the toggle button to permit web redirects when trying to connect to the target.

Response Time Threshold

This threshold controls how long the EtherScope waits for a response from the URL before failing the test. Touch 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**). Touch the field to select a different transfer size.



Response Must Contain

Response Must Not Contain

Return Code
200 - OK

HTTP Proxy
Disabled

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."

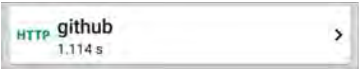
Return Code

The Return Code set here functions as **pass**/**fail** test criteria. The default is "OK (HTTP 200)." Touch 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 EtherScope receives a different return code, the test fails.

HTTP Proxy

The Proxy control in target test settings utilizes the server address and port specified in the main profile settings. Touch the toggle to use those Proxy settings. See Wired Profile Settings or Wi-Fi Profile Settings.

HTTP Test Results

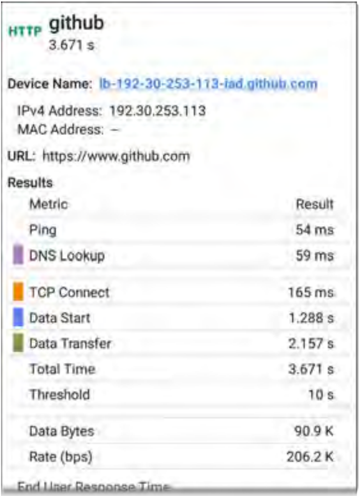


HTTP github

1.114 s

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

HTTP Test Results Screen



github
3.671 s

Device Name: lb-192-30-253-113-iad.github.com

IPv4 Address: 192.30.253.113
MAC Address: –

URL: https://www.github.com

Results

Metric	Result
Ping	54 ms
🟪 DNS Lookup	59 ms
🟧 TCP Connect	165 ms
🟦 Data Start	1.288 s
🟩 Data Transfer	2.157 s
Total Time	3.671 s
Threshold	10 s
Data Bytes	90.9 K
Rate (bps)	206.2 K

End User Response Time

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

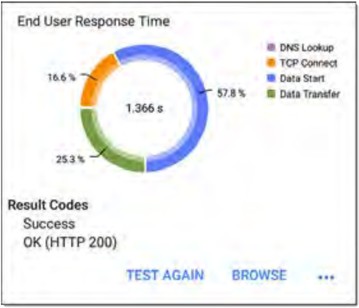
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, test will fail.

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



Result Codes

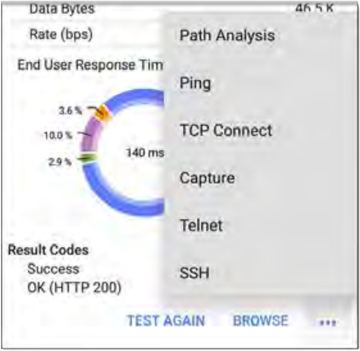
Success

OK (HTTP 200)

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.



Data Bytes 46.5 K

Rate (bps)

End User Response Tim

Result Codes

Success

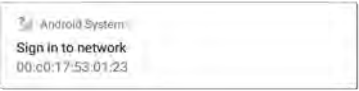
OK (HTTP 200)

Touch 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.

Captive Portal Connections

The HTTP test supports connections through a network with a captive portal requirement.

When running a Profile that connects to a network with a Captive Portal, an Android notification ? appears to prompt you to enter the captive portal credentials.

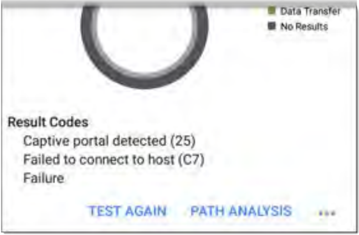


Android System

Sign in to network

00:c0:17:53:01:23

For the HTTP test to pass, you must select the notification and enter the required credentials on the portal website. Otherwise, the HTTP test will fail, with a Result Code of "Captive portal detected (25)."



Result Codes

Captive portal detected (25)

Failed to connect to host (C7)

Failure

See the Captive Portal section in the Connecting to Wi-Fi topic for more instructions.

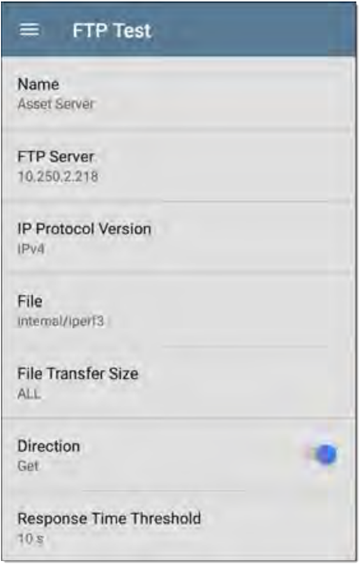
When finished in the captive portal browser window, hit the back button ◁ to return to the HTTP test, and touch **TEST AGAIN** to receive valid results.

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.



Name
Asset Server

FTP Server
10.250.2.218

IP Protocol Version
IPv4

File
internal/iperf3

File Transfer Size
ALL

Direction
Get

Response Time Threshold
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. Touch the field to switch between IPv4 and IPv6.

File

This setting specifies the path and filename of the file that is downloaded from (**Get**) or uploaded to (**Put**) the server, based on the **Direction** setting below. Touch 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 EtherScope to create and upload a file that is 10 MB.

Direction

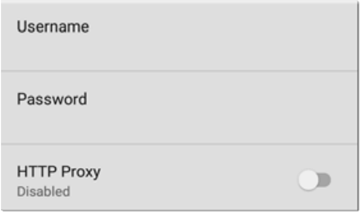
Touch the toggle button to switch between a **Get** (download the **File** from the server) or **Put** (upload the **File** to the server) test.

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

Response Time Threshold

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



Username

Password

HTTP Proxy
Disabled

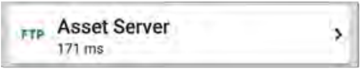
Username and Password

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

HTTP Proxy

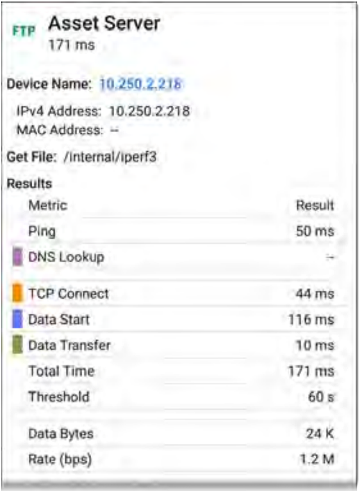
The Proxy control in target test settings utilizes the server address and port specified in the main profile settings. See Wired Profile Settings or Wi-Fi Profile Settings.

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



FTP **Asset Server**
171 ms

Device Name: 10.250.2.218

IPv4 Address: 10.250.2.218
MAC Address: --

Get File: /internal/iperf3

Results

Metric	Result
Ping	50 ms
🟪 DNS Lookup	--
🟧 TCP Connect	44 ms
🟦 Data Start	116 ms
🟩 Data Transfer	10 ms
Total Time	171 ms
Threshold	60 s
Data Bytes	24 K
Rate (bps)	1.2 M

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

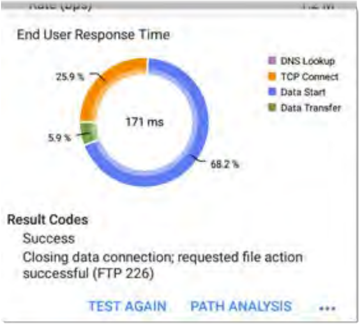
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test will fail.

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



Result Codes

Success

Closing data connection; requested file action successful (FTP 226)

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.

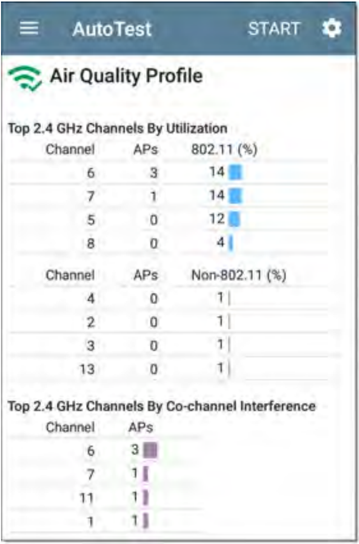
Touch blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the FTP **Test Again**, open another testing app, or **Browse** to the FTP server in your web browser.

Air Quality AutoTest Profiles

Air Quality Profiles perform a single scan of the channels in your wireless network to measure channel utilization and interference.

Each table on the Air Quality results screen shows the top four channels in each band with the highest utilization or co-channel interference, along with the number of APs operating on the channel.

Air Quality Profile results are described next. Touch here to skip to Air Quality Settings.



Air Quality Profile

Top 2.4 GHz Channels By Utilization

Channel	APs	802.11 (%)
6	3	14
7	1	14
5	0	12
8	0	4

Channel	APs	Non-802.11 (%)
4	0	1
2	0	1
3	0	1
13	0	1

Top 2.4 GHz Channels By Co-channel Interference

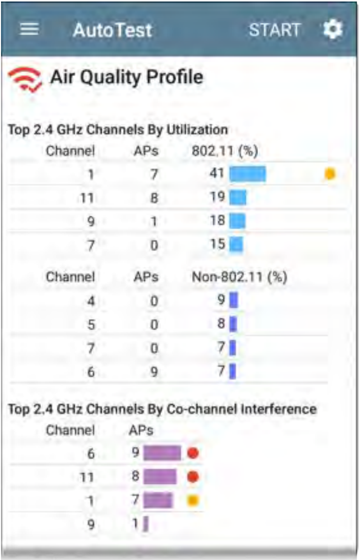
Channel	APs
6	3
7	1
11	1
1	1

First, EtherScope scans the 2.4-GHz band and displays results and then does the same for the 5-GHz band.

Channel usage depends on the number of clients connected to the network and the amount of interference from devices like microwaves or smartphones using Bluetooth. Very high utilization or interference can affect network performance.

Air Quality Profile Results

The image below shows a completed Air Quality Profile test with two **Warnings** and two **Failures** indicated by the yellow and red dots next to the corresponding measurements.



Air Quality Profile

Top 2.4 GHz Channels By Utilization

Channel	APs	802.11 (%)	
1	7	41	●
11	8	19	
9	1	18	
7	0	15	

Channel	APs	Non-802.11 (%)
4	0	9
5	0	8
7	0	7
6	9	7

Top 2.4 GHz Channels By Co-channel Interference

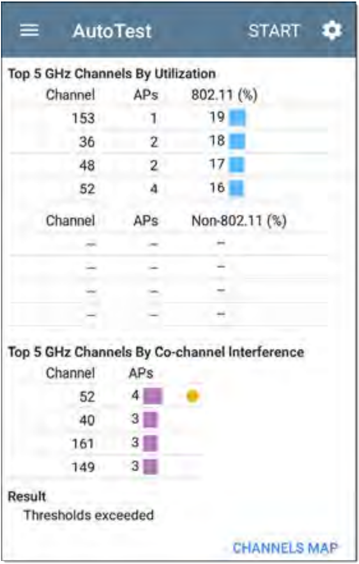
Channel	APs	
6	9	●
11	8	●
1	7	●
9	1	

Air Quality test gradings are based on the Thresholds configured in the Profile's settings. In the case shown here, the Warnings and Failures occurred because of high Utilization and Co-channel Interference caused by the number of APs active on the top three 2.4 GHz channels: 1, 6, and 11.

802.11 Utilization %: Percentage of the displayed channel's capacity being used by all 802.11 WLAN devices

Non-802.11 Utilization %: Percentage of the displayed channel's capacity being used by non-802.11 interferers, which may be non-WLAN sources

If the **Combine Utilization** setting is enabled in General Settings, only combined 802.11 and non-802.11 channel utilization is shown for the top channels. See the General Settings topic for more information.



Top 5 GHz Channels By Utilization

Channel	APs	802.11 (%)
153	1	19 🟦
36	2	18 🟦
48	2	17 🟦
52	4	16 🟦

Channel	APs	Non-802.11 (%)
–	–	–
–	–	–
–	–	–
–	–	–

Top 5 GHz Channels By Co-channel Interference

Channel	APs	
52	4 🟪	●
40	3 🟪	
161	3 🟪	
149	3 🟪	

Result

Thresholds exceeded

Two dashes -- indicate that no Utilization was detected on the Channels shown.

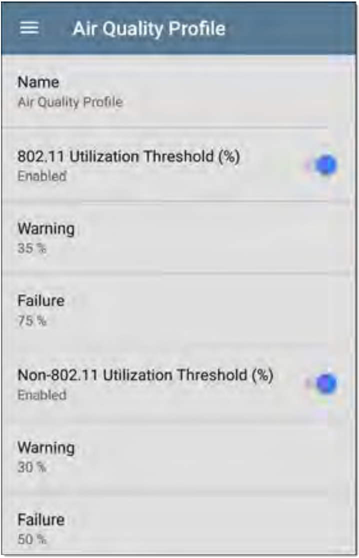
Co-channel Interference: Interference caused by multiple APs operating on the same channel that exceed the minimum **Co-channel Interference AP Signal Level** threshold in the settings. This measurement accounts for 40-MHz and 80-MHz channels in the 5-GHz band by counting an AP on its primary and each secondary channel.

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

Tap the blue link at the bottom of the Air Quality Profile screen to open the Wi-Fi app's CHANNELS MAP, which provides real-time visual results of the utilization on each channel.

Air Quality Profile Settings

To configure the profile settings, touch the settings icon ⚙ on the Air Quality Profile screen, or add a new Air Quality Profile to AutoTest.



Air Quality Profile

Name
Air Quality Profile

802.11 Utilization Threshold (%)
Enabled

Warning
35 %

Failure
75 %

Non-802.11 Utilization Threshold (%)
Enabled

Warning
30 %

Failure
50 %

The settings for Air Quality are thresholds for grading the channel utilization and interference.

On the **Air Quality Profile** settings screen, touch 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

Touch the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Air Quality profile screen header.

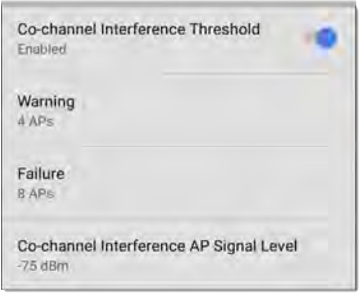
Thresholds

Use the threshold controls to adjust the values that determine **Warning**/**Fail** results for the corresponding utilization and co-channel interference measurements. Touch each Warning or Failure field to select a new value or enter a custom one. Each threshold also has a toggle button that allows you to disable grading based on that measurement entirely.

By default, you can set thresholds for both 802.11 and non-802.11 Utilization. If the **Combine Utilization** setting is enabled in

General Settings, there is only a single combined 802.11 and non-802.11 Utilization Threshold.

Utilization measurements and thresholds are percentages of a channel's capacity. Co-channel interference measurements and thresholds are the number of APs operating on the same channel.



Co-channel Interference Threshold
Enabled

Warning
4 APs

Failure
8 APs

Co-channel Interference AP Signal Level
-75 dBm

Co-channel Interference AP Signal Level

This setting designates the minimum signal level at which an AP must be measured to be counted in Co-Channel Interference measurements. Touch the field to select a new value or enter a custom one.

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).

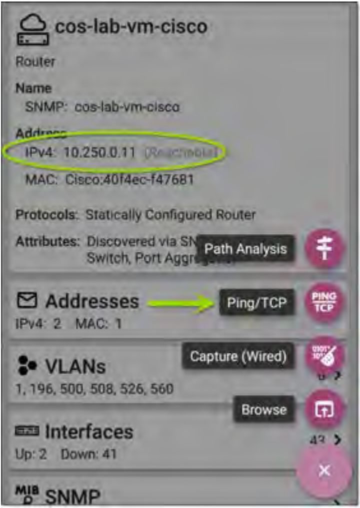
You can open the TCP/Ping app from the Home screen, or you can select **Ping** or **TCP Connect** from another app, such as AutoTest or Discovery, while viewing a device's details.

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 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 SN
Switch, Port Aggr

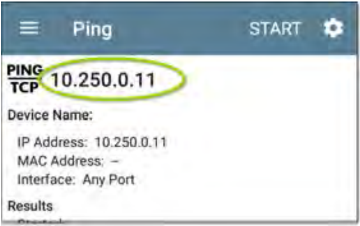
Addresses
IPv4: 2 MAC: 1

VLANs
1, 196, 500, 508, 526, 560

Interfaces
Up: 2 Down: 41

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.



10.250.0.11

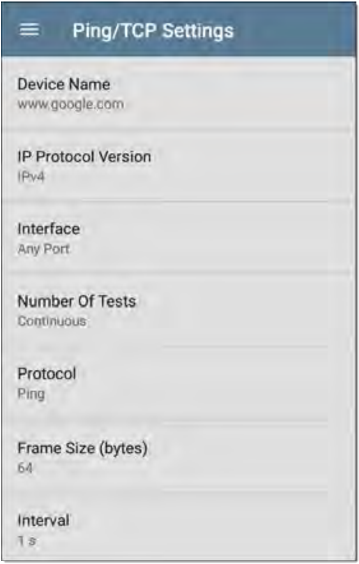
Device Name:

IP Address: 10.250.0.11
MAC Address: –
Interface: Any Port

Results

Configuring Ping/TCP Settings Manually

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



Ping/TCP Settings

Device Name
www.google.com

IP Protocol Version
IPv4

Interface
Any Port

Number Of Tests
Continuous

Protocol
Ping

Frame Size (bytes)
64

Interval
1 s

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

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

Interface: This setting determines the EtherScope port from which the test runs. Touch the field to select Any Port, Wired or Wi-Fi Test Port, or Wired or Wi-Fi Management Port.

See Test and Management Ports for explanations of the different ports.

Number of Tests: Touch to select the number of Ping or TCP connect tests you want to run. The default setting of **Continuous** keeps running tests until you touch 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 EtherScope 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 EtherScope. 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 EtherScope will use to connect to the target address for a TCP Port Open test. If needed, touch the **Port** field to open a pop-up number pad and enter a new port number. Touch **OK** to save it.

Timeout Threshold: This threshold controls how long the EtherScope 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. Touch the toggle button to enable. See the Frame Size setting description above.

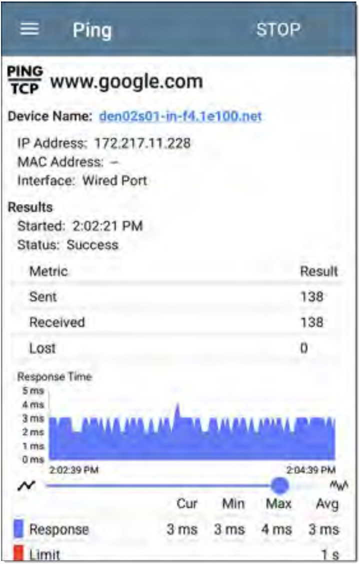
Running Ping/TCP Tests

Your unit must be connected to an active wired or Wi-Fi network (Test or Management Port) to run Ping and TCP Connect tests. Icons in the top Status Bar indicate whether and how your EtherScope 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, touch **START**.

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



www.google.com

Device Name: den02s01-in-f4.1e100.net

IP Address: 172.217.11.228
MAC Address: –
Interface: Wired Port

Results
Started: 2:02:21 PM
Status: Success

Metric	Result
Sent	138
Received	138
Lost	0

	Cur	Min	Max	Avg
🟦 Response	3 ms	3 ms	4 ms	3 ms
🟥 Limit				1 s

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 EtherScope 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 Wi-Fi or wired connections. 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.

On EtherScope, the capture process uses the Wired or Wi-Fi Test port .

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

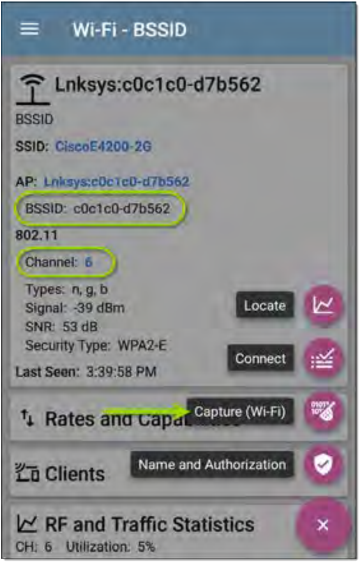
Capture Settings

The Capture app settings allow you to switch between Wired and Wi-Fi, designate file and slice sizes, and apply filters to capture and analyze only certain packet types. For example, you can set a wired filter to capture only packets related to a specific application (based on IP address and port number), or create a Wi-Fi filter to capture only packets to and from a particular AP or client.

When you open Capture from Home and do not configure any filters, all packets from the switch or channel are captured. The default Wired capture saves all the packets sent from the local switch to the EtherScope. The default Wi-Fi capture saves the packets seen on channel 1.

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 or Wi-Fi Channel, Channel Width, and BSSID.

For example, the floating action menu on the Wi-Fi app's BSSID Details screen below contains the option to start a Wi-Fi Capture.



Lnksys:c0c1c0-d7b562

BSSID

SSID: CiscoE4200-2G

AP: Lnksys:c0c1c0-d7b562

BSSID: c0c1c0-d7b562

802.11

Channel: 6

Types: n, g, b

Signal: -39 dBm

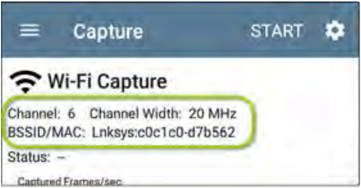
SNR: 53 dB

Security Type: WPA2-E

Last Seen: 3:39:58 PM

CH: 6 Utilization: 5%

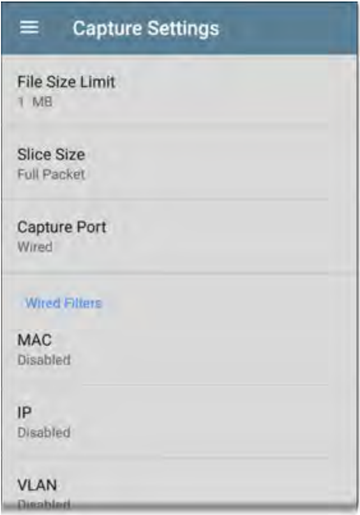
When the Capture app opens, filters are already set with the BSSID, Channel, and Channel Width from the Wi-Fi app.



Channel: 6 Channel Width: 20 MHz
BSSID/MAC: Lnksys:c0c1c0-d7b562
Status: –

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

Touch the settings icon ⚙ in the Capture screen to configure capture settings.



Capture Settings

File Size Limit
1 MB

Slice Size
Full Packet

Capture Port
Wired

Wired Filters

MAC
Disabled

IP
Disabled

VLAN
Disabled

File Size Limit: Touch 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: Touch 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.

Capture Port: Touch to select either the **Wired** or **Wi-Fi** test port.

Wired Filters

All filters are disabled by default unless you open Capture from another app. Touch the fields below to enable 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 IP address of a host to capture only traffic to and from the host. You can specify an IPv4 or IPv6 address.

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: Touch the toggle to enable this setting, which directs the EtherScope NOT to capture the values you have entered in the filters above. For example, if you have set up a filter to capture traffic to and from IP 10.250.0.70 on Port 80 and you enable NOT, all traffic will be captured *except* traffic to and from 10.250.0.70 on port 80.

Wi-Fi Filters

Channel: Tap the channel button to set the channel on which packets will be captured.

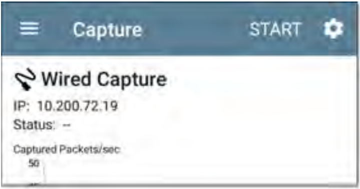
Channel Width: This setting appears if you have selected a Channel number in the 5-GHz band (above channel 14). Tap to select a 20, 40, or 80 MHz width.

BSSID/MAC: Enter a BSSID to capture only packets going to or from the target device.

Control, Data, and Management Frames and Beacons: All frame types are captured by default. Tap the toggle button for each frame type to disable its capture.

Running and Viewing Captures

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



Wired Capture

IP: 10.200.72.19

Status: --

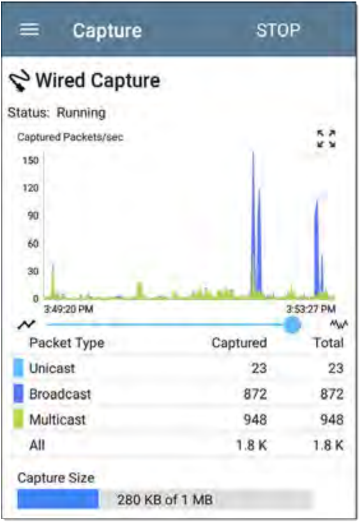
Captured Packets/sec

50

The current Status of the capture and any applied filters are shown under the capture type (Wired or Wi-Fi). The image above indicates that the app will only capture traffic for IP 10.200.72.19.

View the real-time status of the capture as it is running. If you navigate away from the Capture app, the capture process will continue to run in the background until the File Size Limit (in Capture Settings) is reached. However, a Wi-Fi capture will stop if you open the Wi-Fi app, which initiates scanning, or connect to a Wi-Fi network using AutoTest.

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



Wired Capture

Status: Running

Packet Type	Captured	Total
🟦 Unicast	23	23
🟦 Broadcast	872	872
🟩 Multicast	948	948
All	1.8 K	1.8 K

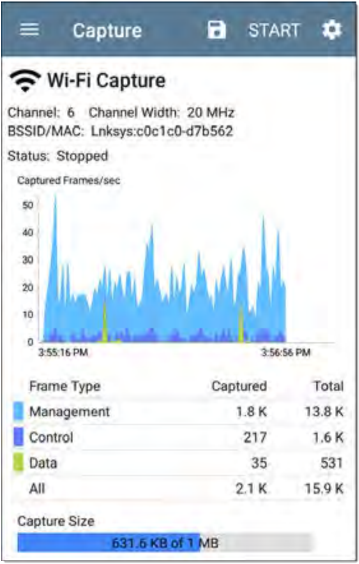
Capture Size

280 KB of 1 MB

The Wired graph plots the type and number of packets being captured during the time the capture is running. By default, wired captures include 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.

Wi-Fi captures graph the Management, Control, and Data Frame Types.



Wi-Fi Capture

Channel: 6 Channel Width: 20 MHz
BSSID/MAC: Lnksys:c0c1c0-d7b562

Status: Stopped

Frame Type	Captured	Total
Management	1.8 K	13.8 K
Control	217	1.6 K
Data	35	531
All	2.1 K	15.9 K

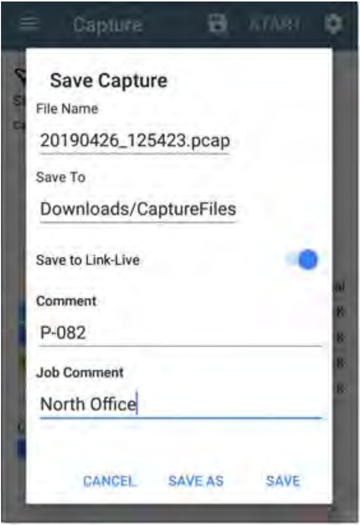
Capture Size

631.6 KB of 1 MB

In this image, the app has captured all three Wi-Fi Frame Types on channel 6 with the BSSID shown. The Total measurements in the table below the graph represent all frames seen, while the Captured frames are those that fall within the filter parameters.

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

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

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

Save to: By default, capture files are saved in the **Downloads** folder in the EtherScope file system, but you can also save them to a Micro SD card or USB storage device or choose a different folder by touching 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 will be 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 will change it throughout your unit.

Discovery App

The EtherScope nXG 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 Wi-Fi, Path Analysis, and connection tests.

Devices are discovered in the local broadcast domains where the EtherScope is physically connected, as well as other configured subnets. By default, discovery processes run out of all available **test and management ports**, wired and wireless.

Discovery Chapter Contents

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

Introduction to Discovery

Discovery finds, classifies, and displays—through Ethernet, fiber, and Wi-Fi—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.

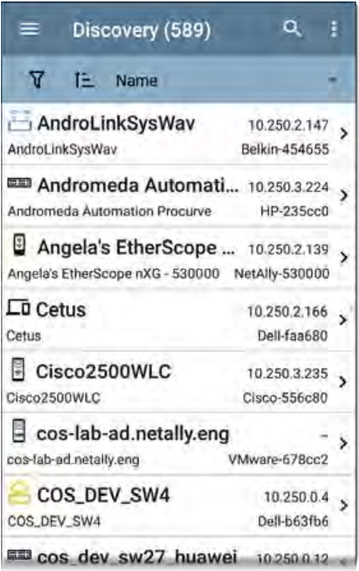
The EtherScope's discovery process begins when the unit is powered on. A channel scanning notification in the top Status Bar indicates that the EtherScope is scanning Wi-Fi channels to passively discover devices on the wireless network. Once a network connection (wired or Wi-Fi, test or management) is 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 EtherScope has discovered.



AndroLinkSysWav 10.250.2.147
AndroLinkSysWav Belkin-454655

Andromeda Automati... 10.250.3.224
Andromeda Automation Procurve HP-235cc0

Angela's EtherScope ... 10.250.2.139
Angela's EtherScope nXG - 530000 NetAlly-530000

Cetus 10.250.2.166
Cetus Dell-faa680

Cisco2500WLC 10.250.3.235
Cisco2500WLC Cisco-556c80

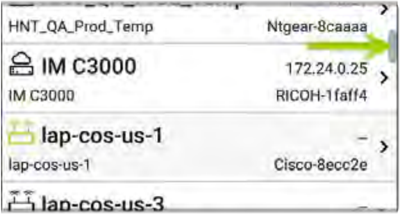
cos-lab-ad.netally.eng -
cos-lab-ad.netally.eng VMware-678cc2

COS_DEV_SW4 10.250.0.4
COS_DEV_SW4 Dell-b63fb6

cos_dev_sw27_huawei 10.250.0.12

Like in AutoTest and other EtherScope 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.



HNT_QA_Prod_Temp Ntgear-8caaaa

IM C3000 172.24.0.25

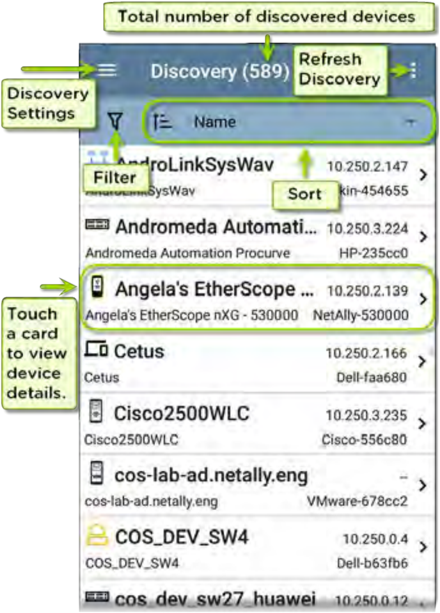
IM C3000 RICOH-1faff4

lap-cos-us-1 –

lap-cos-us-1 Cisco-8ecc2e

lap-cos-us-3 –

From the main Discovery screen, you can filter and sort the listed devices, open the left side navigation drawer to configure settings, and touch a device's card to view its details.



Total number of discovered devices

Refresh Discovery

Discovery Settings

Filter

Sort

Touch a card to view device details.

AndroLinkSysWav 10.250.2.147
AndroLinkSysWav kin-454655

Andromeda Automati... 10.250.3.224
Andromeda Automation Procurve HP-235cc0

Angela's EtherScope ... 10.250.2.139
Angela's EtherScope nXG - 530000 NetAlly-530000

Cetus 10.250.2.166
Cetus Dell-faa680

Cisco2500WLC 10.250.3.235
Cisco2500WLC Cisco-556c80

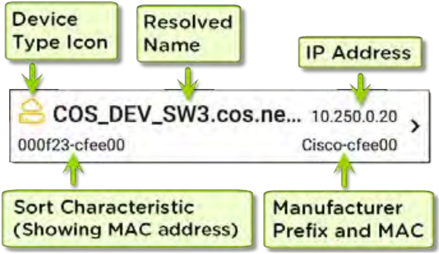
cos-lab-ad.netally.eng --
cos-lab-ad.netally.eng VMware-678cc2

COS_DEV_SW4 10.250.0.4
COS_DEV_SW4 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 EtherScope was able to discover.



COS_DEV_SW3.cos.ne... 10.250.0.20 ›

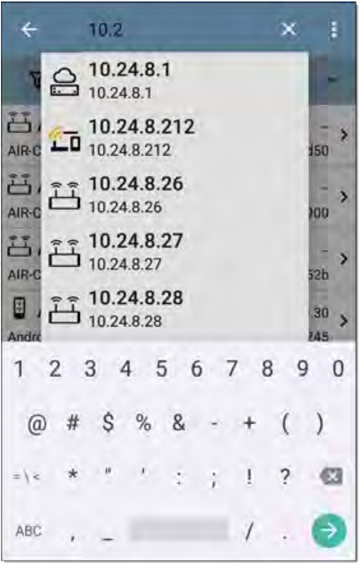
000f23-cfee00 Cisco-cfee00

Device Type Icon
Resolved Name
IP Address
Sort Characteristic (Showing MAC address)
Manufacturer Prefix and MAC

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.

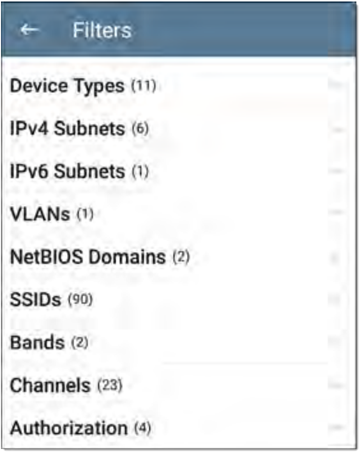
Searching the Discovery List

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

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



Device Types (11)

IPv4 Subnets (6)

IPv6 Subnets (1)

VLANs (1)

NetBIOS Domains (2)

SSIDs (90)

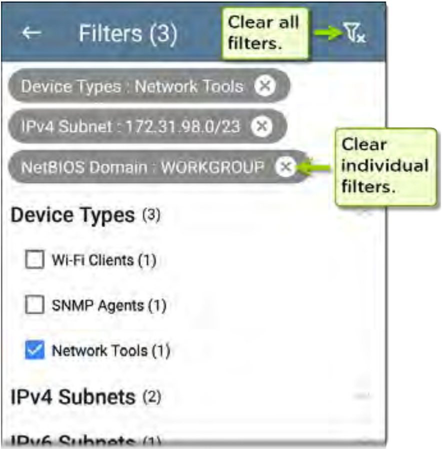
Bands (2)

Channels (23)

Authorization (4)

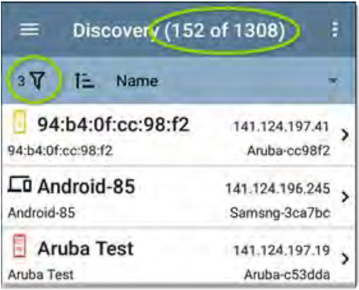
The Filters screen displays the number of devices or domains discovered for each category. Touch a category name to select filters by checking the boxes. The main Discovery screen will show only those devices or IDs that fall under your chosen filter parameters.

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



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

Once you have selected a filter, the Filters screen is also 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, Wi-Fi bands, etc. with a discovered Network Tool remain selectable in the filters list.



Discovery (152 of 1308)

94:b4:0f:cc:98:f2 — 141.124.197.41
94:b4:0f:cc:98:f2 — Aruba-cc98f2

Android-85 — 141.124.196.245
Android-85 — Samsng-3ca7bc

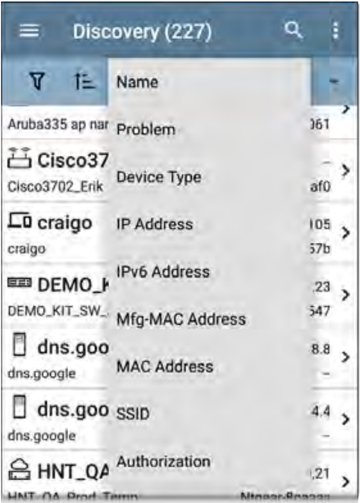
Aruba Test — 141.124.197.19
Aruba Test — Aruba-c53dda

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).

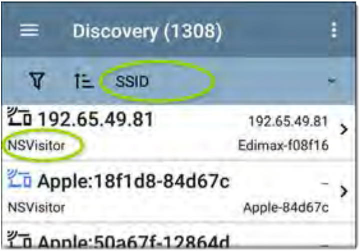
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

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.



192.65.49.81 — NSVisitor — 192.65.49.81 — Edimax-f08f16

Apple:18f1d8-84d67c — NSVisitor — – — Apple-84d67c

Apple:50a67f-12864d — –

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.

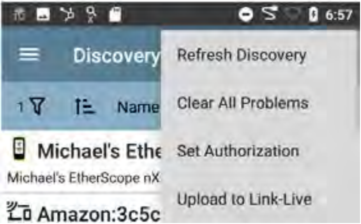
Security Auditing – Batch Authorization

Batch Authorization allows the user to extend the EtherScope nXG's filtering to organize devices into the following security categories:

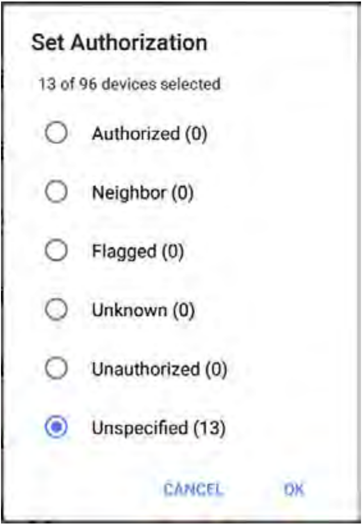
- **Authorized**: For devices approved for use on your network
- **Neighbor**: For devices owned and controlled by neighboring organizations
- **Flagged**: To give visibility to a specific device
- **Unknown**: For devices that have not been identified or classified
- **Unauthorized**: For devices that 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 will be 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. Once you have filtered 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

13 of 96 devices selected

○ Authorized (0)

○ Neighbor (0)

○ Flagged (0)

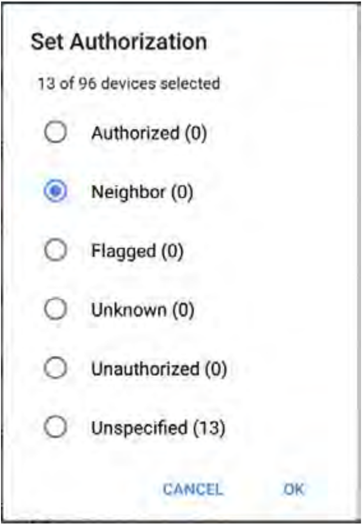
○ Unknown (0)

○ Unauthorized (0)

● Unspecified (13)

NOTE: The initial selection on this screen defaults to the category with the highest count. If other categories have non-zero counts, selecting **OK** will change 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)

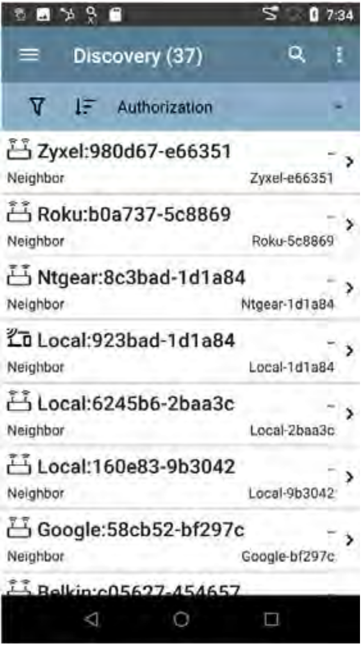
○ Flagged (0)

○ Unknown (0)

○ Unauthorized (0)

○ Unspecified (13)

You will now be able to sort the list of discovered devices and clearly identify the security category of the devices. Devices from other offices will be identified as: Neighbor



Zyxel:980d67-e66351 –
Neighbor Zyxel-e66351

Roku:b0a737-5c8869 –
Neighbor Roku-5c8869

Ntgear:8c3bad-1d1a84 –
Neighbor Ntgear-1d1a84

Local:923bad-1d1a84 –
Neighbor Local-1d1a84

Local:6245b6-2baa3c –
Neighbor Local-2baa3c

Local:160e83-9b3042 –
Neighbor Local-9b3042

Google:58cb52-bf297c –
Neighbor Google-bf297c

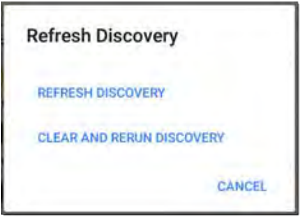
Belkin:c05627-454657

See Assigning a Name and Authorization to a Device for more information on the Authorization feature.

> NOTE: Batch Authorization operates on the default MAC address of a device. If a device has multiple MACs, authorization will only be set 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

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

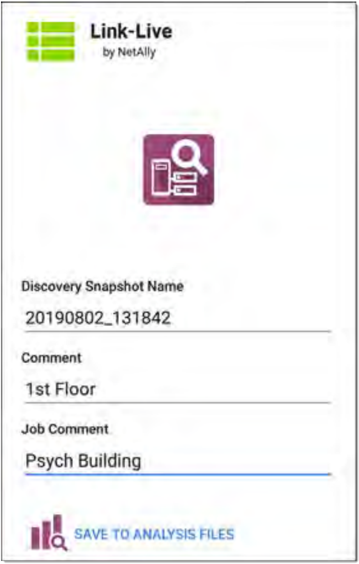


REFRESH DISCOVERY restarts the active discovery process without clearing the already discovered devices.

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

Uploading Discovery Results to Link-Live

Touch 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.



Discovery Snapshot Name

20190802_131842

Comment

1st Floor

Job Comment

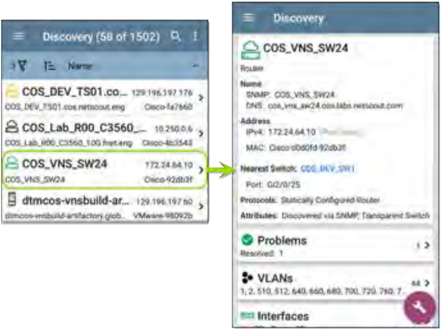
Psych Building

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.



Discovery (59 of 1502)

Name

COS_DEV_TS01.co... 129.196.197.176
COS_DEV_TS01.cos.netscout.eng Cisco-fa7660

COS_Lab_R00_C3560_... 10.250.0.6
COS_Lab_R00_C3560_10G.fnet.eng Cisco-4b3543

COS_VNS_SW24 172.24.64.10
COS_VNS_SW24 Cisco-92db3f

dtmcos-vnsbuild-ar... 129.196.197.60
dtmcos-vnsbuild-artifactory.glob... VMware-9B092b

Discovery

COS_VNS_SW24

Router

Name
SNMP: COS_VNS_SW24
DNS: cos_vns_sw24.cos.labs.netscout.com

Address
IPv4: 172.24.64.10
MAC: Cisco:d0d0fd:92db3f

Nearest Switch: COS_DEV_SW1
Port: Gi2/0/25

Protocols: Statically Configured Router

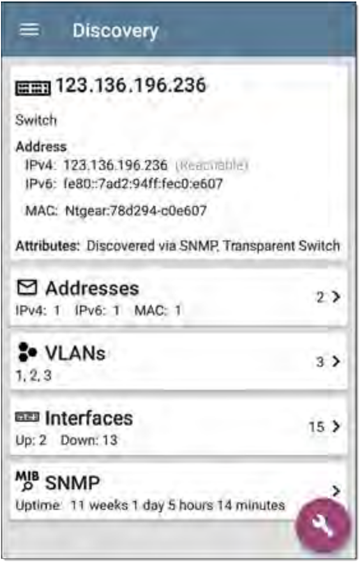
Attributes: Discovered via SNMP, Transparent Switch

Problems 1
Resolved: 1

VLANs 44
1, 2, 510, 512, 640, 660, 680, 700, 720, 760, 7...

Interfaces

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



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

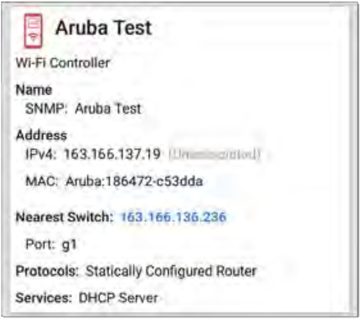
For the Switch screen shown above, Discovery was able to find an IP address but not a name for the switch.

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

See Device Types for specifics about the different devices the EtherScope 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 (Un[illegible])
MAC: Aruba:186472-c53dda

Nearest Switch: 163.166.136.236
Port: g1

Protocols: Statically Configured Router

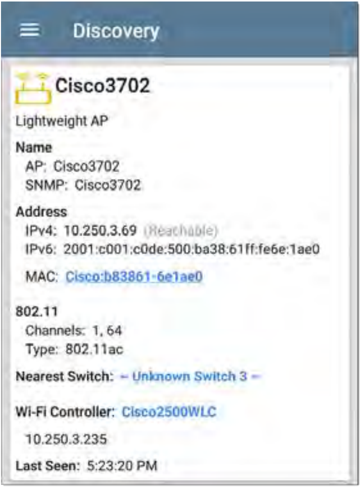
Services: DHCP Server

The top of the card shows the device type 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 EtherScope can discover about the device.

On the Discovery Details screens, you can touch any **blue linked name or address** to open a Discovery or Wi-Fi Analysis 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 (in this case Wi-Fi).



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 linked and underlined Cisco MAC address in the screen image above opens the Wi-Fi app's AP Details screen, where you can view the other wireless attributes associated with the Lightweight AP. 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 EtherScope 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.

802.11: Wireless data

> **Channels**: Wi-Fi channels on which the device is operating
>
> **Type(s)**: 802.11 media type(s) supported by the 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

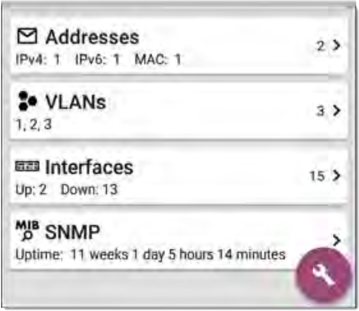
Virtual Machine: Name of the virtual machine

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

Last Seen: Time at which EtherScope 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.



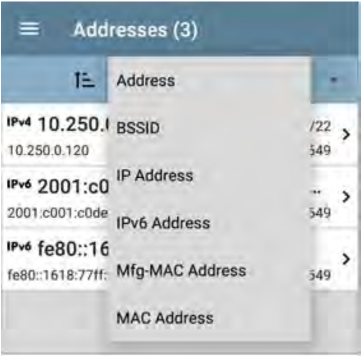
Addresses 2 >
IPv4: 1 IPv6: 1 MAC: 1

VLANs 3 >
1, 2, 3

Interfaces 15 >
Up: 2 Down: 13

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

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

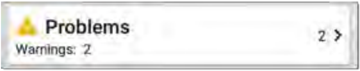


The rest of this topic provides examples of each type of Details screen and options for additional analysis.

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

Problems

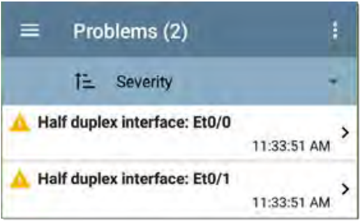
The Problems card shows the icon color of the highest severity problem, and the number of detected **Warning**, **Failure or Error**, **Information**, and **Resolved** conditions for the device or network component.



Problems

Warnings: 2

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).



Problems (2)

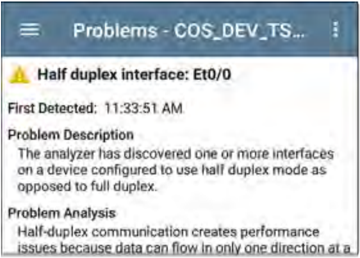
Severity

Half duplex interface: Et0/0 11:33:51 AM

Half duplex interface: Et0/1 11:33:51 AM

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, touch a Problem's row to read a detailed description.



⚠ Half duplex interface: Et0/0

First Detected: 11:33:51 AM

Problem Description

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

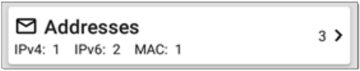
Problem Analysis

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

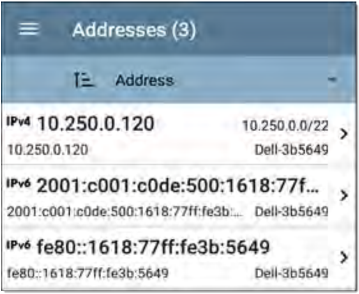
Touch the action overflow button ⋮ at the top right of the Problem list or description screen to **Clear Problems**.

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

Addresses



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



Addresses (3)

Address

IPv4 10.250.0.120 10.250.0.0/22
10.250.0.120 Dell-3b5649

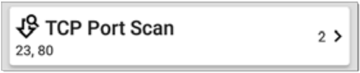
IPv6 2001:c001:c0de:500:1618:77f...
2001:c001:c0de:500:1618:77ff:fe3b:... Dell-3b5649

IPv6 fe80::1618:77ff:fe3b:5649
fe80::1618:77ff:fe3b:5649 Dell-3b5649

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

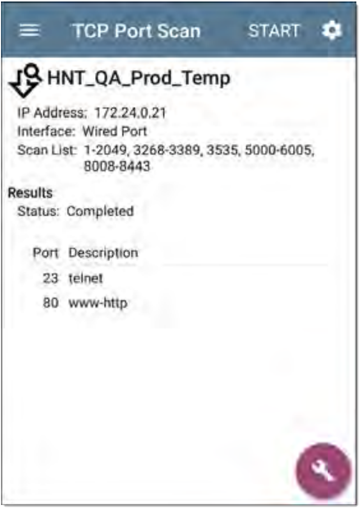
If you have run a TCP Port Scan (from the Discovery FAB) on a device or IP address, a TCP Port Scan card appears on the device's Details screen.



TCP Port Scan
23, 80
2 >

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.



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

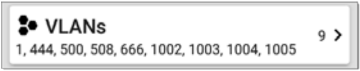
Results

> **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.

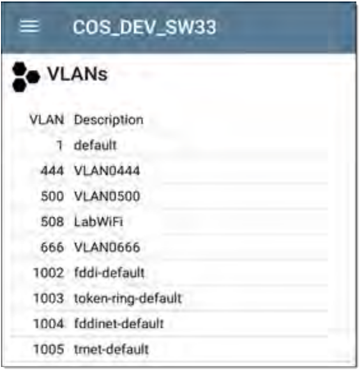


VLANs

1, 444, 500, 508, 666, 1002, 1003, 1004, 1005

9 >

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



COS_DEV_SW33

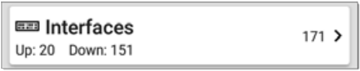
VLANs

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.



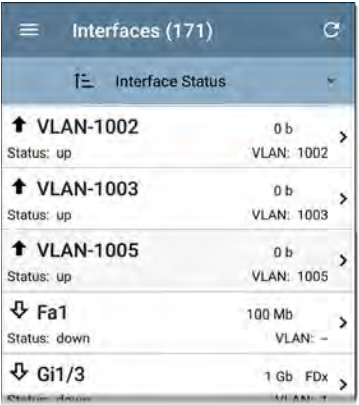
Interfaces

Up: 20 Down: 151

171 >

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)

Interface Status

↑ VLAN-1002 0 b
Status: up VLAN: 1002

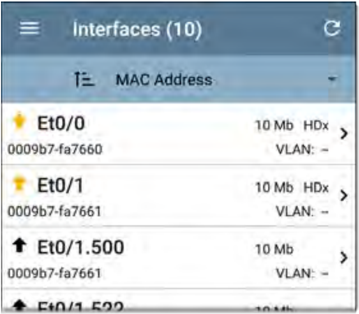
↑ VLAN-1003 0 b
Status: up VLAN: 1003

↑ VLAN-1005 0 b
Status: up VLAN: 1005

⇩ Fa1 100 Mb
Status: down VLAN: –

⇩ Gi1/3 1 Gb FDx

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.

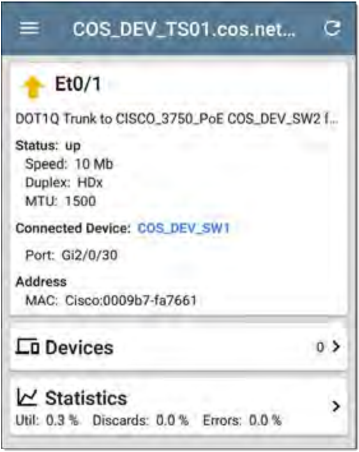


Et0/0 10 Mb HDx
0009b7-fa7660 VLAN: –

Et0/1 10 Mb HDx
0009b7-fa7661 VLAN: –

Et0/1.500 10 Mb
0009b7-fa7661 VLAN: –

Touching an Interface row opens a new Discovery Details screen for the selected Interface.



Et0/1

DOT1Q Trunk to CISCO_3750_PoE COS_DEV_SW2 f...

Status: up
Speed: 10 Mb
Duplex: HDx
MTU: 1500

Connected Device: COS_DEV_SW1
Port: Gi2/0/30

Address
MAC: Cisco:0009b7-fa7661

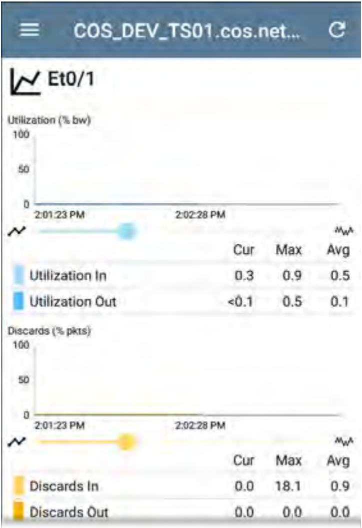
Devices 0

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

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 touch the lower cards to review any discovery **VLANs** and **Devices** for the Interface as well as graphs of the Interface **Statistics**.

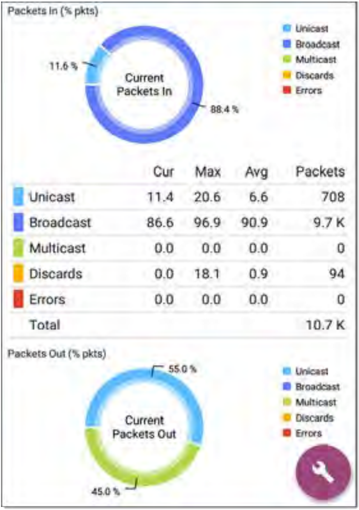


	Cur	Max	Avg
Utilization In	0.3	0.9	0.5
Utilization Out	<0.1	0.5	0.1

	Cur	Max	Avg
Discards In	0.0	18.1	0.9
Discards Out	0.0	0.0	0.0

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.



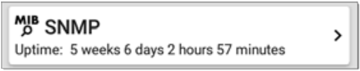
Packets In (% pkts)

	Cur	Max	Avg	Packets
🟦 Unicast	11.4	20.6	6.6	708
🟦 Broadcast	86.6	96.9	90.9	9.7 K
🟩 Multicast	0.0	0.0	0.0	0
🟧 Discards	0.0	18.1	0.9	94
🟥 Errors	0.0	0.0	0.0	0
Total				10.7 K

Packets Out (% pkts)

SNMP

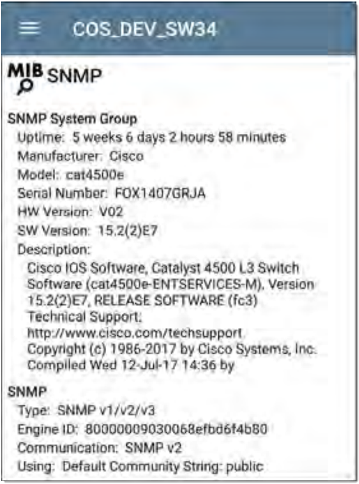
This card shows device details gathered via SNMP and SNMP connectivity to the device.



SNMP

Uptime: 5 weeks 6 days 2 hours 57 minutes

The SNMP card displays the SNMP Uptime. Touch the card for SNMP Details.



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

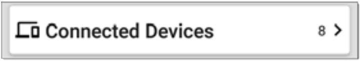
SNMP
Type: SNMP v1/v2/v3
Engine ID: 80000009030068efbd6f4b80
Communication: SNMP v2
Using: Default Community String: public

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

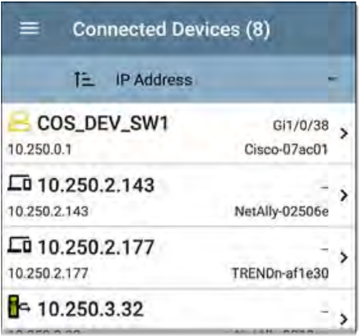
SNMP: SNMP versions the device supports, Engine ID (for v3), and how the EtherScope is currently communicating with the device, along with credentials, including the Community String in use

Connected Devices

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



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



Connected Devices (8)

IP Address

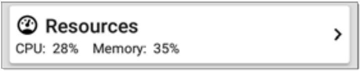
COS_DEV_SW1 Gi1/0/38
10.250.0.1 Cisco-07ac01

10.250.2.143 –
10.250.2.143 NetAlly-02506e

10.250.2.177 –
10.250.2.177 TRENDn-af1e30

10.250.3.32 –

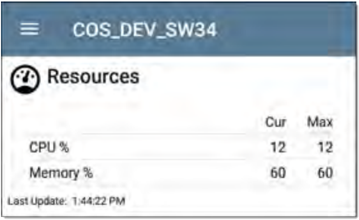
Resources



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.

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



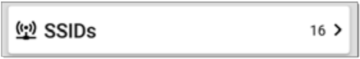
	Cur	Max
CPU %	12	12
Memory %	60	60

Last Update: 1:44:22 PM

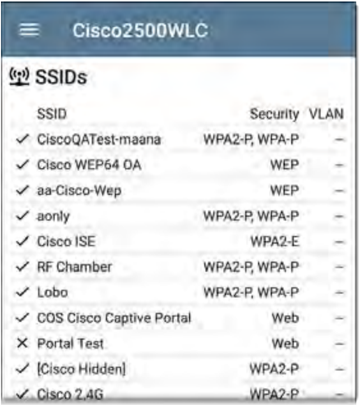
By default, EtherScope displays a **Warning** condition if CPU, Memory, or Storage utilization is above 90%. You can adjust problem detection and thresholds in the Wired Problem Settings accessed from the Discovery navigation drawer.

SSIDs

The SSIDs card appears in the Details for Wi-Fi Controllers. This information is gathered via SNMP.


SSIDs 16 >

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



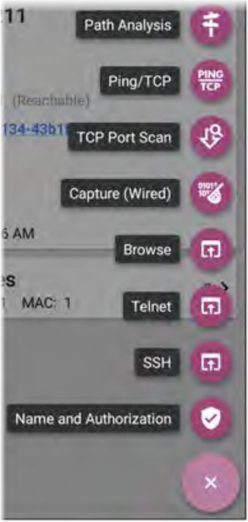
Cisco2500WLC

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.

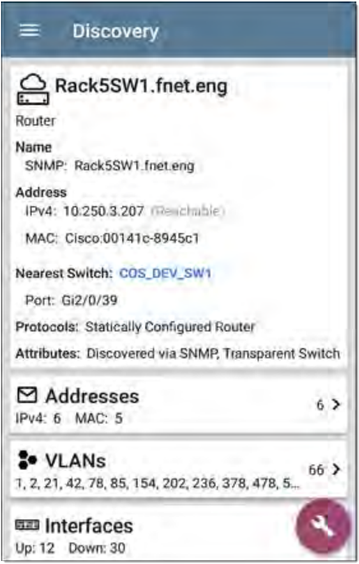
Opening other NetAlly apps, such as Path Analysis, Ping/TCP, or Capture, from a Details screen will auto-populate the new app with the device's name and/or address. In this way, both the Discovery and Wi-Fi apps provide a helpful shortcut and prevent you from needing to type in target addresses or hostnames in other testing apps.

- Touching TCP Port Scan opens the TCP Port Scan screen in the Discovery app.
- Selecting **Browse** opens Google Chrome.
- **Telnet** or **SSH** open the JuiceSSH app.
- For devices with a MAC address or BSSID, touching **Name and Authorization** opens a dialog where you can assign a custom user name and Authorization status. See Assigning a Name and Authorization to a Device in the Wi-Fi chapter.

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 touching the Addresses card).



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

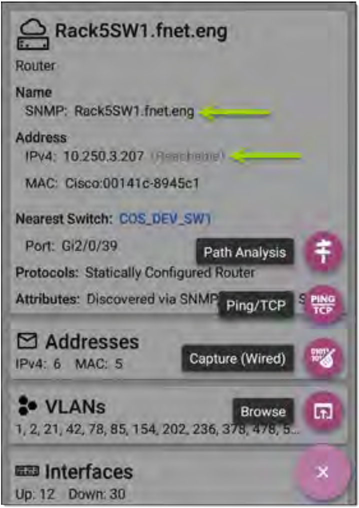
Attributes: Discovered via SNMP, Transparent Switch

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 a user opens the FAB and selects a different app, such as Path Analysis, only the address and name listed at the top of the Details screen will be 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

Nearest Switch: COS_DEV_SW1

Port: Gi2/0/39

Protocols: Statically Configured Router

Attributes: Discovered via SNMP

Addresses

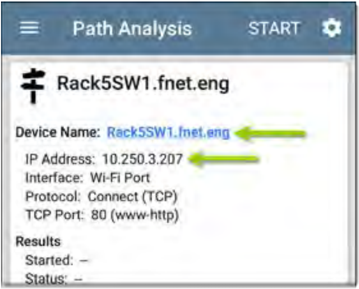
IPv4: 6 MAC: 5

VLANs

1, 2, 21, 42, 78, 85, 154, 202, 236, 378, 478, 5...

Interfaces

Up: 12 Down: 30



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 EtherScope depending on the device type, how it was discovered, and your configured settings.

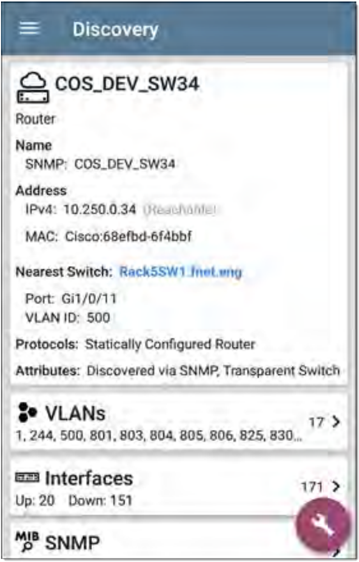
See Discovery Settings for SNMP Configuration and Devices Discovered Through Other Devices options.

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 may display for each device type.

Routers

EtherScope 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...

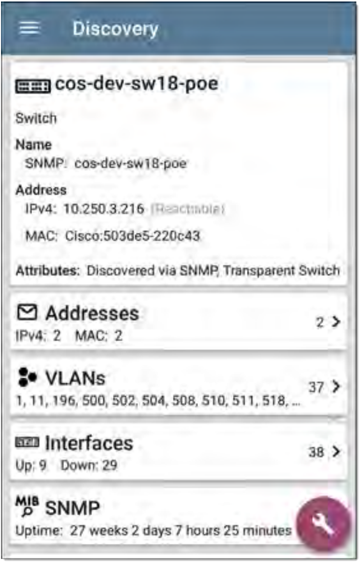
Interfaces 171 >

Up: 20 Down: 151

SNMP

Switches

Switches are also discovered by monitoring traffic and querying hosts.



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, ...

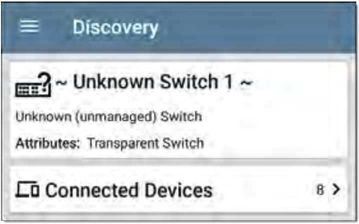
Interfaces 38 >
Up: 9 Down: 29

SNMP
Uptime: 27 weeks 2 days 7 hours 25 minutes

Unknown Switches

Unknown switches are detected indirectly based on analysis of the traffic going through surrounding switches. Though the EtherScope cannot identify the switch itself, it can sense where a switch is active on the network via the device MAC addresses in that space.

Unknown Switches are numbered by the EtherScope as they are discovered. These numbers may change the next time the discovery process runs.



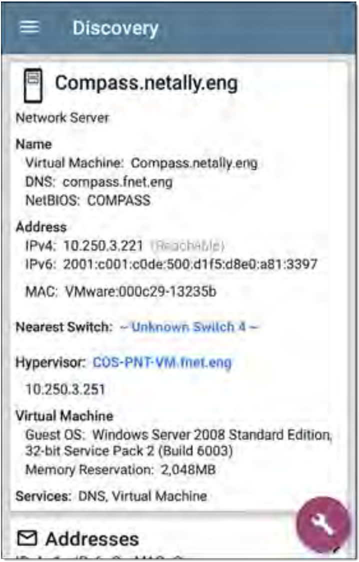
Unknown (unmanaged) Switch

Attributes: Transparent Switch

The Unknown Switches Details screen shows the number of devices connected to the switch and allows you to view the devices that are connected by tapping the Connected Devices card. The connected devices provide clues about where the unknown switch may be located.

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

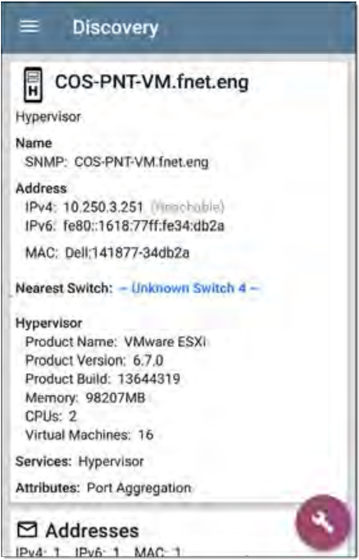
Virtual Machine
Guest OS: Windows Server 2008 Standard Edition, 32-bit Service Pack 2 (Build 6003)
Memory Reservation: 2,048MB

Services: DNS, Virtual Machine

Addresses

Hypervisors

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



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

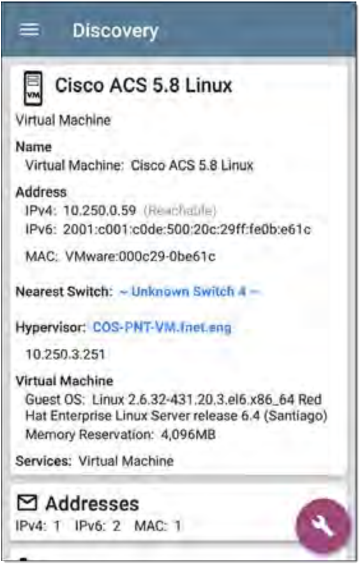
Services: Hypervisor

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.



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

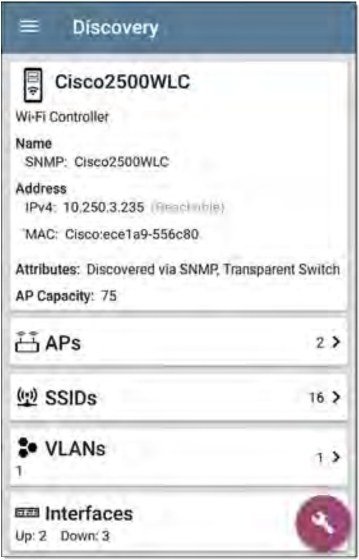
Virtual Machine
Guest OS: Linux 2.6.32-431.20.3.el6.x86_64 Red Hat Enterprise Linux Server release 6.4 (Santiago)
Memory Reservation: 4,096MB

Services: Virtual Machine

Addresses
IPv4: 1 IPv6: 2 MAC: 1

Wi-Fi Controllers

EtherScope 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 >

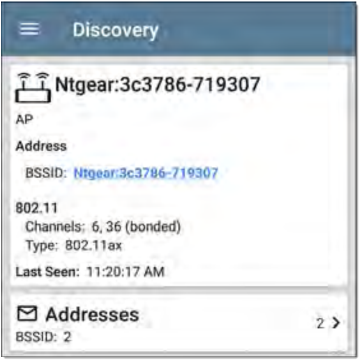
SSIDs 16 >

VLANs 1 >
1

Interfaces
Up: 2 Down: 3

Access Points (APs)

The EtherScope discovers APs through wireless packet analysis and SNMP queries via the wired side of the network.



Ntgear:3c3786-719307

AP

Address

BSSID: Ntgear:3c3786-719307

802.11

Channels: 6, 36 (bonded)

Type: 802.11ax

Last Seen: 11:20:17 AM

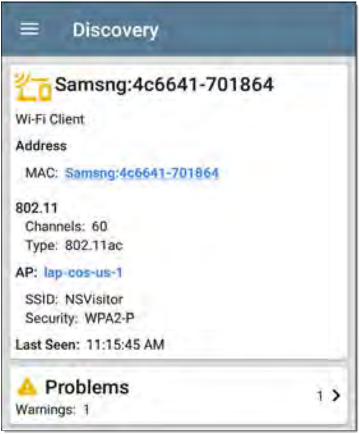
Addresses 2

BSSID: 2

See also APs in the Wi-Fi analysis app.

Wi-Fi Clients

Wireless clients are discovered through wireless packet analysis and SNMP queries through the wired side of the network.



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

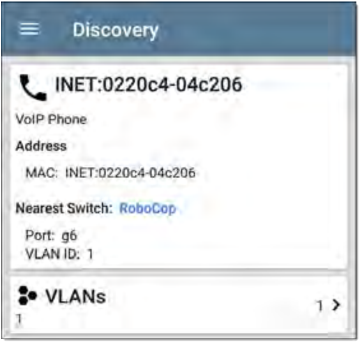
Problems 1

Warnings: 1

See also Clients in the Wi-Fi analysis app.

VoIP Phones

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



☎ INET:0220c4-04c206

VoIP Phone

Address

MAC: INET:0220c4-04c206

Nearest Switch: RoboCop

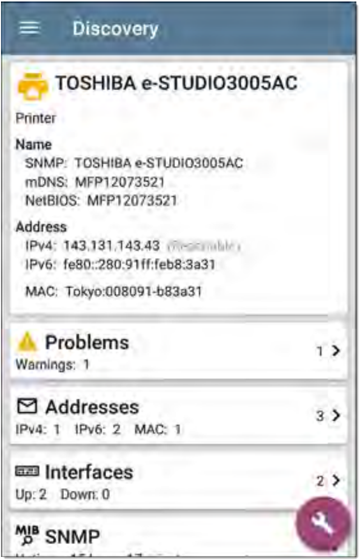
Port: g6
VLAN ID: 1

VLANs
1

1 >

Printers

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



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

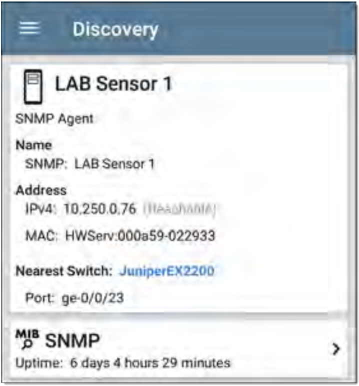
Interfaces 2 >
Up: 2 Down: 0

SNMP

SNMP Agents

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

> NOTE: If EtherScope 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.



LAB Sensor 1

SNMP Agent

Name
SNMP: LAB Sensor 1

Address
IPv4: 10.250.0.76 [illegible]
MAC: HWServ:000a59-022933

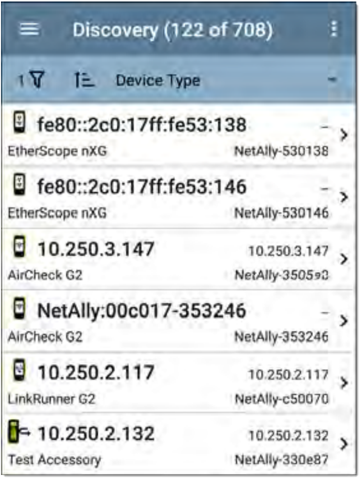
Nearest Switch: JuniperEX2200
Port: ge-0/0/23

SNMP
Uptime: 6 days 4 hours 29 minutes

See also SNMP Details.

NetAlly Tools

The EtherScope can also identify other NetAlly network testers, including EtherScopes, AirCheck G2s, OneTouches, LinkRunners (AT and G2), and Test Accessories.



Discovery (122 of 708)

1 Device Type

fe80::2c0:17ff:fe53:138 –
EtherScope nXG NetAlly-530138

fe80::2c0:17ff:fe53:146 –
EtherScope nXG NetAlly-530146

10.250.3.147 10.250.3.147
AirCheck G2 NetAlly-3505a0

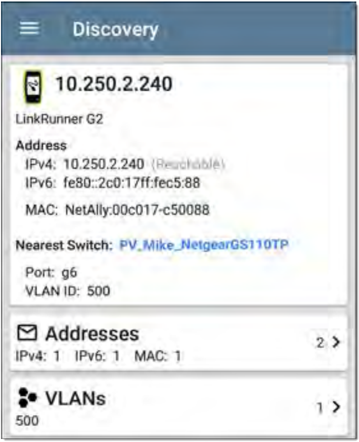
NetAlly:00c017-353246 –
AirCheck G2 NetAlly-353246

10.250.2.117 10.250.2.117
LinkRunner G2 NetAlly-c50070

10.250.2.132 10.250.2.132
Test Accessory NetAlly-330e87

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

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



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

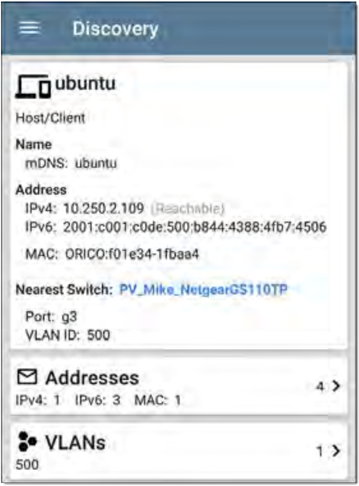
IPv4: 1 IPv6: 1 MAC: 1

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.



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

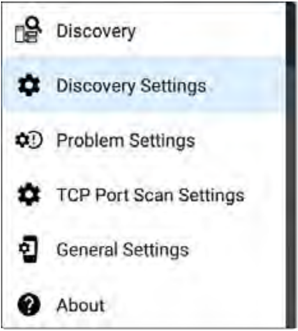
Addresses
IPv4: 1 IPv6: 3 MAC: 1 4 >

VLANs
500 1 >

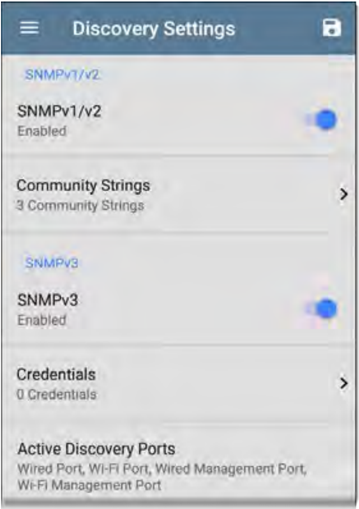
Discovery Settings

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**.



(Touch here to skip to Problem Settings, TCP Port Scan, or back to General Settings.)



Discovery Settings

SNMPv1/v2

SNMPv1/v2
Enabled

Community Strings
3 Community Strings

SNMPv3

SNMPv3
Enabled

Credentials
0 Credentials

Active Discovery Ports
Wired Port, Wi-Fi Port, Wired Management Port, Wi-Fi Management Port

To adjust Discovery Settings:

1. On the **Discovery Settings** screen, touch 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.

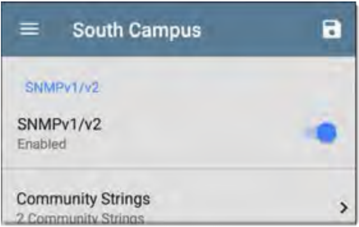
3. Then, Refresh Discovery from the action overflow menu ⋮ to apply the new configuration.

You can load, save, import, and export configured Discovery settings by touching 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**: Create an export file of the 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.



South Campus

SNMPv1/v2

SNMPv1/v2
Enabled

Community Strings
2 Community Strings

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

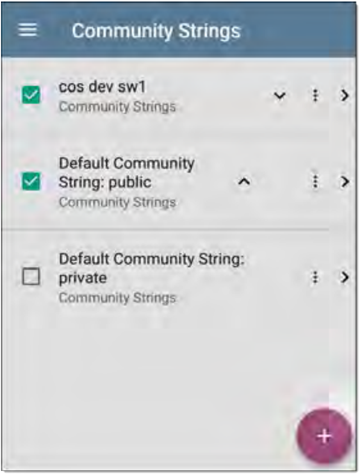
SNMP credentials are required to communicate with the SNMP agents on your interconnect devices, such as switches and routers. The Discovery Settings allow you to enter the SNMP community strings and credential sets the EtherScope uses to communicate with those devices.

SNMPv1/v2

Touch 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

Touch this field to open the Community Strings list screen and add, edit, or remove community strings.



Community Strings

☑ cos dev sw1
Community Strings

☑ Default Community String: public
Community Strings

☐ Default Community String: private
Community Strings

The EtherScope 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 EtherScope uses the strings to query a device.
- Touch the action overflow icon ⋮ to **Duplicate** or **Delete** a Community String. **CAUTION**: When you delete a string, you delete it from all saved Discovery configurations. To remove a string from those used by the current Discovery configuration, simply uncheck it.
- Touch the FAB ⊕ to add new Community Strings.
- Touch 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.

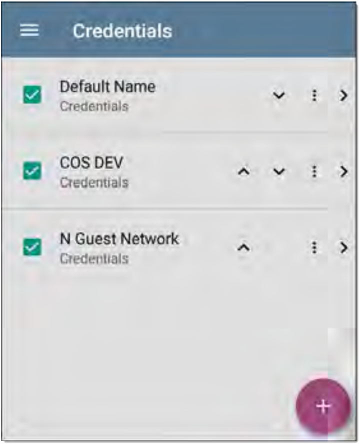
SNMPv3

Touch 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 EtherScope will discover the engine IDs of all SNMPv3 agents. This is a good way to discover if a device support SNMPv3.

Credentials

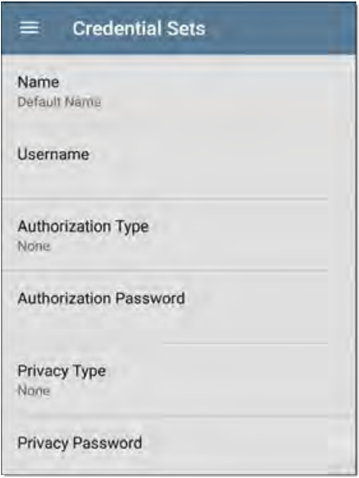
Touch this field to open the Credentials list screen.



This screen interface works like the Community Strings screen above. EtherScope 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.
- Touch a row to edit its credentials.

- Touch 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

Touch the **Name** field to enter a custom name for the Credential Set.

Username

Touch to enter the SNMPv3 username.

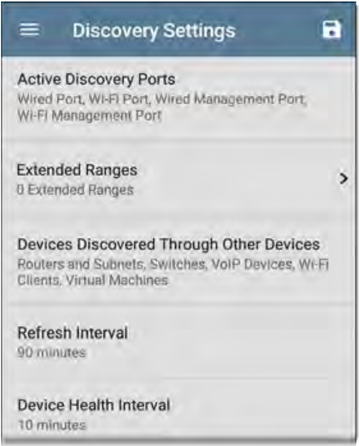
Authorization Type and Password

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

Privacy Type and Password

EtherScope Discovery supports four Privacy Types: CBC-DES, AES-128, AES-192, AND AES-256. If needed, enter the appropriate Privacy Password.

Back to Title and Contents



Active Discovery Ports
Wired Port, Wi-Fi Port, Wired Management Port, Wi-Fi Management Port

Extended Ranges
0 Extended Ranges

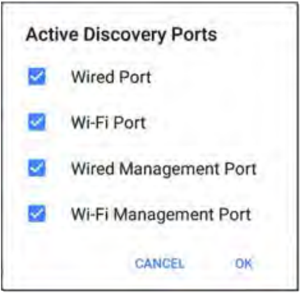
Devices Discovered Through Other Devices
Routers and Subnets, Switches, VoIP Devices, Wi-Fi Clients, Virtual Machines

Refresh Interval
90 minutes

Device Health Interval
10 minutes

Active Discovery Ports

Touch Active Discovery Ports to select the port Discovery uses to gather data. Discovery only runs through the enabled ports if an active network link is available.



Active Discovery Ports

☑ Wired Port

☑ Wi-Fi Port

☑ Wired Management Port

☑ Wi-Fi Management Port

Discovery uses all of the ports by default. Uncheck them to limit which ports are used.

> NOTE: The top two Wired and Wi-Fi Ports refer to the Test ports. An AutoTest Wired or Wi-Fi Profile must run to establish test port links. The last listed Wired Profile runs automatically when you start up the EtherScope if a connection is available.

See also Test and Management Ports.

Extended Ranges

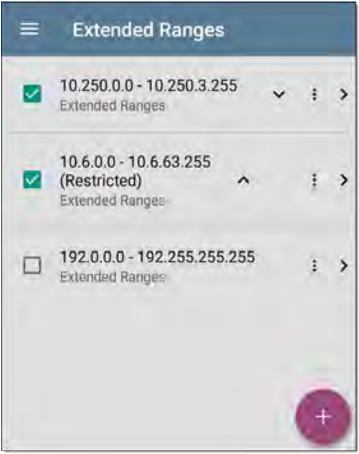
The Extended Ranges screen allows you to enter addresses of non-local subnets on which you want the Discovery process to run. Discovery sweeps all of the enabled Extended Ranges for devices, whether directly connected or off-net. The EtherScope performs Ping sweeps on subnets that are not directly connected 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 EtherScope always discovers management subnets, regardless of your network port connections.

Touch the field to open the Extended Ranges list screen.



Extended Ranges

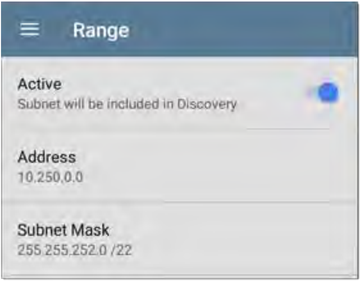
☑ 10.250.0.0 - 10.250.3.255
Extended Ranges

☑ 10.6.0.0 - 10.6.63.255 (Restricted)
Extended Ranges

□ 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).

- Touch any Extended Range's row to edit its address and subnet.
- Touch the FAB ⊕ to add new extended ranges.



Range

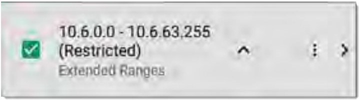
Active
Subnet will be included in Discovery

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 EtherScope will *not* communicate with devices within the restricted range.

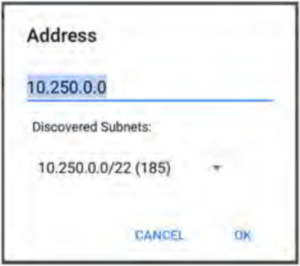


☑ 10.6.0.0 - 10.6.63.255 (Restricted)
Extended Ranges

- 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)

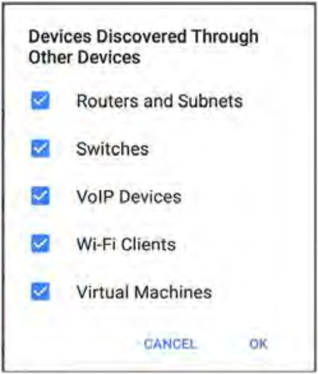
Tap the drop-down menu to select a previously Discovered Subnet. The Address field will be automatically populated with your selection.

Subnet Mask

Touch this field to select a subnet mask. If you select an already Discovered Subnet, the Subnet Mask is also pre-populated.

Devices Discovered Through Other Devices

By default, EtherScope 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

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, and the process will run from that router and find 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 EtherScope is reading the CDP and LLDP caches of one switch, it will contain other switches. If this option is enabled, the EtherScope 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 will add 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.

Wi-Fi Clients

When the Wi-Fi Clients checkbox is enabled, discovery will add any wireless clients it finds in SNMP tables of APs and Wireless LAN Controllers. Enabling this option along with

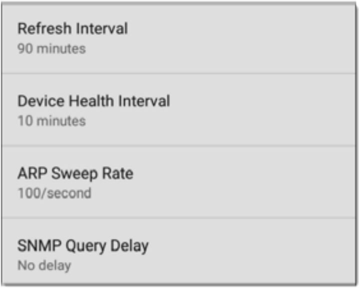
Switches provides best chance of finding all Wi-Fi clients.

> NOTES: Enabling Wi-Fi Clients here may cause Wi-Fi devices to show in Discovery that do not appear in the Wi-Fi analysis app because Wi-Fi analysis only shows what it detects on wirelessly transmitted packets.

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.

Back to Title and Contents



Refresh Interval
90 minutes

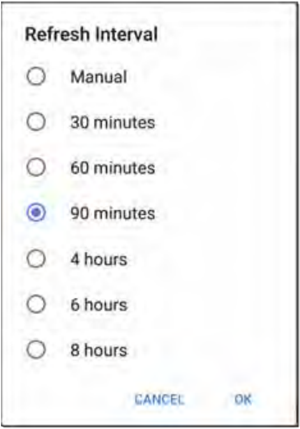
Device Health Interval
10 minutes

ARP Sweep Rate
100/second

SNMP Query Delay
No delay

Refresh Interval

This setting controls the time between runs of the Discovery process. By default, Discovery runs every 90 minutes. Touch the **Refresh Interval** field to select a different interval, up to 8 hours.



Refresh Interval

○ Manual

○ 30 minutes

○ 60 minutes

● 90 minutes

○ 4 hours

○ 6 hours

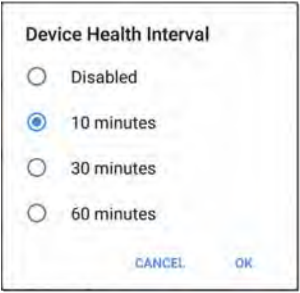
○ 8 hours

The **Manual** option turns off regular automatic Discovery, and the process will only refresh if you select **Refresh Discovery** from the main Discovery list screen.

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. Touch the field to disable Device Health testing or to change the interval from the default of 10 minutes to 30 or 60 minutes.



Device Health Interval

○ Disabled

● 10 minutes

○ 30 minutes

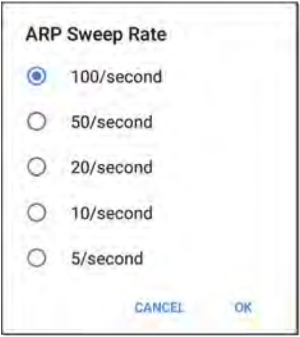
○ 60 minutes

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

See also Problem Settings.

ARP Sweep Rate

Touch the ARP Sweep Rate field to select a rate between 5 and 100 ARP requests per second.



ARP Sweep Rate

● 100/second

○ 50/second

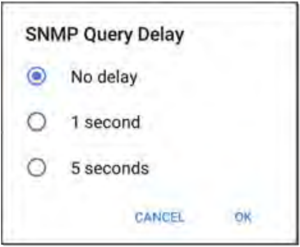
○ 20/second

○ 10/second

○ 5/second

This setting can prevent the EtherScope from shutting down ports that sense too many ARPs are being sent.

SNMP Query Delay



SNMP Query Delay

● No delay

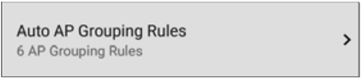
○ 1 second

○ 5 seconds

This function controls how long your EtherScope 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 EtherScope asks for more data as soon as a response has been received. You can select a 1 or 5 second delay if needed.

Auto AP Grouping Rules

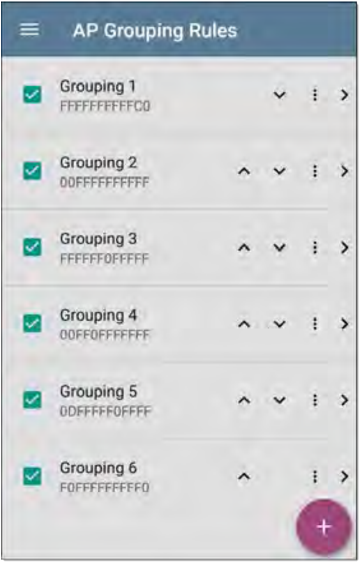


Auto AP Grouping Rules
6 AP Grouping Rules

This feature allows you to adjust the AP Grouping Rules that control how the EtherScope groups BSSIDs with their Access Points, such that they are grouped appropriately for your AP types and environment.

For example, if BSSIDs from different APs are being grouped together inaccurately, you can disable the rule that is causing the grouping. If your AP manufacturer uses a BSSID variation scheme that is not covered by one of the six default rules, you can add a new rule.

Touch the setting to open the AP Grouping Rules list screen. The image below shows the six default AP Grouping Rules on the EtherScope. The **Prefix filters** in all of the default grouping rules are set to 000000-000000.



AP Grouping Rules

☑ Grouping 1
FFFFFFFFFFC0

☑ Grouping 2
00FFFFFFFFFF

☑ Grouping 3
FFFFFF0FFFFF

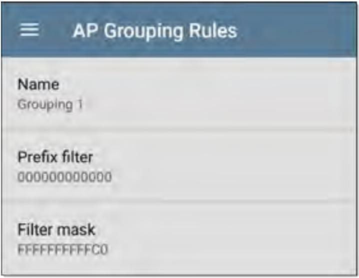
☑ Grouping 4
00FF0FFFFFFF

☑ Grouping 5
0DFFFFF0FFFF

☑ Grouping 6
F0FFFFFFFFF0

As with other settings list screens on the EtherScope, you can enable or disable, add, delete, and edit the grouping rules from this screen.

- Check or uncheck the boxes to include or exclude a rule from use in the current Discovery configuration.
- Touch the action overflow icon ⋮ to **Duplicate** or **Delete** a rule.
  CAUTION: When you delete a rule, you delete it from all saved Discovery configurations. To remove a rule from those used by the current Discovery configuration, simply uncheck it.
- Touch the FAB ⊕ to add a new rule.
- Touch any rule's row to edit it.



☰ AP Grouping Rules

Name
Grouping 1

Prefix filter
000000000000

Filter mask
FFFFFFFFFFC0

Name

If desired, enter a custom name for a default or new rule. If you intend to use a Prefix filter, a best practice would be to name the rule with the AP manufacturer's name.

Prefix filter

Use the **Prefix filter** to create a rule for a specific AP manufacturer's BSSID scheme, meaning a rule for just one AP manufacturer prefix. The default rules all contain a default Prefix filter of 000000-000000.

If a Prefix filter is non-zero, its second and third bytes are compared to discovered BSSIDs before the **Filter mask** (described below) is applied. These two bytes must match exactly, or the two BSSIDs are not grouped together. This behavior allows you to specify a fairly open Filter mask, as the mask will only be applied to one manufacturer.

For example, you could have Cisco APs whose BSSIDs all start with b83861. By specifying a Prefix filter of 003861-000000, you limit the grouping rule to just those APs.

Filter mask

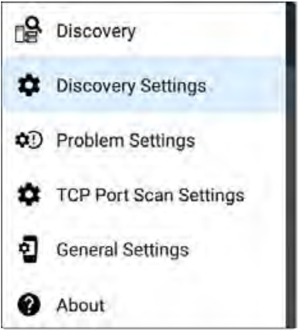
The Filter mask specifies what parts of the BSSIDs are compared when determining AP groupings.

For example, default **Grouping Rule 1** has a Filter mask of FFFFFF-FFFFC0, so any BSSIDs that vary only by the lower six bits will be grouped together.

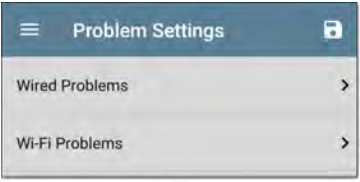
Problem Settings

The Problem settings determine which issues are detected and displayed by *both* the Discovery and Wi-Fi Analysis apps 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**.



(Touch here to go to Discovery Settings or back to General Settings.)

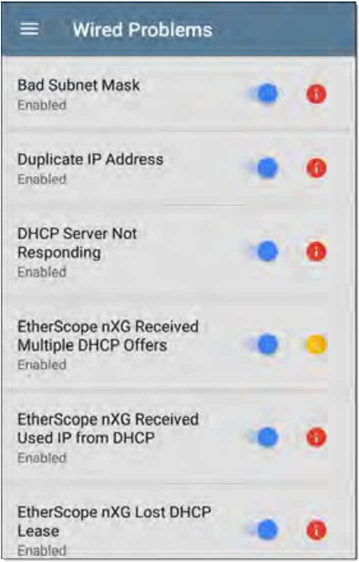


Problems are categorized as Wired or Wi-Fi.

> NOTE: The Wi-Fi Problems configured here also control the Problems detected and displayed in the Wi-Fi Analysis app.

As with Discovery Settings, you can save, load, import, and export configured Problem Settings by touching the save button 💾 on this screen. See Managing Testing App Settings for more instructions.

Problems are categorized as Wired or Wi-Fi. Tap the row for each to enable or disable the problem types and set thresholds where applicable.



Wired Problems

Bad Subnet Mask
Enabled

Duplicate IP Address
Enabled

DHCP Server Not Responding
Enabled

EtherScope nXG Received Multiple DHCP Offers
Enabled

EtherScope nXG Received Used IP from DHCP
Enabled

EtherScope nXG Lost DHCP Lease
Enabled

All Problem types are enabled by default. Tap the toggle button to the right to disable each one.

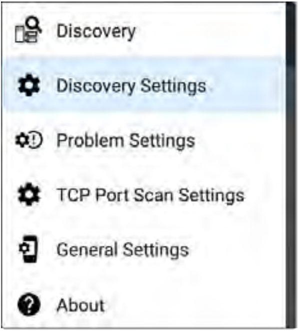
Touch the red ⓘ , yellow ⓘ, or blue ⓘ information icons to the right of each Problem to read a detailed description and recommended actions. **Red** icons indicate Failure conditions and **yellow** indicate Warning conditions. **Blue** icons are simply informational.

When you finish configuring, tap the back button ◁ to return to the main Discovery screen.

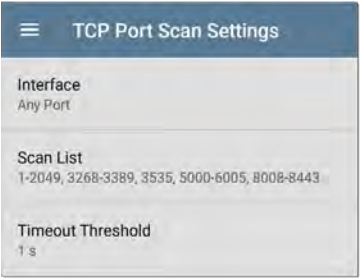
TCP Port Scan Settings

The TCP Port Scan feature checks for open ports on the current device from the Discovery Details screen's FAB. The EtherScope 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 tapping the menu icon ☰ in the Discovery app.



Select **TCP Port Scan Settings**.



TCP Port Scan Settings

Interface
Any Port

Scan List
1-2049, 3268-3389, 3535, 5000-6005, 8008-8443

Timeout Threshold
1 s

Interface

This setting determines the EtherScope port from which the port scan runs. Touch the field to select Any Port, Wired or Wi-Fi Test Port, or Wired or Wi-Fi Management Port. See Test and Management Ports for explanations of the different ports.

Scan List

This setting contains the port numbers that are tested during the port scan. Tap the field to enter different port numbers, or ranges, separated by commas.

Timeout Threshold

This threshold controls how long the EtherScope waits for a response from each port. Once all the ports in the Scan List have had this amount of time to respond, the scan ends, and the TCP Port Scan results screen lists the ports that responded within the threshold.

See also the TCP Port Scan results card and screen.

Back to Title and Contents

Wi-Fi Analysis App

The Wi-Fi Analysis app scans the wireless channels in your environment to discover and gather data about the devices and traffic on your Wi-Fi networks. Wi-Fi discovery begins when you power on the EtherScope, and measurements update with each channel scan cycle.

The EtherScope nXG supports 802.11a/b/g/n/ac technologies and operates in both the 2.4 GHz and 5 GHz bands. EtherScope can also detect and indicate the 802.11ax media type (known as Wi-Fi 6) being used on APs and Clients, as reported in the wireless management frames.

The Wi-Fi app features separate screens that list and display characteristics of the different devices and elements of your wireless environment. Tap a link below to go directly to the description of the screen listed:

- Channels Map – Utilization or Overlap
- Channels
- SSIDs
- APs
- BSSIDs
- Clients
- Interferers

Wi-Fi Analysis and Discovery

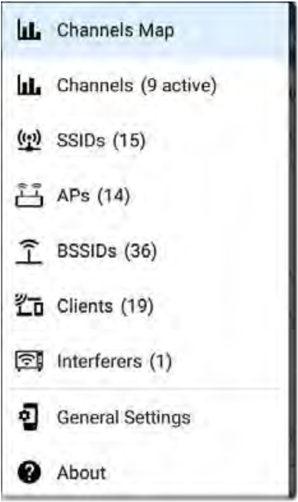
Wi-Fi Analysis utilizes the Wi-Fi Test Port to scan the channels and acquire information about your wireless networks. If the Wi-Fi Test Port is linked (for instance after running a Wi-Fi AutoTest Profile), the port unlinks and resumes scanning when you open the Wi-Fi Analysis app.

Wi-Fi Analysis is enhanced with data gathered by Discovery. When the EtherScope is linked to a network through any of the other three ports (Wi-Fi Management, Wired Test, or Wired Management), Discovery can obtain information from network layers 3 and above, such as IP addresses, Protocols, and SNMP data.

Therefore, the information Wi-Fi Analysis is able to display also depends on configured Discovery Settings, such as SNMP Community Strings and Credentials, Active Discovery Ports, Extended Ranges, and Device Health testing.

Wi-Fi App List Screens

To switch between the different Wi-Fi app screens, tap the menu icon ☰ (or swipe right) to open the left-side navigation drawer.



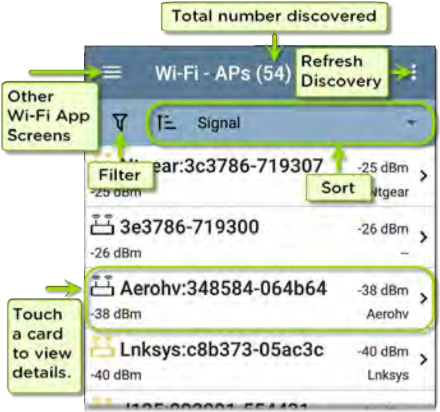
The Wi-Fi app's navigation drawer displays a real-time count (in parentheses) of each wireless component EtherScope has detected. Tap an option to open the corresponding screen.

> NOTE: The **General Settings** for Wi-Fi control which channels and bands are scanned to populate the Wi-Fi screens. See the General Settings topic for more explanation.

Wi-Fi App List Screens

The Wi-Fi app screens, except for Channels Map, display a list of discovered items, much like a Discovery App list screen. You can Filter ⛛ and Sort the list by different characteristics and touch a network component's card to view its details.

The example image below shows the APs screen with the common Wi-Fi app screen functions pointed out.

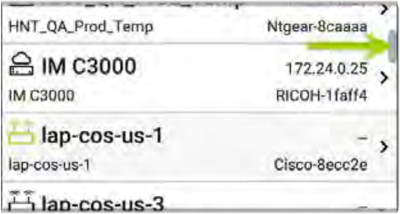


Like in AutoTest and other EtherScope screens, the icons in Wi-Fi analysis change color to indicate a **Warning** or **Failure** condition. The app also displays icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous Problem has been resolved.

> NOTE: To adjust the Problem Settings, access them from the Discovery app's left-

side navigation drawer. Problem Settings in the Discovery app are also applied to the Wi-Fi Analysis app.

The Wi-Fi list screens, 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.


HNT_QA_Prod_Temp Ntgear-8caaaa

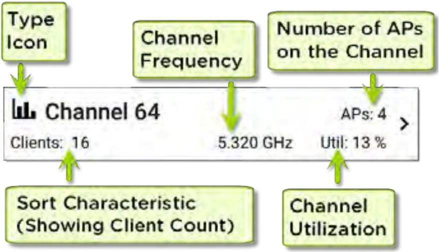
IM C3000 172.24.0.25
IM C3000 RICOH-1faff4

lap-cos-us-1 –
lap-cos-us-1 Cisco-8ecc2e

lap-cos-us-3

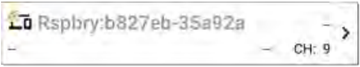
Wi-Fi List Cards

The information displayed on each card varies depending on the selected Sort characteristic and the data the EtherScope was able to discover. For example, a card on the Channels list screen displays the channel number, frequency, connected APs, and utilization.

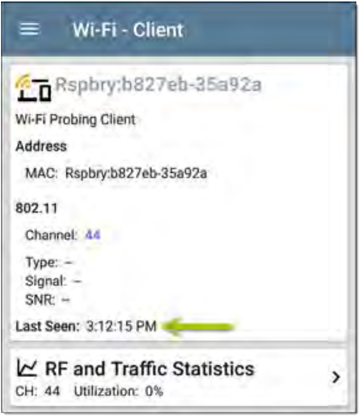


The lower left field displays the characteristic by which the list screen is currently sorted. In the image above, the Channels list is sorted by Client Count.

If a device is grayed out, the EtherScope no longer detects a signal from it. The client card shown below indicates that the "Rspbry" client cannot be detected currently.



The time the device was Last Seen, meaning last detected by the EtherScope, is shown on the device's Details screen.



Rspbry:b827eb-35a92a

Wi-Fi Probing Client

Address

MAC: Rspbry:b827eb-35a92a

802.11

Channel: 44

Type: –
Signal: –
SNR: –

Last Seen: 3:12:15 PM

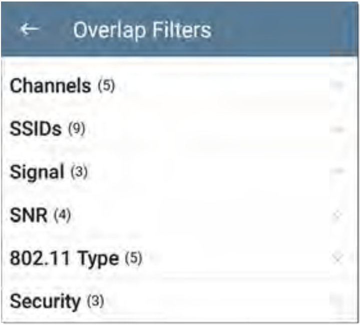
RF and Traffic Statistics
CH: 44 Utilization: 0%

Filtering in the Wi-Fi App

Each Wi-Fi Analysis screen has different Filter options that are appropriate for the network component type you are analyzing.

Touch the filter button near the top left of the Wi-Fi screens to set filters that control which network components are displayed.

As an example, the Channels Map Overlap Filters screen is shown below.



← Overlap Filters

Channels (5)

SSIDs (9)

Signal (3)

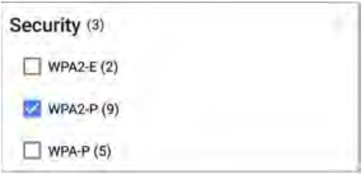
SNR (4)

802.11 Type (5)

Security (3)

The Channels Overlap Filters screen indicates (in parentheses) the number of active network characteristics detected (for example, number of active Channels or detected Security types).

Touch a category to select filters by tapping the checkboxes or radio buttons.

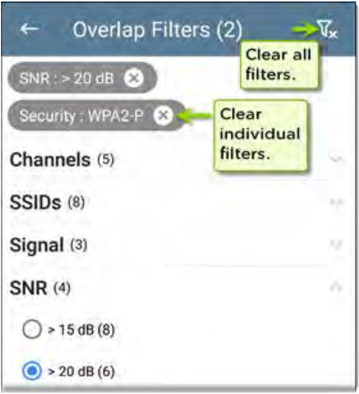


Security (3)

- ☐ WPA2-E (2)
- ☑ WPA2-P (9)
- ☐ WPA-P (5)

Under each category, the number of discovered APs is shown for each characteristic. (In the image above, there are 3 Security types detected and 9 APs using the WPA2-P Security type.)

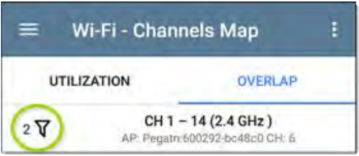
In this example, the Overlap screen will show only those APs that fall under your chosen filter parameters.



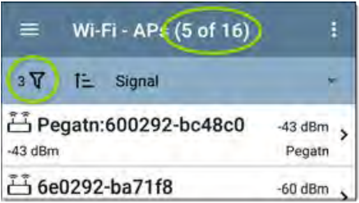
When filters are selected, those active filters are displayed at the top of the Filters screen.

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

Back on the Overlap screen, the number of active filters displays to the left of the filter icon, like this: 2 ▽.

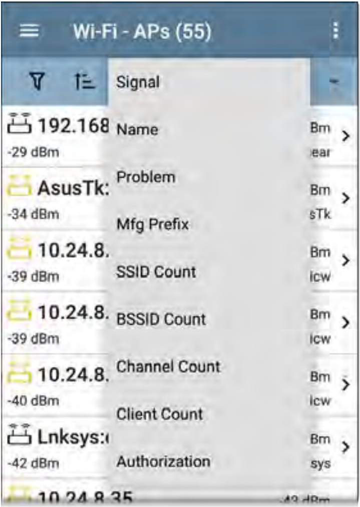


If the screen is a list, like the APs screen below, the screen title shows the number of filtered devices out of the total discovered devices (5 filtered devices out of 16 total).

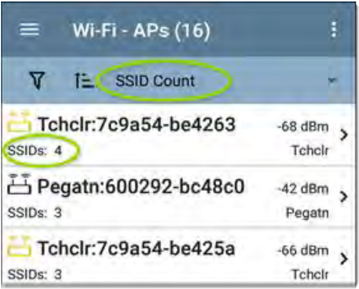


Sorting in the Wi-Fi App

Tap the Sort bar or down arrow to open the Sort drop-down menu. Each list screen supports relevant Sort options based on what you are viewing. The APs screen Sort options are shown below as an example.



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



Wi-Fi - APs (16)

SSID Count

Tchclr:7c9a54-be4263 -68 dBm
SSIDs: 4 Tchclr

Pegatn:600292-bc48c0 -42 dBm
SSIDs: 3 Pegatn

Tchclr:7c9a54-be425a -66 dBm
SSIDs: 3 Tchclr

The selected Sort option displays in the Sort bar above the list, and the sort characteristic for each item is shown under the type icon and name. In the image above, the discovered APs are sorted by SSID Count, which is shown below each AP icon.

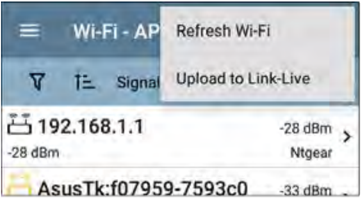
Tap the sort order icon to switch the sort order between normal and reverse order.

Wireless devices and IDs 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.

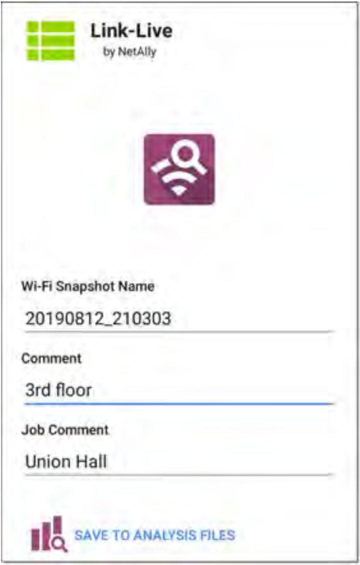
Refreshing Wi-Fi

Touch the action overflow icon ⋮ at the top right of the screen, and select **Refresh Wi-Fi** to clear and repopulate the Wi-Fi app screens with data.



Uploading Wi-Fi Results to Link-Live

Touch the action overflow icon ⋮ at the top right of the main Wi-Fi app screen, and select **Upload to Link-Live** to send the current Wi-Fi results to the Analysis page on Link-Live.com.



Wi-Fi Snapshot Name
20190812_210303

Comment
3rd floor

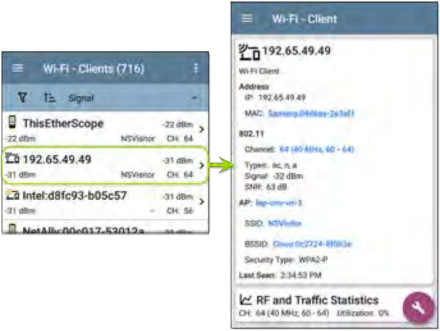
Job Comment
Union Hall

See the Link-Live chapter for more information.

Wi-Fi Details Screens

Tapping any card on a list screen (Channels, SSIDs, APs, BSSIDs, Clients, and Interferers) opens the Details screen for that device or network ID.

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



Wi-Fi - Clients (716)

Signal

ThisEtherScope -22 dBm
-22 dBm NSVishor CH: 64

192.65.49.49 -31 dBm
-31 dBm NSVishor CH: 64

Intel:d8fc93-b05c57 -31 dBm
-31 dBm -- CH: 56

NetAlly:00c017-53012a

Wi-Fi - Client

192.65.49.49
Wi-Fi Client

Address
IP: 192.65.49.49
MAC: Samsung:04d6aa-2e3af1

802.11
Channel: 64 (40 MHz, 60 - 64)
Types: ac, n, a
Signal: -32 dBm
SNR: 63 dB

AP: lap-cme-un-3

SSID: NSVisitor

BSSID: Cisco:0c2724-8f083e

Security Type: WPA2-P

Last Seen: 2:34:53 PM

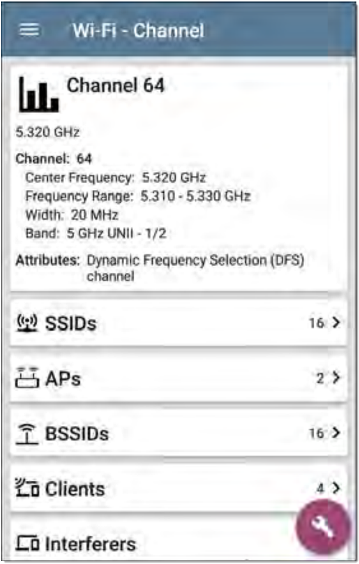
RF and Traffic Statistics
CH: 64 (40 MHz, 60 - 64) Utilization: 0%

On the Wi-Fi Details screens, you can touch any **blue linked name or address** to open a Discovery or Wi-Fi app screen for the linked device.

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

Each Details screen shows additional information about the selected item, any Problems detected by the EtherScope, and counts for other connected network devices or IDs.

See also Data Fields on the Top Details Card in the Discovery chapter, many of which are the same as the data fields shown in Wi-Fi Details.



Channel 64

5.320 GHz

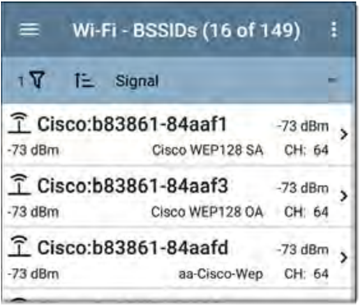
Channel: 64
Center Frequency: 5.320 GHz
Frequency Range: 5.310 - 5.330 GHz
Width: 20 MHz
Band: 5 GHz UNII - 1/2

Attributes: Dynamic Frequency Selection (DFS) channel

SSIDs	16 >
APs	2 >
BSSIDs	16 >
Clients	4 >
Interferers	

The Channel Details screen above shows how many SSIDs, APs, BSSIDs, Clients, and Interferers are detected on Channel 64. Touch the lower cards in Wi-Fi Details to open a list screen that is filtered for the network component you are examining.

If the user selects BSSIDs on the Details screen for Channel 64, the BSSIDs screen opens and filters for BSSIDs found on Channel 64 only.



Wi-Fi - BSSIDs (16 of 149)

1 Signal

Cisco:b83861-84aaf1 -73 dBm
-73 dBm Cisco WEP128 SA CH: 64

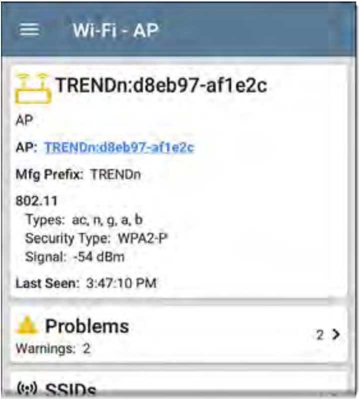
Cisco:b83861-84aaf3 -73 dBm
-73 dBm Cisco WEP128 OA CH: 64

Cisco:b83861-84aafd -73 dBm
-73 dBm aa-Cisco-Wep CH: 64

See the topics for each Wi-Fi app screen type (SSIDs, APs, etc.) for more discussion of the corresponding Details screen.

Wi-Fi Problems Screen

If any of the enabled Wi-Fi Problems are detected, the Problems card appears on the Wi-Fi Details screen.



TRENDn:d8eb97-af1e2c

AP

AP: TRENDn:d8eb97-af1e2c

Mfg Prefix: TRENDn

802.11

Types: ac, n, g, a, b

Security Type: WPA2-P

Signal: -54 dBm

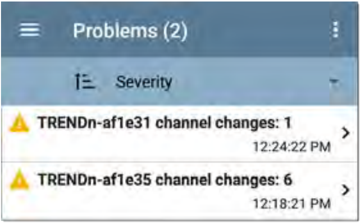
Last Seen: 3:47:10 PM

Problems

Warnings: 2

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

Touch the card to open the Problems screen.



Problems (2)

Severity

TRENDn-af1e31 channel changes: 1
12:24:22 PM

TRENDn-af1e35 channel changes: 6
12:18:21 PM

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

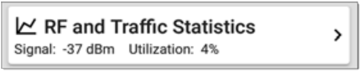
You can also tap the sort field to sort the list by **Severity** or by the time when the problem was **First Detected**. Touch the action overflow button ⋮ at the top right to **Clear Problems**.

See Problem Settings in the Discovery app to select which Wi-Fi Problems are detected and displayed by your EtherScope.

RF and Traffic Statistics Overview

The Channel, BSSID, and Client Details screens can display RF and Traffic Statistics if any traffic is detected.

This section describes the common elements of the RF and Traffic Statistics screen. See the topic for each type of Details screen for differences.



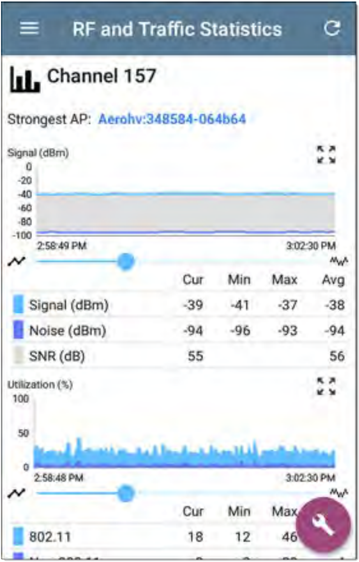
RF and Traffic Statistics

Signal: -37 dBm Utilization: 4%

The RF and Traffic Statistics card shows the Channel number or the Signal strength of the strongest AP on the channel and the channel's Utilization percentage.

Tap the card to view graphs of Signal, Noise, Utilization, and Retries.

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.



Channel 157

Strongest AP: Aerohv:348584-064b64

	Cur	Min	Max	Avg
Signal (dBm)	-39	-41	-37	-38
Noise (dBm)	-94	-96	-93	-94
SNR (dB)	55			56

	Cur	Min	Max
802.11	18	12	46

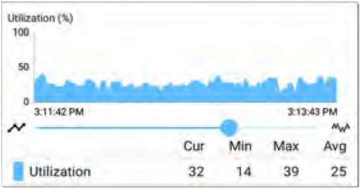
Strongest AP: The AP on the channel with the strongest signal

Under each graph, a legend table displays the Current, Minimum, Maximum, and Average measurements. The Current column contains measurements from the last second. Min, Max, and Avg columns show cumulative measurements gathered during the time the RF and Traffic screen has been open.

Tap the refresh button ↻ at the top of the screen to clear and restart the measurements.

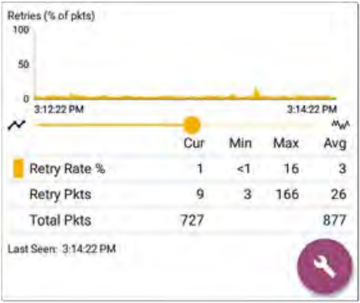
Signal (dBm) graph: Plots the signal strength in dBm of the selected AP or AP with the strongest signal on a channel

- Signal - The AP's signal strength in dBm
- Noise - The noise level in dBm on the channel used
- SNR - The network's signal-to-noise ratio, a measure of signal strength relative to noise, measured in decibels (dB)



	Cur	Min	Max	Avg
Utilization	32	14	39	25

Utilization (%) graph: Plots percentage of the channel capacity being used by 802.11 devices and by non-802.11 interference. If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows combined channel utilization and 802.11 utilization only for BSSIDs and Clients (as shown in the image above).



	Cur	Min	Max	Avg
🟨 Retry Rate %	1	<1	16	3
Retry Pkts	9	3	166	26
Total Pkts	727			877

Last Seen: 3:14:22 PM

Retries (% of packets) graph: Plots percentage of transmitted packets that are retry packets

- Retry Rate % - The percentage of total packets that are retry packets
- Retry Pkts - The number of retry packets

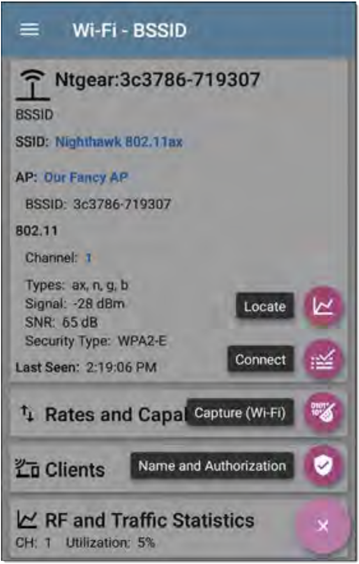
- Total Pkts - The total number of transmitted packets

Locating Wi-Fi Devices

You can use your EtherScope to locate APs and Wi-Fi clients from the RF and Traffic Statistics screen for BSSIDs and Clients.

To access the RF and Traffic Statistics screen, from a BSSID or Client Details screen, select the RF and Traffic Statistics card or touch **Locate** from the floating action menu.

Back to Title and Contents



Wi-Fi - BSSID

Ntgear:3c3786-719307

BSSID

SSID: Nighthawk 802.11ax

AP: Our Fancy AP

BSSID: 3c3786-719307

802.11

Channel: 1

Types: ax, n, g, b

Signal: -28 dBm

SNR: 65 dB

Security Type: WPA2-E

Last Seen: 2:19:06 PM

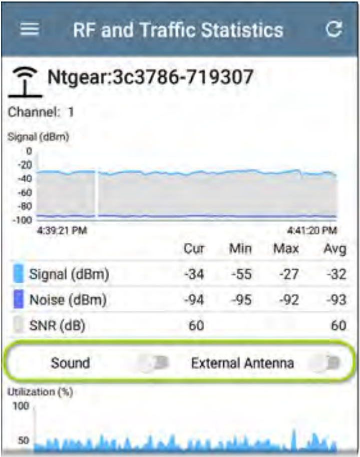
Rates and Capal

Clients

RF and Traffic Statistics

CH: 1 Utilization: 5%

Touching **Locate** opens the RF and Traffic Statistics screen.



Ntgear:3c3786-719307

Channel: 1

	Cur	Min	Max	Avg
■ Signal (dBm)	-34	-55	-27	-32
■ Noise (dBm)	-94	-95	-92	-93
■ SNR (dB)	60			60

Sound ○ External Antenna ○

The **Sound** function emits an audible tone that increases in rate and pitch as the signal strength of the device increases (as you get closer to it). Use the device's volume buttons to turn the sound up or down.

The **External Antenna** toggle enables the optional external antenna.

EtherScope can help you locate wireless devices using either the four internal antennas or the optional external antenna (sold separately).

In large, open areas, the external antenna can help locate devices more quickly. See Using the Optional External Antenna below.

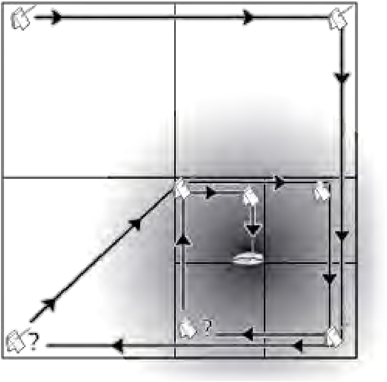
In areas with many rooms, like a hospital or school, the internal antennas are more effective.

Using the Internal Antennas to Locate

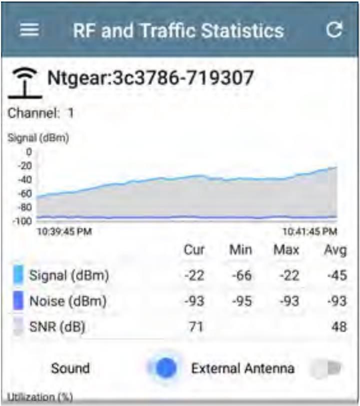
EtherScope uses the internal antennas by default.

1. Navigate to the RF and Traffic Statistics screen for the BSSID (AP) or client you need to locate.
2. If desired, touch the **Sound** toggle to enable an audible tone.

3. Divide the area you want to search into four sections.



4. Go to one corner of your search area, and note the device's signal strength on the Signal graph.



	Cur	Min	Max	Avg
Signal (dBm)	-22	-66	-22	-45
Noise (dBm)	-93	-95	-93	-93
SNR (dB)	71			48

Sound ● External Antenna ○

5. Go to the other three corners of the area, and note the signal strength at each corner.
6. Go to the section with the strongest signal.
7. Repeat steps 3 through 6 until you find the device.

If you still cannot find the device, try looking on the floors above or below you. If you cannot find a client, try locating the AP to which the client is connected first.

Using the Optional External Antenna

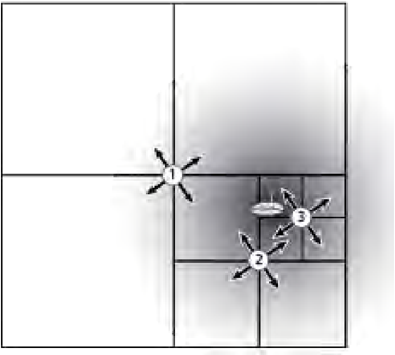
In large, open areas, the external antenna can help determine the direction of a signal source more precisely than the internal antenna. Visit NetAlly.com for purchasing information.

To get the best measurements with the external antenna, hold it at a constant height, above any cubicle walls, and point the front of the antenna towards your search area, as shown below.

1. Screw the external antenna cord into the antenna port on the top of the EtherScope.
2. On the RF and Traffic Statistics screen, touch the **External Antenna** toggle to enable the external antenna.

3. If desired, touch the **Sound** toggle to enable an audible tone.

4. Divide the area you want to search into four sections.



5. Go to the center of your search area.

6. Point the antenna towards each corner of the area.

7. Go to the middle of the section with the strongest signal.

8. Repeat steps 4 through 7 until you find the device.

Assigning a Name and Authorization to a Device

The Wi-Fi and Discovery apps provide the option to assign a **Name and Authorization** to any discovered device with a MAC Address or BSSID.

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 EtherScope on which the Name and Authorization are assigned.

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

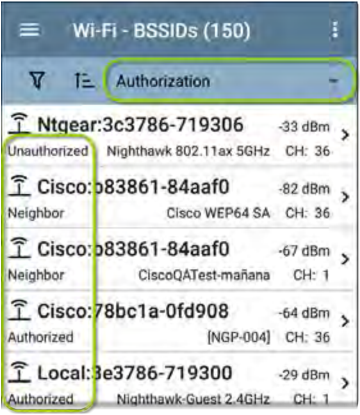
This feature allows you to quickly identify your known devices and categorize them with the following statuses:

- **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 and Wi-Fi apps.

You can Sort and Filter by the assigned Authorization in the Wi-Fi and Discovery apps. 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 the BSSIDs list screen sorted this way:



Wi-Fi - BSSIDs (150)

Authorization

Ntgear:3c3786-719306 -33 dBm
Unauthorized Nighthawk 802.11ax 5GHz CH: 36

Cisco:b83861-84aaf0 -82 dBm
Neighbor Cisco WEP64 SA CH: 36

Cisco:b83861-84aaf0 -67 dBm
Neighbor CiscoQATest-mañana CH: 1

Cisco:78bc1a-0fd908 -64 dBm
Authorized [NGP-004] CH: 36

Local:3e3786-719300 -29 dBm
Authorized Nighthawk-Guest 2.4GHz CH: 1

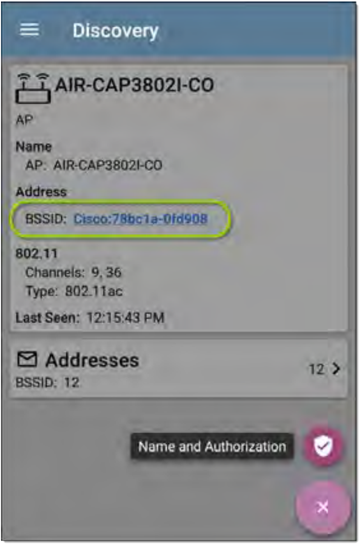
Applying a Name and/or Authorization

Access the **Name and Authorization** function from the floating action menu on a

Discovery Details screen or a Wi-Fi Details screen for a BSSID or Client.

NOTE: When applying an Authorization to a device with multiple BSSIDs or MAC addresses, the Authorization status is only applied to the MAC address/BSSID displayed on the Details screen, as shown in this section.

1. Touch the FAB on a Discovery or Wi-Fi Details screen for a device with a discovered MAC/BSSID.



AIR-CAP3802I-CO

AP

Name
AP: AIR-CAP3802I-CO

Address
BSSID: Cisco:78bc1a-0fd908

802.11
Channels: 9, 36
Type: 802.11ac

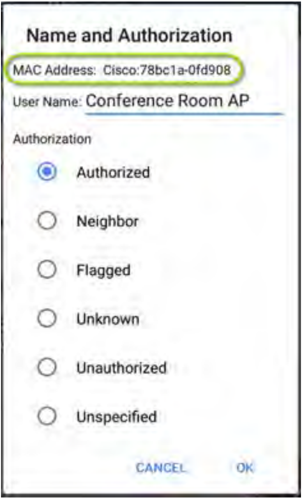
Last Seen: 12:15:43 PM

Addresses
BSSID: 12

12

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

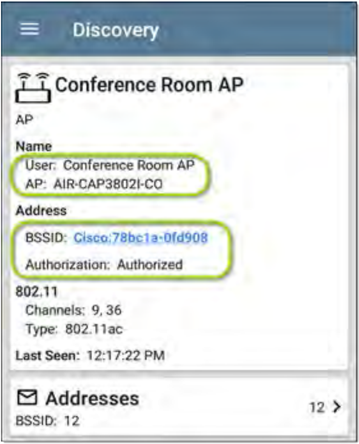
○ Unspecified

3. In the Name and Authorization dialog, touch 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. Touch **OK** to apply.

Once applied, the User Name and Authorization are displayed on the Discovery Details screen.



Conference Room AP

AP

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

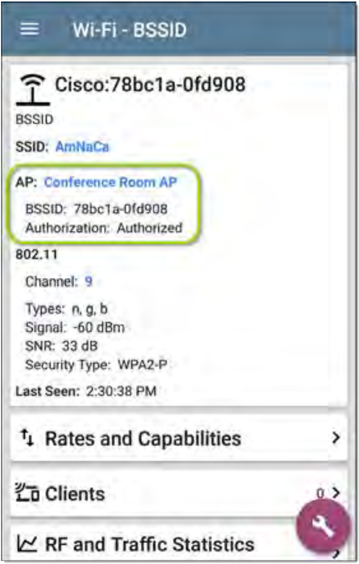
Address
BSSID: Cisco:78bc1a-0fd908
Authorization: Authorized

802.11
Channels: 9, 36
Type: 802.11ac

Last Seen: 12:17:22 PM

Addresses
BSSID: 12

The user-assigned name for the AP and Authorization for the BSSID also appear on the Wi-Fi BSSID Details screen, as shown below.



Wi-Fi - BSSID

Cisco:78bc1a-0fd908

BSSID

SSID: AmNaCa

AP: Conference Room AP

BSSID: 78bc1a-0fd908

Authorization: Authorized

802.11

Channel: 9

Types: n, g, b

Signal: -60 dBm

SNR: 33 dB

Security Type: WPA2-P

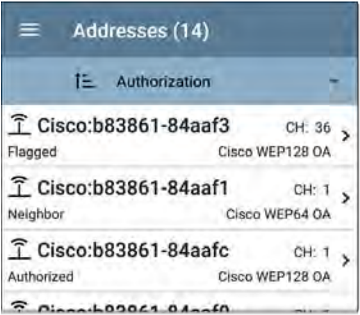
Last Seen: 2:30:38 PM

NOTE: If different Authorization statuses are assigned for different BSSIDs or 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 BSSID or 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 or Wi-Fi Details screen for the device and view the Addresses or BSSIDs screen. Then, sort by Authorization.



Addresses (14)

Authorization

Cisco:b83861-84aaf3 CH: 36
Flagged Cisco WEP128 OA

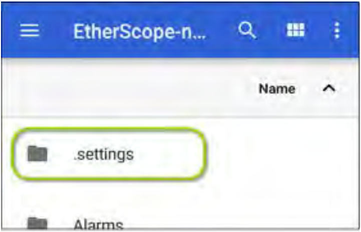
Cisco:b83861-84aaf1 CH: 1
Neighbor Cisco WEP64 OA

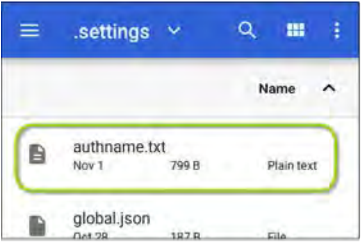
Cisco:b83861-84aafc CH: 1
Authorized Cisco WEP128 OA

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, touch OK.

Revising or Importing authname.txt

Custom Names and Authorizations are stored in the **authname.txt** file in the EtherScope's internal storage **.settings** folder, accessible from the Files app.

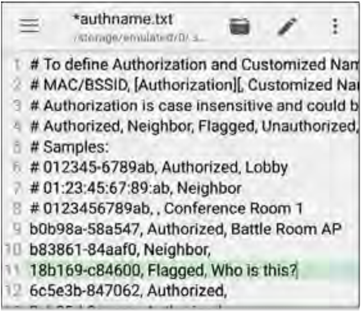




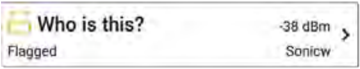
NOTE: In the Files app, you may need to tap the action overflow icon ⋮ at the top right and select **Show Internal Storage** to navigate to the **EtherScope-nXG** folder and sub-folders.

If desired, you can manually edit this file on the EtherScope unit, or you can create a new authname.txt file on a PC and import it onto your unit in the same file location.

The default authname.txt file on your unit contains instructions on how to format your Name and Authorization entries.



```
# To define Authorization and Customized Nam
# MAC/BSSID, [Authorization][, Customized Na
# Authorization is case insensitive and could b
# Authorized, Neighbor, Flagged, Unauthorized,
# Samples:
# 012345-6789ab, Authorized, Lobby
# 01:23:45:67:89:ab, Neighbor
# 0123456789ab, , Conference Room 1
b0b98a-58a547, Authorized, Battle Room AP
b83861-84aaf0, Neighbor,
18b169-c84600, Flagged, Who is this?
6c5e3b-847062, Authorized,
```



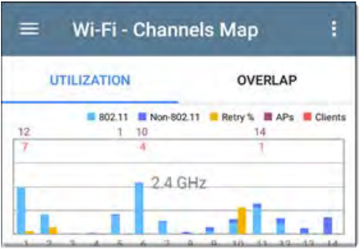
To edit the authname.txt file on the EtherScope, third-party apps, such QuickEdit Text Editor, are available from the NetAlly App Store ▶ .

For help importing a file, see the Managing Files topic.

> NOTE: After importing and overriding the authname.txt file, we recommend Refreshing Discovery in the Discovery app or restarting your unit.

Channels Map

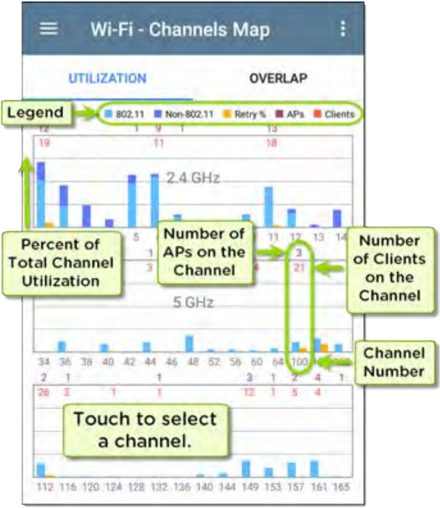
The Channels Map screens provide graphical representations of channel utilization, AP coverage, and overlap.



The Channels Map features two tabs: Utilization and Overlap. Touch the tab names to switch between the two screen types.

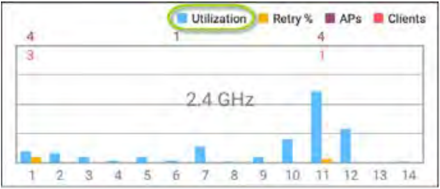
Channels Utilization

The Channels Utilization screen displays a bar graph of 802.11 and non-802.11 utilization, retry percentage, and the number of APs and clients for each channel.



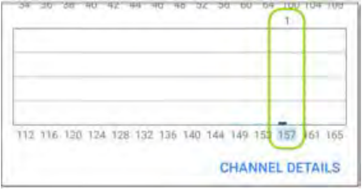
In the image above, the vertical light and dark blue bars show how much of the channel's capacity is being used by 802.11 devices and non-802.11 interference, with channel numbers on the x-axis and Utilization percentage on the y-axis.

If the **Combine Utilization** setting is enabled in General Settings, only combined 802.11 and non-802.11 Utilization is shown on the graph.

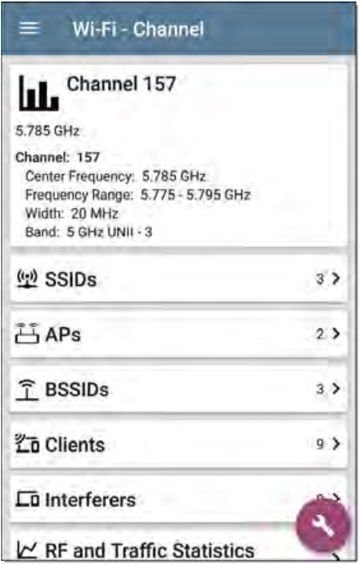


AP counts are shown on the APs' primary channel. Channels that do not have APs can still show 802.11 utilization because of overlap from adjacent channels.

Touch a Channel's column on the Utilization graph to select and highlight a channel.



Then, tap **CHANNEL DETAILS** at the bottom to open the Details screen for the channel.



Channel 157

5.785 GHz

Channel: 157
Center Frequency: 5.785 GHz
Frequency Range: 5.775 - 5.795 GHz
Width: 20 MHz
Band: 5 GHz UNII - 3

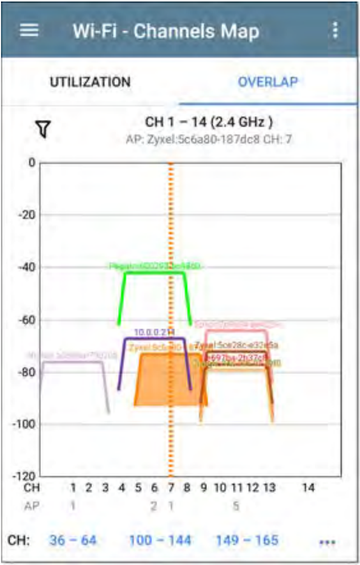
From the Channel Details screen, you can examine the addresses and devices operating on the channel and perform a deeper analysis.

See Channel Details for more about this screen.

Channels Overlap

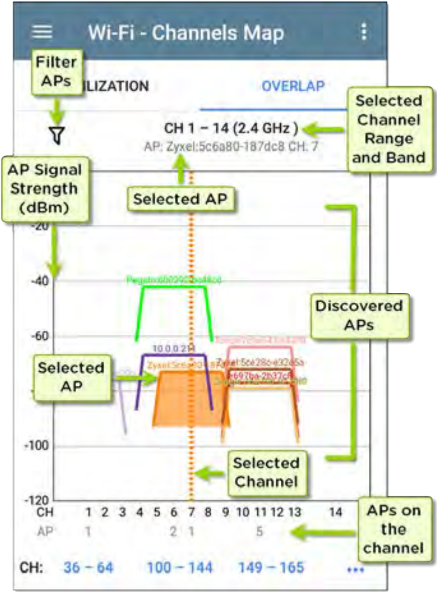
The Channels Overlap screen provides a visualization of access point deployment with respect to channel, coverage, and overlap, allowing you to spot potential coverage issues.

Each discovered AP is shown as a colored trapezoid and plotted on the graph based on its channel coverage (on the x-axis) and signal strength in dBm (on the y-axis).

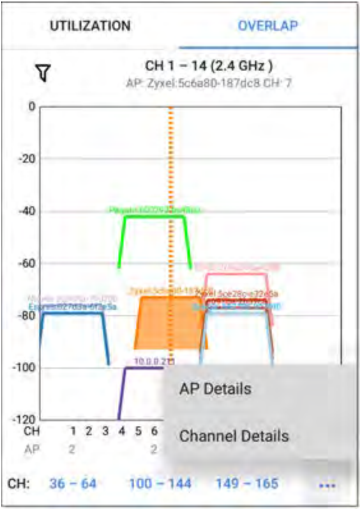


CH 1 – 14 (2.4 GHz)
AP: Zyxel:5c6a80-187dc8 CH: 7

- Touch an AP on the graph to select it and its primary channel. In the image above, the AP named "Zyxel:5c6a..." on channel 7 is selected.



- Touch the **blue channel range** selectors at the bottom to view a different channel range on the graph.

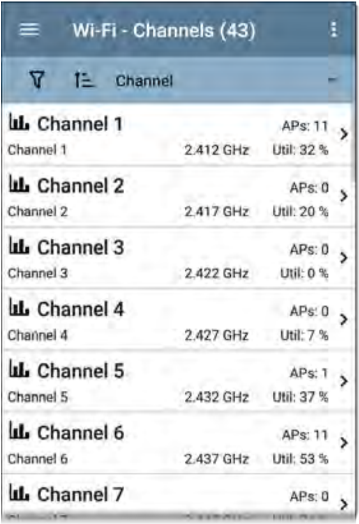


- Touch the action overflow button ••• to open the AP Details or Channel Details screens for the selected AP or Channel.

See Filtering in the Wi-Fi App for an explanation of the Overlap screen's filtering options.

Channels

The Channels list screen displays the characteristics of the wireless Channels as they are scanned in your location.



Wi-Fi - Channels (43)

Channel

Channel 1
Channel 1 2.412 GHz APs: 11 Util: 32 %

Channel 2
Channel 2 2.417 GHz APs: 0 Util: 20 %

Channel 3
Channel 3 2.422 GHz APs: 0 Util: 0 %

Channel 4
Channel 4 2.427 GHz APs: 0 Util: 7 %

Channel 5
Channel 5 2.432 GHz APs: 1 Util: 37 %

Channel 6
Channel 6 2.437 GHz APs: 11 Util: 53 %

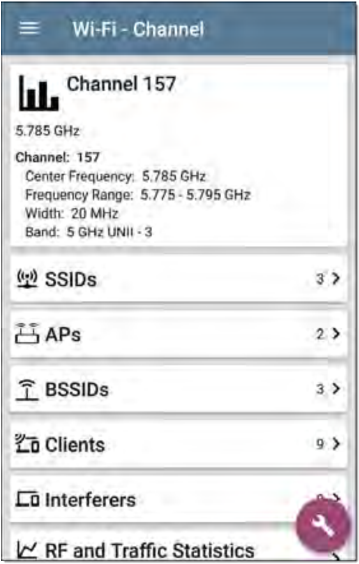
Channel 7
APs: 0

Refer to the Wi-Fi App List Screens topic for instructions on viewing, filtering, and sorting.

By default, Channels are ordered by channel number, and each card shows the channel frequency, number of APs, and total Utilization percent.

Touch a Channel card to open the Channel Details screen.

Channel Details



Wi-Fi - Channel

Channel 157

5.785 GHz

Channel: 157
  Center Frequency: 5.785 GHz
  Frequency Range: 5.775 - 5.795 GHz
  Width: 20 MHz
  Band: 5 GHz UNII - 3

SSIDs 3 >

APs 2 >

BSSIDs 3 >

Clients 9 >

Interferers 0 >

RF and Traffic Statistics >

The Channel Details screen displays the channel's Center Frequency under the icon, along with the Frequency Range, Width, and Band.

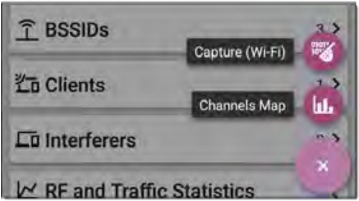
Dynamic Frequency Selection (DFS) channels also display an Attributes field that indicates DFS.

Channel RF and Traffic Statistics

The RF and Traffic Statistics card appears when there is an active AP and Utilization on the channel. See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic.

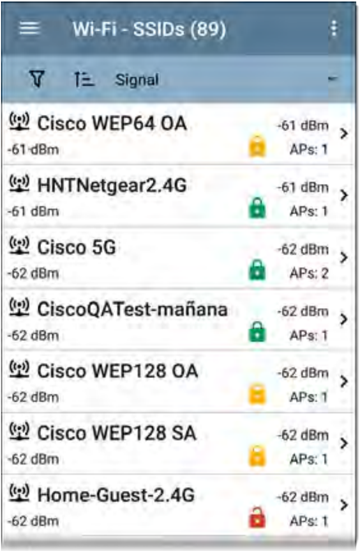
Channel FAB

Tap the FAB on the Channel Details screen to open the Capture app and record a packet capture on the channel or to open the Channels Map screen with the current channel selected.



SSIDs

The SSIDs list screen shows all the network SSIDs the EtherScope has discovered.



Wi-Fi - SSIDs (89)

Signal

Cisco WEP64 OA -61 dBm	🔒	-61 dBm APs: 1
HNTNetgear2.4G -61 dBm	🔒	-61 dBm APs: 1
Cisco 5G -62 dBm	🔒	-62 dBm APs: 2
CiscoQATest-mañana -62 dBm	🔒	-62 dBm APs: 1
Cisco WEP128 OA -62 dBm	🔒	-62 dBm APs: 1
Cisco WEP128 SA -62 dBm	🔒	-62 dBm APs: 1
Home-Guest-2.4G -62 dBm	🔒	-62 dBm APs: 1

Refer to the Wi-Fi App List Screens topic if needed.

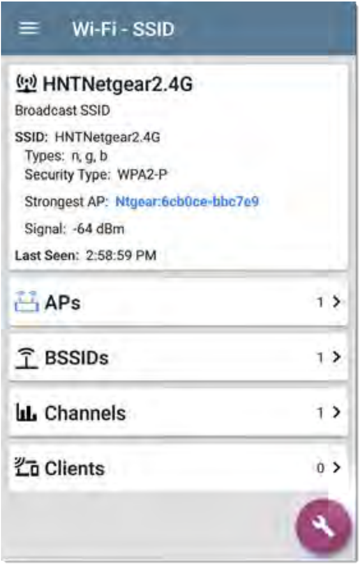
By default, SSIDs are ordered by Signal strength, and each card shows the network security status and number of APs on the network.

The security status icons have the following meanings:

- 🔒 Green closed lock: All APs on the network use secure protocols, like WPA2 or WPA3.
- 🔒 Yellow closed lock: One or more APs use WEP or Cisco LEAP protocols, which are less secure.
- 🔓 Red open lock: The network does not have security enabled.

Touch a SSID card to open the SSID Details screen.

SSID Details



HNTNetgear2.4G

Broadcast SSID

SSID: HNTNetgear2.4G
Types: n, g, b
Security Type: WPA2-P
Strongest AP: Ntgear:6cb0ce-bbc7e9
Signal: -64 dBm
Last Seen: 2:58:59 PM

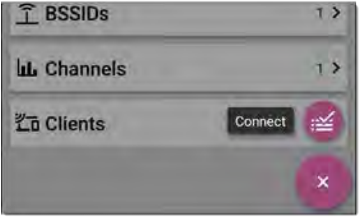
In addition to the Signal and Security Type, the SSID Details displays the AP on the network with the strongest signal, 802.11 Types that the

APs in the network support, and the time the EtherScope last detected activity on the network (Last Seen).

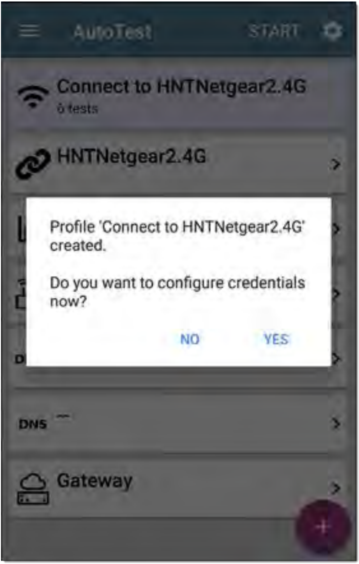
EtherScope nXG can detect and display 802.11 types a/b/g/n/ac/ax.

SSID FAB

Tap the FAB on the SSID Details screen to **Connect** to the network.



This action opens the AutoTest app and creates a new Wi-Fi profile called "Connect to [SSID]."



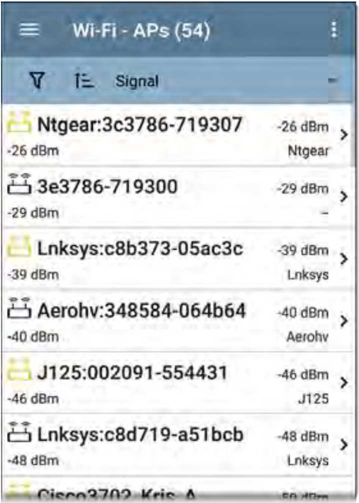
Profile 'Connect to HNTNetgear2.4G' created.

Do you want to configure credentials now?

See Creating a Wi-Fi Profile from the Wi-Fi Analysis App in the AutoTest chapter for a more detailed description of this process.

APs

The APs list screen displays all the Access Points discovered operating on your wireless networks.



Ntgear:3c3786-719307 -26 dBm
-26 dBm Ntgear

3e3786-719300 -29 dBm
-29 dBm –

Lnksys:c8b373-05ac3c -39 dBm
-39 dBm Lnksys

Aerohv:348584-064b64 -40 dBm
-40 dBm Aerohv

J125:002091-554431 -46 dBm
-46 dBm J125

Lnksys:c8d719-a51bcb -48 dBm
-48 dBm Lnksys

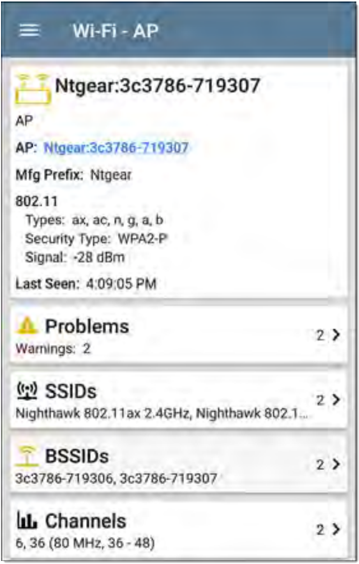
Cisco3702_Kris_A

Use the Filter and Sort functions to determine which APs are shown and their order in the list. Refer to the Wi-Fi App List Screens topic if needed.

By default, APs are ordered by Signal strength, and each card shows the Signal strength in dBm and the AP's manufacturer prefix.

Touch an individual AP's card to open the AP Details screen.

AP Details



Ntgear:3c3786-719307

AP

AP: Ntgear:3c3786-719307

Mfg Prefix: Ntgear

802.11

Types: ax, ac, n, g, a, b

Security Type: WPA2-P

Signal: -28 dBm

Last Seen: 4:09:05 PM

Problems 2 >

Warnings: 2

SSIDs 2 >

Nighthawk 802.11ax 2.4GHz, Nighthawk 802.1...

BSSIDs 2 >

3c3786-719306, 3c3786-719307

Channels 2 >

6, 36 (80 MHz, 36 - 48)

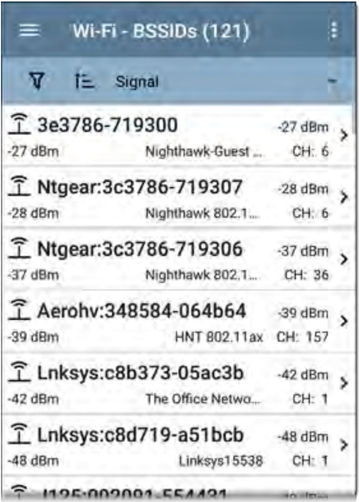
The AP Details screen shows the 802.11 Types the AP supports, the AP's Security Type, and the time the AP was last detected (Last Seen) by the EtherScope.

Touch the lower cards to view the network IDs, Channels, and Clients associated with the AP.

See Wi-Fi Problems for more information about the Problems card.

BSSIDs

The BSSIDs list screen shows the BSSID addresses discovered in your wireless environment.



Wi-Fi - BSSIDs (121)

Signal

3e3786-719300 -27 dBm
-27 dBm Nighthawk-Guest ... CH: 6

Ntgear:3c3786-719307 -28 dBm
-28 dBm Nighthawk 802.1... CH: 6

Ntgear:3c3786-719306 -37 dBm
-37 dBm Nighthawk 802.1... CH: 36

Aerohv:348584-064b64 -39 dBm
-39 dBm HNT 802.11ax CH: 157

Lnksys:c8b373-05ac3b -42 dBm
-42 dBm The Office Netwo... CH: 1

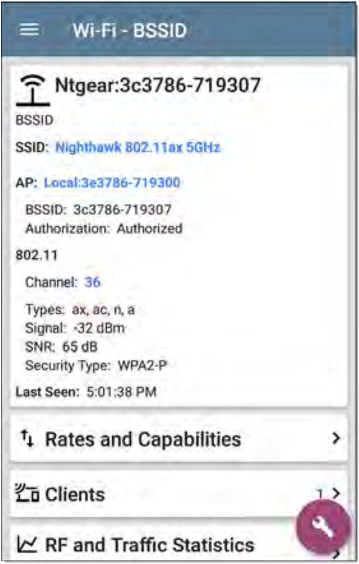
Lnksys:c8d719-a51bcb -48 dBm
-48 dBm Linksys15538 CH: 1

Refer to the Wi-Fi App List Screens topic if needed.

By default, the BSSIDs are ordered by Signal strength, and each card shows the Signal strength, SSID, and channel number on which the BSSID is operating.

Touch an BSSID's card to open the Details screen.

BSSID Details



Wi-Fi - BSSID

Ntgear:3c3786-719307

BSSID

SSID: Nighthawk 802.11ax 5GHz

AP: Local:3e3786-719300

BSSID: 3c3786-719307
Authorization: Authorized

802.11

Channel: 36

Types: ax, ac, n, a
Signal: -32 dBm
SNR: 65 dB
Security Type: WPA2-P

Last Seen: 5:01:38 PM

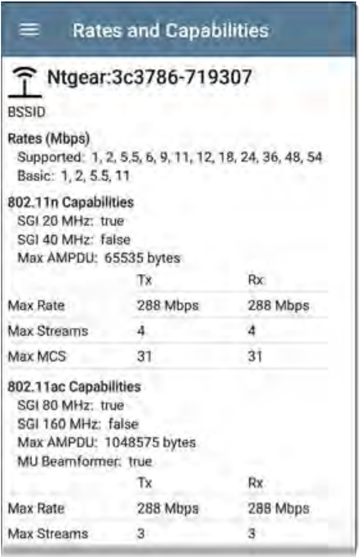
In addition to the characteristics on the BSSID cards, the Details screen displays the following information:

- User-assigned Authorization status (if set)
- Supported **802.11 Types**
- Signal-to-Noise ratio (**SNR**) measurement
- Network **Security** type
- Time activity was **Last Seen** on the BSSID

BSSID Details can also include Rates and Capabilities and RF and Traffic Statistics.

Rates and Capabilities

Touch the Rates and Capabilities card to open the full screen.



Rates and Capabilities

Ntgear:3c3786-719307

BSSID

Rates (Mbps)

Supported: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54

Basic: 1, 2, 5.5, 11

802.11n Capabilities

SGI 20 MHz: true

SGI 40 MHz: false

Max AMPDU: 65535 bytes

	Tx	Rx
Max Rate	288 Mbps	288 Mbps
Max Streams	4	4
Max MCS	31	31

802.11ac Capabilities

SGI 80 MHz: true

SGI 160 MHz: false

Max AMPDU: 1048575 bytes

MU Beamformer: true

	Tx	Rx
Max Rate	288 Mbps	288 Mbps
Max Streams	3	3

This screen shows advanced information about the transmit and receive rates and 802.11 capabilities reported by the beacon.

Rates (Mbps)

Supported: The extended physical (PHY) rates that the AP is configured to support

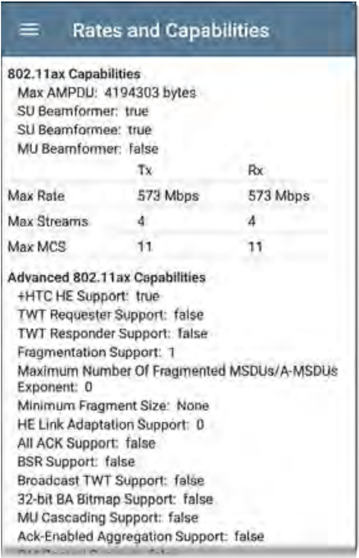
Basic: The basic physical (PHY) rates that the AP is configured to support

802.11 Capabilities

- 802.11n capabilities are gathered from HT capabilities in the beacon.
- 802.11ac capabilities are gathered from VHT capabilities in the beacon.
- 802.11ax capabilities are gathered from HE capabilities in the beacon.

802.11ax Rates and Capabilities

EtherScope nXG can also report Advanced 802.11ax (Wi-Fi 6) capabilities it sees in the beacon.



802.11ax Capabilities
Max AMPDU: 4194303 bytes
SU Beamformer: true
SU Beamformee: true
MU Beamformer: false

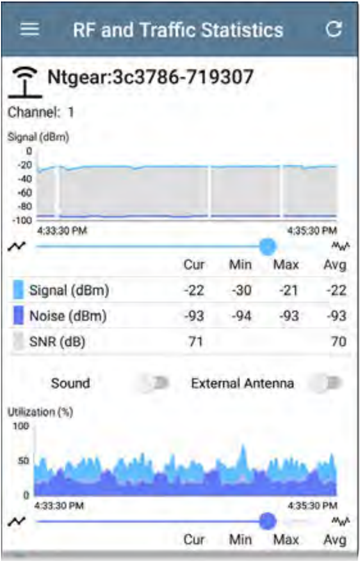
	Tx	Rx
Max Rate	573 Mbps	573 Mbps
Max Streams	4	4
Max MCS	11	11

Advanced 802.11ax Capabilities
+HTC HE Support: true
TWT Requester Support: false
TWT Responder Support: false
Fragmentation Support: 1
Maximum Number Of Fragmented MSDUs/A-MSDUs Exponent: 0
Minimum Fragment Size: None
HE Link Adaptation Support: 0
All ACK Support: false
BSR Support: false
Broadcast TWT Support: false
32-bit BA Bitmap Support: false
MU Cascading Support: false
Ack-Enabled Aggregation Support: false

BSSID RF and Traffic Statistics

See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.

The RF and Traffic Statistics screen for BSSIDs displays the BSSID and the channel number at the top of the screen.



RF and Traffic Statistics

Ntgear:3c3786-719307

Channel: 1

	Cur	Min	Max	Avg
Signal (dBm)	-22	-30	-21	-22
Noise (dBm)	-93	-94	-93	-93
SNR (dB)	71			70

Sound

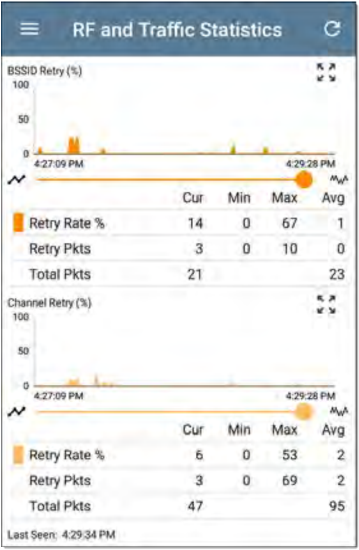
External Antenna

NOTE: The **Sound** and **External Antenna** toggles are used for locating the device. See Locating Wi-Fi Devices.

The Utilization graph shows separate measurements for Channel Utilization, BSSID Utilization, and Non-802.11 interference using different colors.

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.

The screen also displays separate graphs for Channel Retries and BSSID Retries.



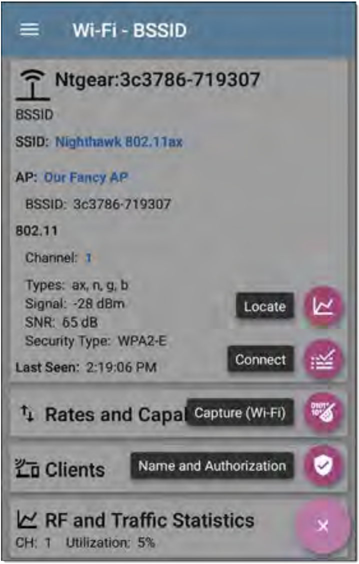
	Cur	Min	Max	Avg
▮ Retry Rate %	14	0	67	1
Retry Pkts	3	0	10	0
Total Pkts	21			23

	Cur	Min	Max	Avg
▮ Retry Rate %	6	0	53	2
Retry Pkts	3	0	69	2
Total Pkts	47			95

Last Seen: 4:29:34 PM

BSSID FAB

The floating action button on the BSSID screen lets you **Locate** the wireless device, **Connect** to the BSSID, record a packet **Capture** of the network traffic with the current BSSID on the connected channel, and assign or change its **Name and Authorization**.



Wi-Fi - BSSID

Ntgear:3c3786-719307

BSSID

SSID: Nighthawk 802.11ax

AP: Our Fancy AP

BSSID: 3c3786-719307

802.11

Channel: 1

Types: ax, n, g, b

Signal: -28 dBm

SNR: 65 dB

Security Type: WPA2-E

Last Seen: 2:19:06 PM

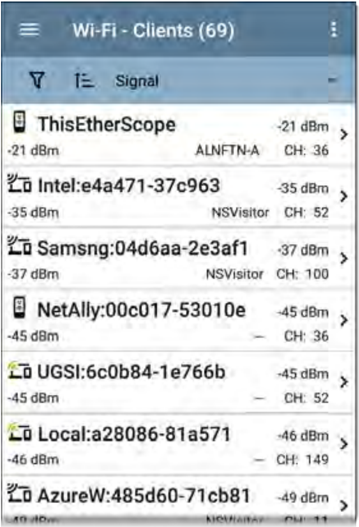
RF and Traffic Statistics

CH: 1 Utilization: 5%

- Selecting **Locate** opens the RF and Traffic Statistics screen where the sound and antenna controls are displayed. See Locating Wi-Fi Devices.
- Touching **Connect** opens the AutoTest app and creates a new Wi-Fi profile called "Connect to [BSSID]." See Creating a Wi-Fi Profile from the Wi-Fi Analysis App in the AutoTest chapter for a more detailed description of this process.
- Selecting **Capture** opens the Capture app populated with the Channel and BSSID. See the Capture app chapter.
- Selecting **Name and Authorization** opens the Name and Authorization dialog. See Assigning a Name and Authorization to a Device.

Clients

The Clients list screen displays the wireless clients the EtherScope has discovered connected to your wireless networks.



Wi-Fi - Clients (69)

Signal

ThisEtherScope			-21 dBm
-21 dBm	ALNFTN-A	CH: 36	
Intel:e4a471-37c963			-35 dBm
-35 dBm	NSVisitor	CH: 52	
Samsng:04d6aa-2e3af1			-37 dBm
-37 dBm	NSVisitor	CH: 100	
NetAlly:00c017-53010e			-45 dBm
-45 dBm	—	CH: 36	
UGSI:6c0b84-1e766b			-45 dBm
-45 dBm	—	CH: 52	
Local:a28086-81a571			-46 dBm
-46 dBm	—	CH: 149	
AzureW:485d60-71cb81			-49 dBm
-49 dBm	NSVisitor	CH: 11	

Refer to the Wi-Fi App List Screens topic if needed for explanations of how to Filter and Sort the Clients on this screen.

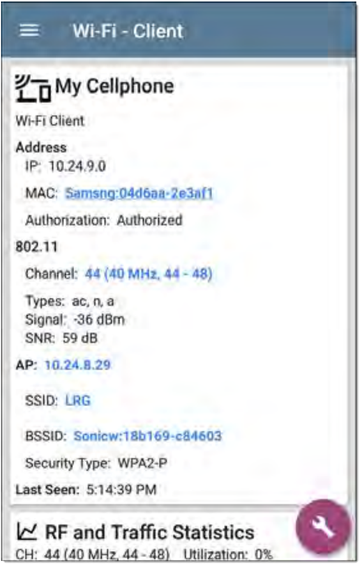
By default, the Clients are ordered by Signal strength, and each card shows the client's Signal strength in dBm, the SSID of the network to which the client is connected, and the channel number on which the Client is operating.

The general Client icons indicate whether the device is Probing or Connected to a network and able to receive data. If a Client is probing, two dashes -- display where the SSID would appear.

The Clients screen also shows specific icons for NetAlly testers, like the EtherScope icon shown in the image above.

Touch a Client's card to open the Details screen.

Client Details



My Cellphone

Wi-Fi Client

Address

IP: 10.24.9.0

MAC: Samsng:04d6aa-2e3af1

Authorization: Authorized

802.11

Channel: 44 (40 MHz, 44 - 48)

Types: ac, n, a
Signal: -36 dBm
SNR: 59 dB

AP: 10.24.8.29

SSID: LRG

BSSID: Sonicw:18b169-c84603

Security Type: WPA2-P

Last Seen: 5:14:39 PM

RF and Traffic Statistics

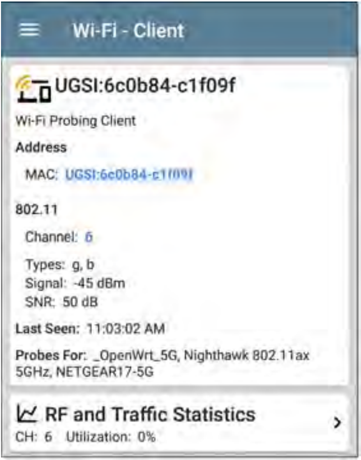
CH: 44 (40 MHz, 44 - 48) Utilization: 0%

The top Client Details card for a connected Client displays the following information:

- Client's **MAC** address
- User-assigned **Authorization** status (if set)
- Supported **802.11** media **Types**
- Signal-to-Noise ratio (**SNR**) measurement
- Name of the **AP** to which the Client is connected
- **SSID** of the network to which the Client is connected
- **BSSID** on which the Client is operating
- Network **Security** type
- Time the Client was **Last Seen** by the Ether-Scope

Probing Clients

The Probing Client Details screen does not show AP details, but can instead list the SSIDs for which the Client is probing in the **Probes For** field.



Wi-Fi - Client

UGSI:6c0b84-c1f09f

Wi-Fi Probing Client

Address

MAC: UGSI:6c0b84-c1f09f

802.11

Channel: 6

Types: g, b
Signal: -45 dBm
SNR: 50 dB

Last Seen: 11:03:02 AM

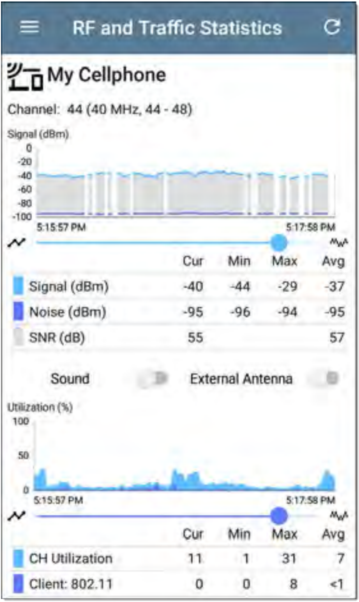
Probes For: _OpenWrt_5G, Nighthawk 802.11ax 5GHz, NETGEAR17-5G

RF and Traffic Statistics
CH: 6 Utilization: 0%

Client RF and Traffic Statistics

See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.

The RF and Traffic Statistics screen for Clients displays the Client's MAC or IP address and the channel number at the top of the screen.



My Cellphone

Channel: 44 (40 MHz, 44 - 48)

	Cur	Min	Max	Avg
Signal (dBm)	-40	-44	-29	-37
Noise (dBm)	-95	-96	-94	-95
SNR (dB)	55			57

Sound External Antenna

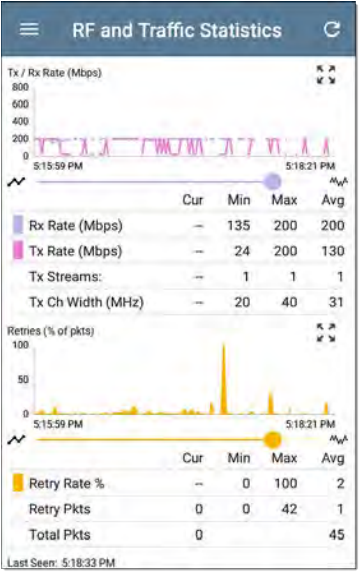
	Cur	Min	Max	Avg
CH Utilization	11	1	31	7
Client: 802.11	0	0	8	<1

NOTE: The **Sound** and **External Antenna** toggles are used for locating the device. See Locating Wi-Fi Devices.

The Utilization graph for Clients shows separate measurements for Channel (CH) Utilization and Client Utilization, using different colors.

See the Trending Graphs topic for an overview of the graph's pan and zoom controls.

The breaks in the Client RF and Traffic graphs occur because the Client is not consistently transmitting, so there is no data for EtherScope to display during those times.



RF and Traffic Statistics

	Cur	Min	Max	Avg
🟪 Rx Rate (Mbps)	–	135	200	200
🟥 Tx Rate (Mbps)	–	24	200	130
Tx Streams:	–	1	1	1
Tx Ch Width (MHz)	–	20	40	31

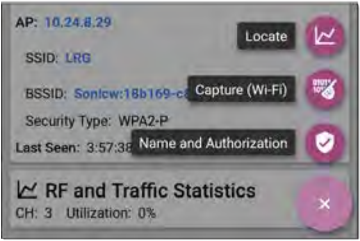
	Cur	Min	Max	Avg
🟧 Retry Rate %	–	0	100	2
Retry Pkts	0	0	42	1
Total Pkts	0			45

Last Seen: 5:18:33 PM

The Clients RF and Traffic Statistics screen also displays a graph of Transmit (Tx) and Receive (Rx) Rates in Mbps, number of Tx Streams, and Tx Channel Width in MHz.

Clients FAB

Tap the FAB on the Client Details screen to **Locate** the client device, open the **Capture** app and record a packet capture of traffic going to and from the client, or assign or change its **Name and Authorization**.



AP: 10.24.8.29

SSID: LRG

BSSID: Sonicw:18b169-c

Security Type: WPA2-P

Last Seen: 3:57:38

RF and Traffic Statistics

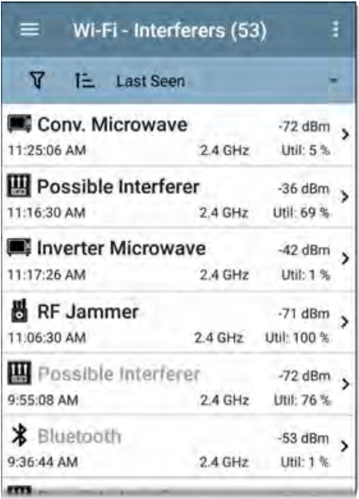
CH: 3 Utilization: 0%

- Selecting **Locate** opens the RF and Traffic Statistics screen where the sound and antenna controls are displayed. See Locating Wi-Fi Devices.
- Selecting **Capture** opens the Capture app populated with the Channel and MAC address of the client. See the Capture app chapter.

- Selecting **Name and Authorization** opens the Name and Authorization dialog. See Assigning a Name and Authorization to a Device.

Interferers

The Interferers screen displays devices detected by the EtherScope that may be interfering on your networks.



Wi-Fi - Interferers (53)

Last Seen

Conv. Microwave -72 dBm
11:25:06 AM 2.4 GHz Util: 5 %

Possible Interferer -36 dBm
11:16:30 AM 2.4 GHz Util: 69 %

Inverter Microwave -42 dBm
11:17:26 AM 2.4 GHz Util: 1 %

RF Jammer -71 dBm
11:06:30 AM 2.4 GHz Util: 100 %

Possible Interferer -72 dBm
9:55:08 AM 2.4 GHz Util: 76 %

Bluetooth -53 dBm
9:36:44 AM 2.4 GHz Util: 1 %

By default, Interferers are ordered by the time they were most recently detected by the

EtherScope. Each card shows the Last Seen time, the device's Power measurement in dBm, the frequency band on which it was detected, and its Utilization.

Refer to the Wi-Fi App List Screens topic if needed.

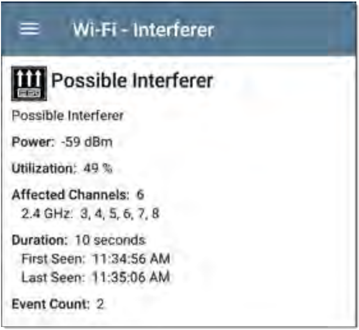
EtherScope can detect and display the following potential Interfering devices types:

- Baby Monitor
- Bluetooth
- DS Cordless Phone
- FH Cordless Phone
- Game Controller
- Possible Interferer
- Unknown Interferer
- RF Jammer
- YDI Narrowband Jammer
- Conventional Microwave
- Inverter Microwave
- Motion Detector

- Narrowband CW Signal
- Video camera

Touch an Interferer card to open the Details screen.

Interferer Details



Possible Interferer

Possible Interferer

Power: -59 dBm

Utilization: 49 %

Affected Channels: 6
2.4 GHz: 3, 4, 5, 6, 7, 8

Duration: 10 seconds
First Seen: 11:34:56 AM
Last Seen: 11:35:06 AM

Event Count: 2

Power: The most recently observed power output from the device

Utilization: The percentage of time, during the most recent sample, for which the interferer was detected

Affected Channels: The bands and channels on which EtherScope detects the interfering device

Duration: Amount of time EtherScope detected the device and when it was first and last detected

Event Count: Number of separate instances of detected transmission from the interferer

Path Analysis App

Path Analysis traces the connection points, including intermediate routers and switches, between the EtherScope nXG 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, EtherScope shows the number of hops to the destination device. A maximum of 30 hops can be reported.

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

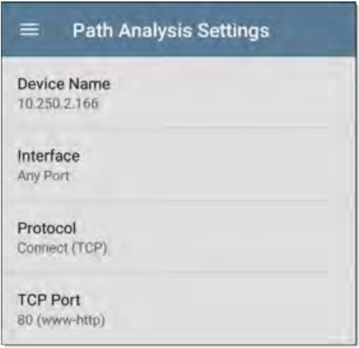
The Path Analysis source device is always your EtherScope nXG. The default destination is www.google.com.

Populating Path Analysis from Another App

Like other EtherScope 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, touch 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

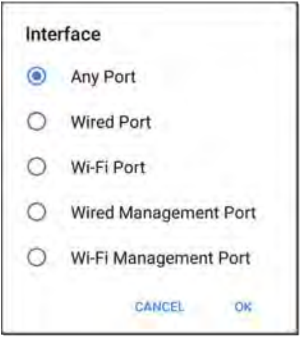
Protocol
Connect (TCP)

TCP Port
80 (www-http)

On the Path Analysis Settings screen, touch each field as needed to configure your target:

Device Name: Touch to enter the IP address or DNS name of the Path destination. The default is www.google.com.

Interface: This setting determines the EtherScope port from which the test runs. Touch the field to select Any Port, Wired Test Port, Wi-Fi Test Port, Wired Management Port, or Wi-Fi Management Port.



Interface

● Any Port

○ Wired Port

○ Wi-Fi Port

○ Wired Management Port

○ Wi-Fi Management Port

EtherScope 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.

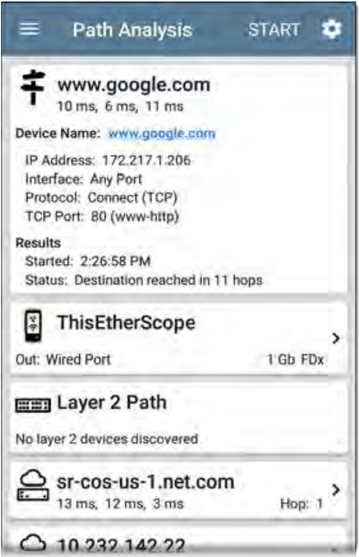
Protocol: Tap to select the Connect (TCP), Ping (ICMP), or Echo (UDP/7) protocol for your Path Analysis.

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

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

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



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

Device Name: www.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

ThisEtherScope
Out: Wired Port 1 Gb FDx

Layer 2 Path
No layer 2 devices discovered

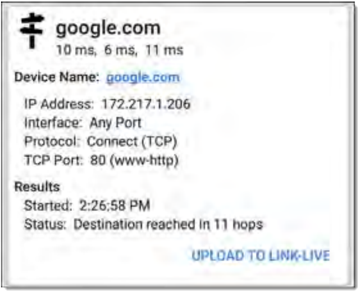
sr-cos-us-1.net.com
13 ms, 12 ms, 3 ms Hop: 1

10.232.142.22

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 EtherScope nXG), and the following cards show the Layer 2 and Layer 3 Hops in the path, which are sequentially ordered.

Touch any **blue linked name or address** in the Path Analysis results screens to open the Discovery or Wi-Fi app and further examine the linked element.

Path Analysis Results and Source EtherScope 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

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.

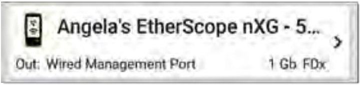
Results

Started: Time at which the Path Analysis began

Status: Current status of the Path Analysis test, including any error messages

UPLOAD TO LINK-LIVE: Touch this link to upload your results to a Link-Live account. See Uploading Path Analysis Results to Link-Live later in this topic.

Source EtherScope Card



Angela's EtherScope nXG - 5...

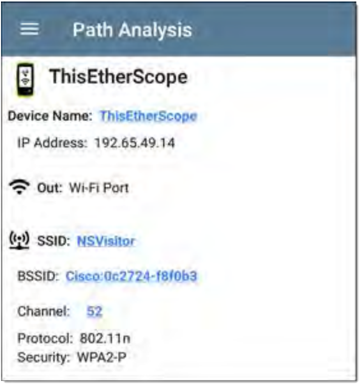
Out: Wired Management Port 1 Gb FDx

The source This EtherScope card displays the port from which the Path Analysis ran.

- For Wired Test or Management port analyses (shown above), this card displays connection speed and duplex.
- For Wi-Fi port analyses, the card displays the SSID and channel number.

  NOTE: This card and screen only display a custom name for your EtherScope if you have claimed it to Link-Live.

Touch the card to view more details.



ThisEtherScope

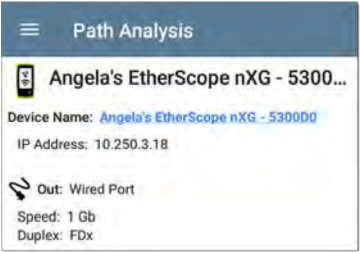
Device Name: ThisEtherScope
IP Address: 192.65.49.14

Out: Wi-Fi Port

SSID: NSVisitor
BSSID: Cisco:0c2724-f8f0b3
Channel: 52
Protocol: 802.11n
Security: WPA2-P

The example image above shows the SSID, Channel, and other Wi-Fi information the EtherScope can display after running a Path Analysis over Wi-Fi.

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



Angela's EtherScope nXG - 5300...

Device Name: Angela's EtherScope nXG - 5300D0

IP Address: 10.250.3.18

Out: Wired Port

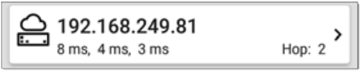
Speed: 1 Gb

Duplex: FDx

Beneath the EtherScope 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.



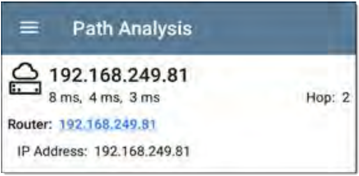
192.168.249.81

8 ms, 4 ms, 3 ms

Hop: 2

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.

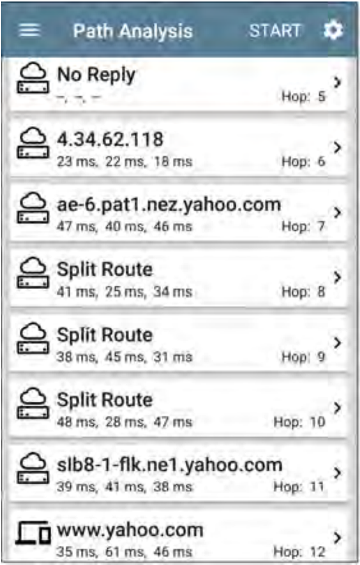
Touch the card to view the hop Details screen.



192.168.249.81
8 ms, 4 ms, 3 ms
Hop: 2
Router: 192.168.249.81
IP Address: 192.168.249.81

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.



No Reply
-, -, -
Hop: 5

4.34.62.118
23 ms, 22 ms, 18 ms
Hop: 6

ae-6.pat1.nez.yahoo.com
47 ms, 40 ms, 46 ms
Hop: 7

Split Route
41 ms, 25 ms, 34 ms
Hop: 8

Split Route
38 ms, 45 ms, 31 ms
Hop: 9

Split Route
48 ms, 28 ms, 47 ms
Hop: 10

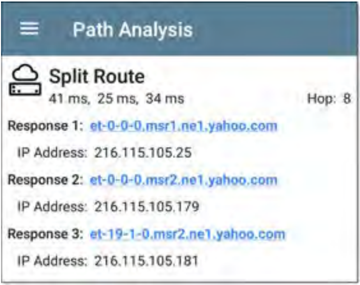
slb8-1-flk.ne1.yahoo.com
39 ms, 41 ms, 38 ms
Hop: 11

www.yahoo.com
35 ms, 61 ms, 46 ms
Hop: 12

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.

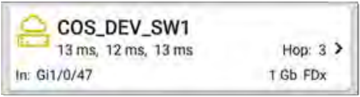


Split Route
41 ms, 25 ms, 34 ms Hop: 8

Response 1: et-0-0-0.msr1.ne1.yahoo.com
IP Address: 216.115.105.25
Response 2: et-0-0-0.msr2.ne1.yahoo.com
IP Address: 216.115.105.179
Response 3: et-19-1-0.msr2.ne1.yahoo.com
IP Address: 216.115.105.181

Layer 3 Interfaces and Statistics

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



COS_DEV_SW1
13 ms, 12 ms, 13 ms Hop: 3
In: Gi1/0/47 1 Gb FDx

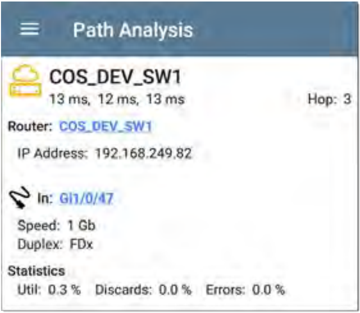
Touch a Hop card to see a summary of Interface Details and Statistics, if they are available.

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.



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 %

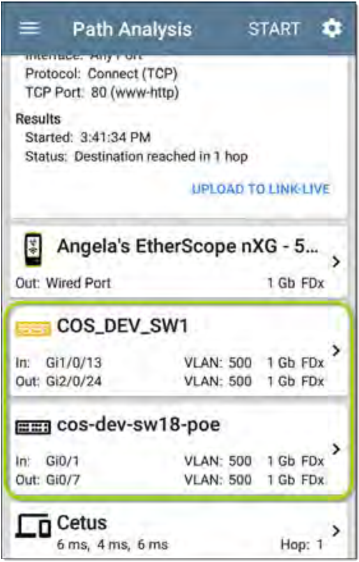
Tapping the blue linked switch name will open a Discovery Details screen for the switch, where the user can investigate the cause of the Warning.

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.



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

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

Angela's EtherScope nXG - 5...
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

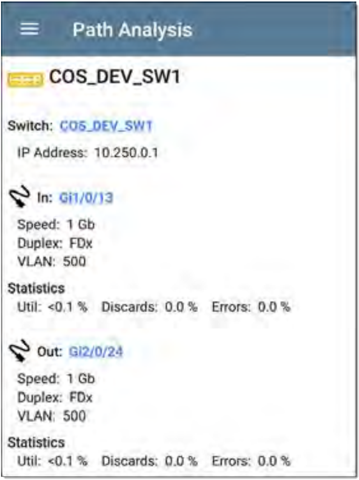
cos-dev-sw18-poe
In: Gi0/1 VLAN: 500 1 Gb FDx
Out: Gi0/7 VLAN: 500 1 Gb FDx

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

The EtherScope 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.

Touching a Layer 2 card opens a Details screen for the device.



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 EtherScope 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

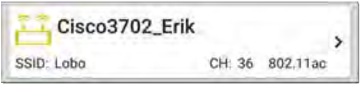
Discards: Percentage of total packets that have been dropped

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.

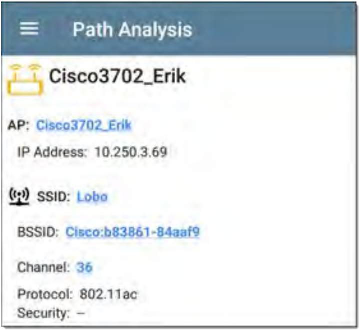
A Layer 2 AP card indicates the connected network SSID, channel, and 802.11 type in use.



Cisco3702_Erik

SSID: Lobo CH: 36 802.11ac

Layer 2 AP Details screens allow you to further examine the wireless characteristics by selecting their blue links, which open a Wi-Fi app Details screen.



Path Analysis

Cisco3702_Erik

AP: Cisco3702_Erik

IP Address: 10.250.3.69

SSID: Lobo

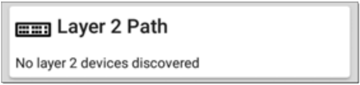
BSSID: Cisco:b83861-84aaf9

Channel: 36

Protocol: 802.11ac

Security: –

No layer 2 devices discovered



Layer 2 Path

No layer 2 devices discovered

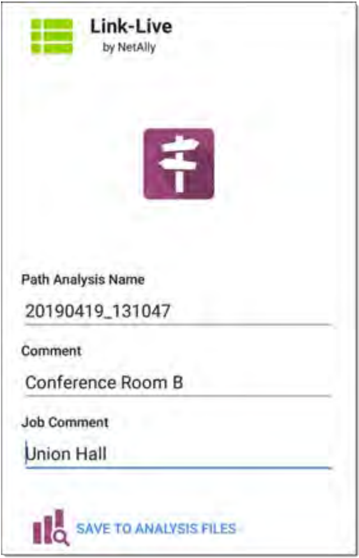
In some cases, the EtherScope does not discover Layer 2 devices between Layer 3 devices. There may not be any Layer 2 devices, or EtherScope might not have SNMP access to those switches.

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 Path Analysis Results to Link-Live

Touching the **UPLOAD TO LINK-LIVE** link on the top card opens the Link-Live sharing screen for path analysis results:



Path Analysis Name

20190419_131047

Comment

Conference Room B

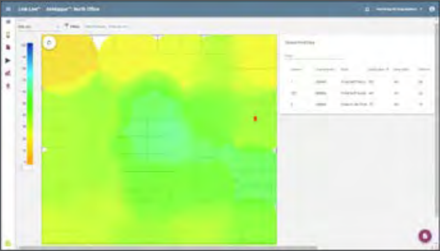
Job Comment

Union Hall

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

AirMapper™ App

The AirMapper Site Survey application enables you to perform a Wi-Fi survey of an indoor or outdoor location and upload it to Link-Live Cloud Service. On Link-Live.com, you can view heatmaps and Wi-Fi measurements for each data collection point.



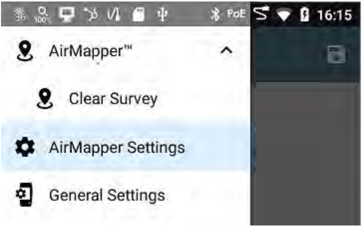
The Signal heatmap is available to all Link-Live users. **AllyCare** Support customers can also view maps of Noise, SNR, and Max TX and RX Rates. Visit NetAlly.com/Support.

AirMapper Settings

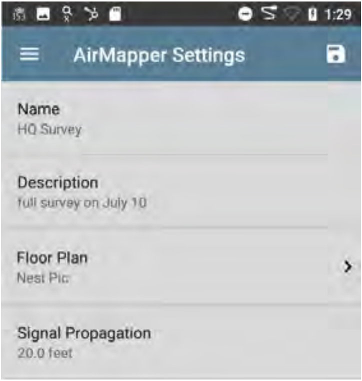
Setting up the AirMapper app to perform a survey involves naming the survey, loading a floor plan image, specifying its dimensions, setting scanning mode, and overriding bands and channels.

- Only .png and .jpg image files types are supported.
- You may need to use an image editing application to crop your floor plan image to known dimensions, such as the walls of a building or property boundary.

Access the AirMapper settings by selecting the menu icon ☰ or settings icon ⚙ at the top of the main app screen.



Configuring an AirMapper Survey



Name
HQ Survey

Description
full survey on July 10

Floor Plan
Nest Pic

Signal Propagation
20.0 feet

Name

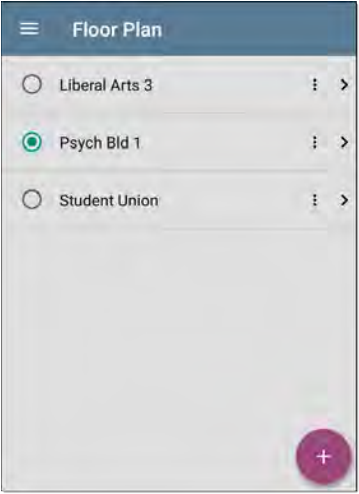
Touch the **Name** field to enter a custom name for your AirMapper project. This name is uploaded to Link-Live to identify this survey project.

Description

Enter any additional information you want for the survey.

Floor Plan

1. Open the Floor Plan list screen to select or load a new floor plan or map of the area to be surveyed.



Floor Plan

○ Liberal Arts 3

● Psych Bld 1

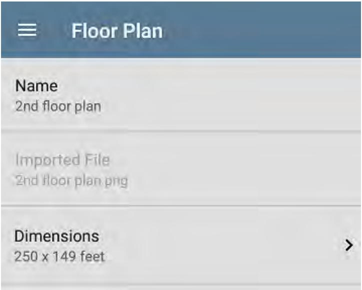
○ Student Union

2. On the Floor Plan screen, tap the floating action button + to load a new image file

into the AirMapper app. The EtherScope opens the Files app.

3. Navigate to the map image file in the file system, and touch to select it.

4. Back on the Floor Plan screen, tap the fields to configure the floor plan.



Name
2nd floor plan

Imported File
2nd floor plan.png

Dimensions
250 x 149 feet

Name: Enter a name for this floor plan. This field defaults to the file name.

Imported File: The original image filename

Interactive Calibration: In the Floor Plan menu pressing on Dimensions allows the user to interactively calibrate the floorplan by moving the two indicators to known locations and entering the corresponding distance between the two points.

The units (feet or meters) displayed in the AirMapper app are set in the General Settings for the test apps, accessed from the left-side navigation drawer ☰.

Touch back ◁ to return to the main AirMapper settings.

Signal Propagation

This setting is the radius measurement of the sample points. Touch the field to adjust the size of the data points on the map.

When you finish configuring, touch ◁ to return to the main AirMapper screen.

Wi-Fi General Settings that Affect AirMapper

See the Wi-Fi heading in General Settings for longer descriptions of the **Wi-Fi Bands and Channels** and **Dwell Time** settings. These settings control which bands and channels EtherScope scans during a survey and how longs it lingers on each channel to gather data.

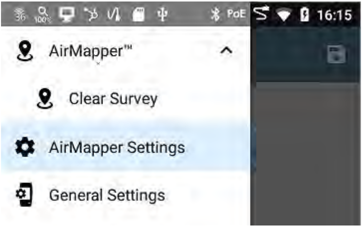
NOTE: For the best AirMapper results, we recommend setting a **Dwell Time** of **250 ms** or greater.

For faster AirMapper scans, enable only the **Wi-Fi Bands and Channels** of interest.

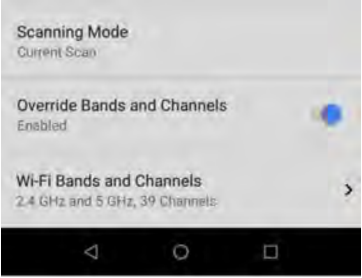
Override Bands and Channels

EtherScope AirMapper supports the selection of different channels, bands and dwell time from the values defined in General Settings. These override settings are only used during a site survey.

To set survey-specific settings, select the menu icon ☰ or settings icon ⚙ at the top of the AirMapper screen.



From the AirMapper Settings screen, enable the Override Bands and Channels selection.

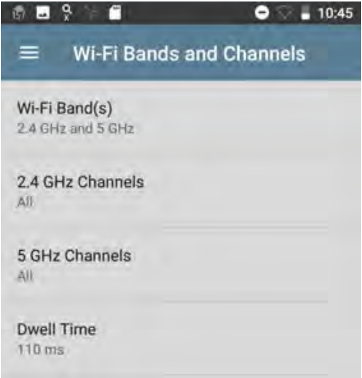


Scanning Mode
Current Scan

Override Bands and Channels
Enabled

Wi-Fi Bands and Channels
2.4 GHz and 5 GHz, 39 Channels

Select Wi-Fi Bands and Channels to modify AirMapper channels, bands and dwell time.



Wi-Fi Bands and Channels

Wi-Fi Band(s)
2.4 GHz and 5 GHz

2.4 GHz Channels
All

5 GHz Channels
All

Dwell Time
110 ms

Set the bands, channels and dwell time that meet the specific requirements of the AirMapper survey.

Note: Selecting a subset of channels and bands improves the survey performance as unnecessary channels are not included in the scanning process and it removes extraneous data from the survey.

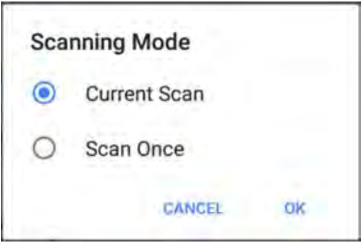
Scanning Mode

Scanning Mode provides two Wi-Fi data collection methods:

1. Current Scan is the default and preferred way to perform a survey. It allows immediate data collection based on the most recent Access Point beacon seen from each BSSID. Beacons are aged-out after 30 seconds.

2. Scan Once is a more precise and time-consuming mode. When a point is selected, all the BSSID information is cleared, and a single scan of the selected channels for the selected dwell time is acquired. This is an exact measurement but in congested environments beacons not seen during the dwell time are not included in that sample point.

To set the AirMapper scanning mode, select Scanning Mode from AirMapper Settings screen.



Scanning Mode

● Current Scan

○ Scan Once

Select the scan mode which best suits your Wi-Fi environment and survey data collection requirements.

Changing Settings after Starting

Once you **START** your survey on the main AirMapper screen, with the **Override Bands and Channels** settings enabled, you can revisit the Wi-Fi Bands and Channels to adjust **Bands and Channels** or **Dwell Time**; with the **Override Bands and Channels** disabled, you can still revisit the General Settings to adjust **Bands and Channels** or **Dwell Time**.

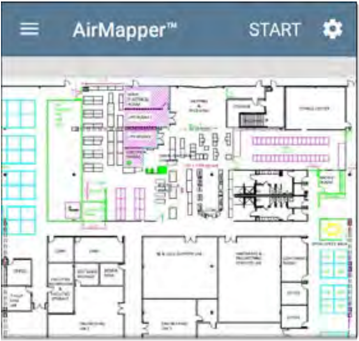
You can also reopen the AirMapper settings to change the **Floor Plan > Dimensions** or **Signal Propagation** size. Existing data points are retained on the map unless you select a different Floor Plan.

Hidden SSIDs and APs

For any [Hidden] APs or SSIDs at your site that you want detected during a survey, we recommend creating and enabling a Wi-Fi Profile in the AutoTest app, configured with the appropriate credentials. Otherwise, AirMapper will detect the BSSIDs associated with hidden devices but may not determine their APs/SSIDs.

Collecting AirMapper Data

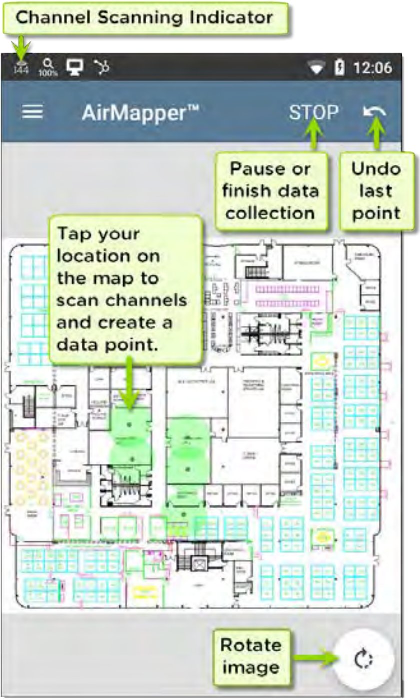
Once selected, your floor plan appears on the main AirMapper screen.



Touch **START** to begin the survey.

To collect data, travel around your site, and touch the map at your current location to scan the enabled wireless channels in that spot.

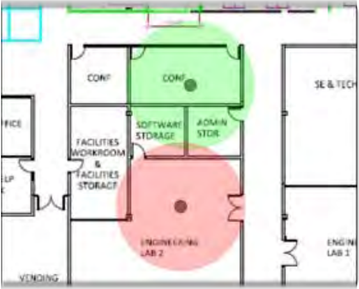
Do not move from that location until the scan is complete and the data point on the screen turns from red to green.


Channel Scanning Indicator
144
100%
12:06
AirMapper™
STOP
Pause or finish data collection
Undo last point
Tap your location on the map to scan channels and create a data point.
Rotate image

As shown in the image above, you can undo previous collection points and rotate the image as needed.

Use swiping and pinch-to-zoom gestures to pan and zoom the map.

While the EtherScope is scanning, the Signal Propagation circle is red. Once the scan is complete, the circle turns green.

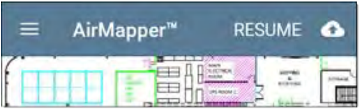


The completed data points in the AirMapper app are always green. The colored heatmap is generated once you upload the AirMapper results to Link-Live.

Watch the Wi-Fi status icon 64 in the top status bar to see the channels the EtherScope is scanning in real time.

> NOTE: To adjust the **Dwell Time**, meaning the amount of time the EtherScope lingers on each channel gathering data, enable the Override Bands and Channels and open the Wi-Fi Bands and Channels, or open the General Settings > **Wi-Fi Bands and Channels**, accessed from the left-side navigation drawer. For the best AirMapper results, we recommend setting a **Dwell Time** of **250 ms** or greater.

When you finish adding data points, or if you want to pause, touch **STOP**.

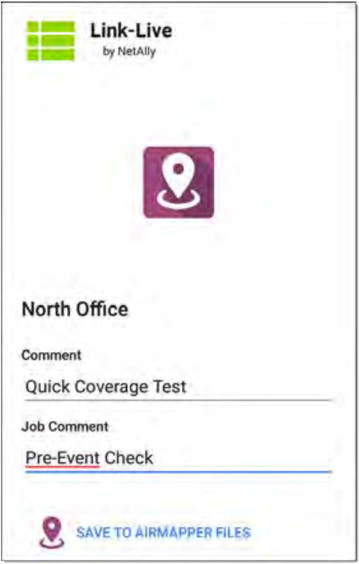


Touch **RESUME** to add more data points.

Touch the Link-Live upload icon to send your survey results to Link-Live's AirMapper page.

Uploading AirMapper Surveys to Link-Live

When you touch the upload icon ⇪, select **Upload to Link-Live** to display the Link-Live sharing screen.



North Office

Comment
Quick Coverage Test

Job Comment
Pre-Event Check

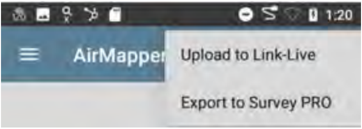
Enter any **Comments** you want attached to your AirMapper result in Link-Live, and tap **SAVE TO AIRMAPPER FILES**.

The current survey remains on the AirMapper screen until you **Clear Survey**, allowing you to add additional points if needed and re-upload.

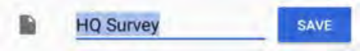
Export AirMapper Data to AirMagnet Survey PRO

Survey data can be exported as a .amp file for import into AirMagnet Survey PRO version 10 for more advanced analysis, planning and reporting.

When your survey data collection is complete, touch the upload icon and select **Export to Survey PRO** to create the .amp file.



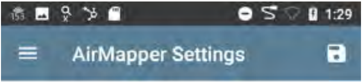
Optionally rename the .amp file and select the Save button to create the .amp file.



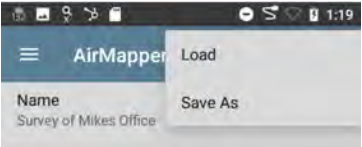
You can copy the file to external storage at a later time using the Files app.

Load and Save AirMapper Settings

The entire survey configuration can be saved as named settings using the disk icon in the title bar.



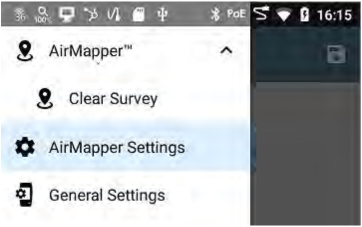
This allows fast recall of any specific survey configuration.



Name
Survey of Mikes Office

Starting a New Survey

To start a new AirMapper survey, open the left-side drawer and select **Clear Survey**.


PoE
16:15
AirMapper™
Clear Survey
AirMapper Settings
General Settings

Performance Test App

The EtherScope nXG'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 EtherScope, 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 EtherScope reports round-trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

The EtherScope nXG 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 EtherScope nXG or a OneTouch AT 10G.

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

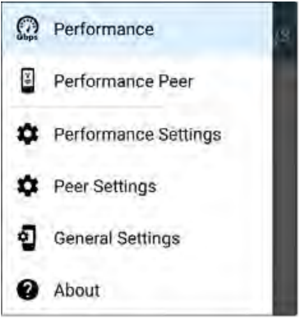
- **OneTouch AT 10G** can act as the Source or a Peer for Performance tests. (NetAlly.com/products/OneTouch)
- **LinkRunner AT** and **LinkRunner G2** each have a Reflector feature for exchanging Performance test traffic. (NetAlly.com/products/LinkRunner G2)
- NetAlly's **Network Performance Test (NPT)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

In this Chapter

Performance Test Settings

The Performance app has both **Performance** settings that apply when the EtherScope 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 touching 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 EtherScope is the source.

Peer Settings control the EtherScope Performance Peer when another device is the source. See Running EtherScope nXG as a Performance Peer.

Saving Custom Performance Tests

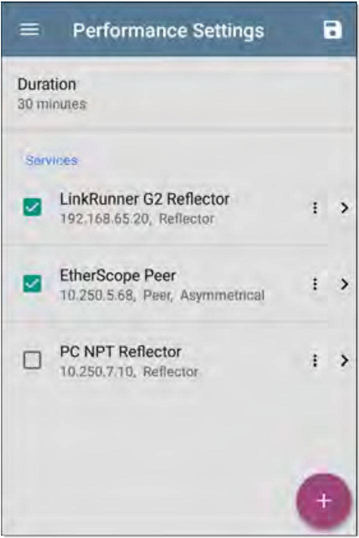
The Performance app allows you to save two levels of test configurations: individual **Services** and complete **Performance Tests** with *up to four* enabled Services.

- **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

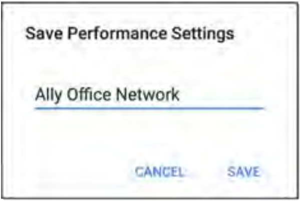
☐ PC NPT Reflector
10.250.7.10, Reflector

Touch 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.

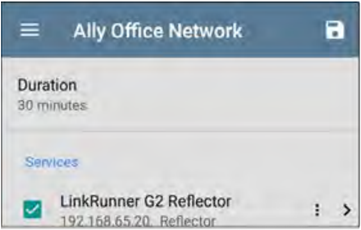
See Saving App Settings Configurations for more instructions.



Save Performance Settings

Ally Office Network

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



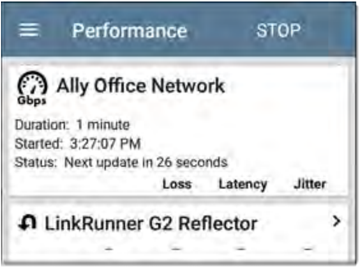
Ally Office Network

Duration
30 minutes

Services

☑ LinkRunner G2 Reflector
192.168.65.20, Reflector

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).



Performance STOP

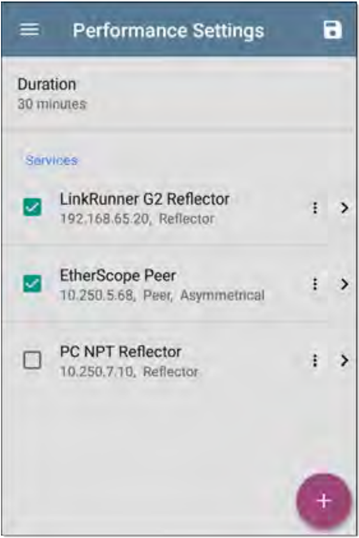
Ally Office Network
Gbps

Duration: 1 minute
Started: 3:27:07 PM
Status: Next update in 26 seconds

	Loss	Latency	Jitter
LinkRunner G2 Reflector	–	–	–

Configuring the Source EtherScope nXG

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 will run. 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 EtherScope 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 a Service from the currently active Performance Test.

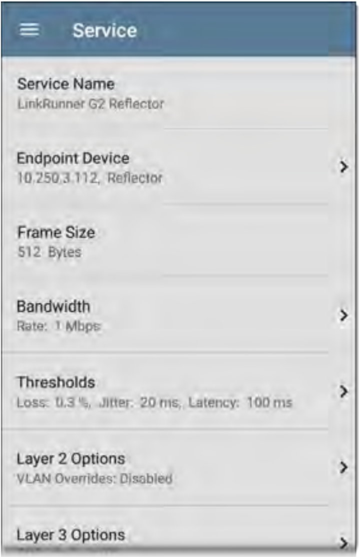
  NOTE: Only four services can be tested at once. If you select more than four services, the Performance Test will fail.

- Touch 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.

- Touch the FAB icon ⊕ to add a new Service.

- Touch 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 Name
LinkRunner G2 Reflector

Endpoint Device
10.250.3.112, Reflector

Frame Size
512 Bytes

Bandwidth
Rate: 1 Mbps

Thresholds
Loss: 0.3 %, Jitter: 20 ms, Latency: 100 ms

Layer 2 Options
VLAN Overrides: Disabled

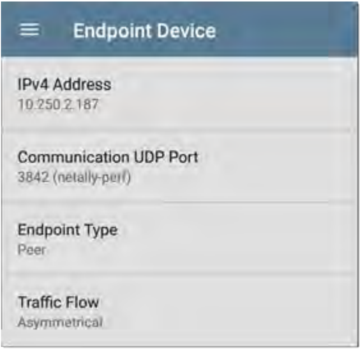
Layer 3 Options

Service Name

Touch 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.



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, touch 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.

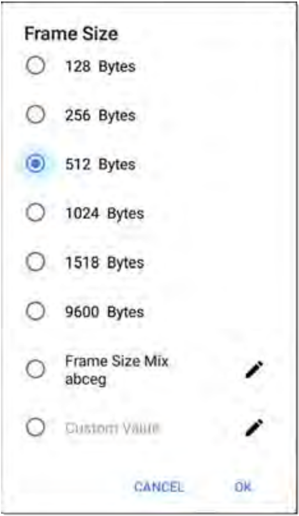
Endpoint Type: Select **Peer** or **Reflector** depending on the type of endpoint you are using for the performance test.

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

Touch 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

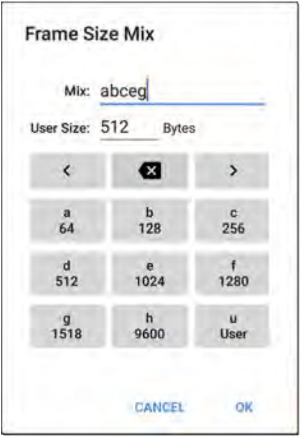
○ 1518 Bytes

○ 9600 Bytes

○ Frame Size Mix abceg ✏

○ Custom Value ✏

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

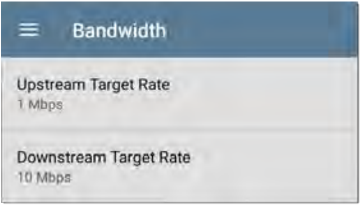
On the Frame Size Mix keyboard shown above, each letter (a through h) is associated with a frame size. The default pattern is "abceg," meaning the traffic pattern will follow a repeating sequence of 64, 128, 256, 1024, and 1518 bytes. Use the letter keys along with the arrows and backspace button to 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. Touch 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 will be four bytes longer. You do not need to account for this frame size increase in the settings.

Bandwidth

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

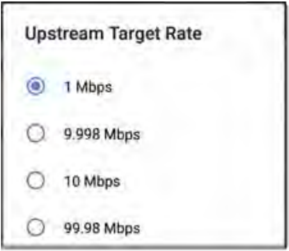


Upstream Target Rate
1 Mbps

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.

Touch the **Target Rate** field(s) to select or enter a new rate. The default is 1 Mbps.



Upstream Target Rate

● 1 Mbps

○ 9.998 Mbps

○ 10 Mbps

○ 99.98 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.

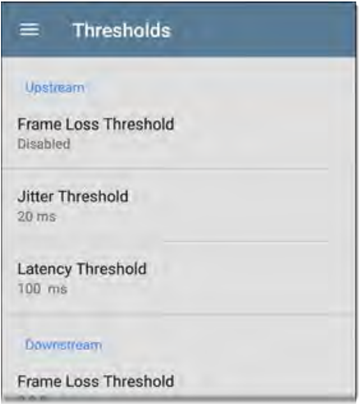
> NOTE: The 99.98 Mbps and similar values provided in the Target Rate options are meant to test the maximum, worst case throughput on an Ethernet link. Though greater rates are possible under perfect conditions, the limitation of 99.98% of the link rate results from asynchronous clocks in Ethernet. The 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 EtherScope 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.



Upstream

Frame Loss Threshold
Disabled

Jitter Threshold
20 ms

Latency Threshold
100 ms

Downstream

Frame Loss Threshold

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.

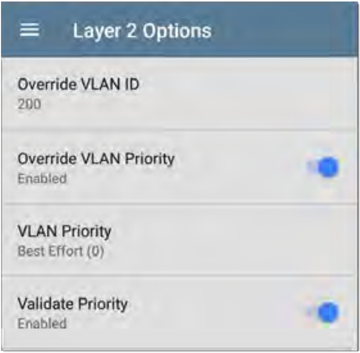
Latency Threshold: Latency is the amount of time it takes for a packet to go from the source to the endpoint and endpoint to source in milliseconds. The default threshold is 100 ms.

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.



Layer 2 Options

Override VLAN ID
200

Override VLAN Priority
Enabled

VLAN Priority
Best Effort (0)

Validate Priority
Enabled

Override VLAN ID: Touch 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.

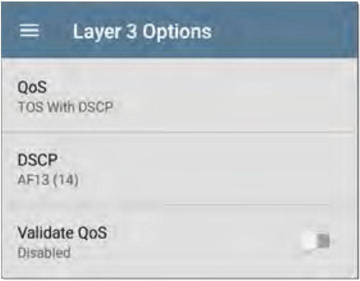
Override VLAN Priority: Touch the toggle button to enable. By default, the VLAN priority is set to Best Effort (0). Use this setting to simulate a traffic stream of a certain type. If Override VLAN Priority is not enabled, the VLAN priority is set to the value used for the Wired Test port.

VLAN Priority: This setting only appears if the **Override VLAN Priority** setting above is Enabled. Touch to select a VLAN Priority.

Validate Priority: Touch the toggle button to enable the EtherScope to validate the selected VLAN priority. When the Validate Priority option is enabled, EtherScope 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.



QoS
TOS With DSCP

DSCP
AF13 (14)

Validate QoS
Disabled

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.” Touch the field to select a different DSCP.

IP Precedence: This field is only available when **TOS with IP Precedence** is selected. Touch 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. Touch the field to select an IP Precedence Type other than the default of Normal (0).

Validate QoS: When this setting enabled, the EtherScope 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.

Back to Title and Contents

Configuring Performance Endpoints

EtherScope nXG can run a Performance Test to any of the following Endpoints:

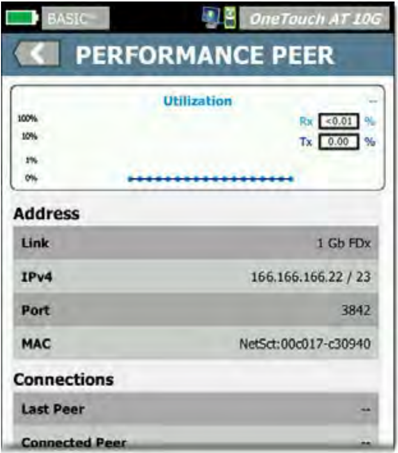
- Another EtherScope nXG (Peer)
- A OneTouch AT 10G (Peer)
- A LinkRunner G2 or LinkRunner AT (Reflector)
- NPT Reflector Software (Reflector)

See our website NetAlly.com for more information about OneTouch and LinkRunner and to download the free NPT Reflector PC application.

EtherScope Performance Peer

To run an EtherScope nXG as a Performance Peer, see the Running as a Performance Peer topic.

OneTouch 10G Performance Peer



Rx <0.01 %

Tx 0.00 %

Address

Link	1 Gb FDx
IPv4	166.166.166.22 / 23
Port	3842
MAC	NetSct:00c017-c30940

Connections

Last Peer	--
Connected Peer	--

Follow these steps to set up a OneTouch 10G Performance Peer:

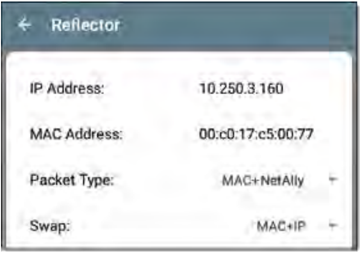
1. Ensure the OneTouch is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.

2. With the unit powered on, touch 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 EtherScope.
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 EtherScope nXG's Performance test Services settings.

For additional details on the OneTouch Performance Peer, see the OneTouch 10G User Manual, available online.

LinkRunner G2 Reflector



IP Address: 10.250.3.160

MAC Address: 00:c0:17:c5:00:77

Packet Type: MAC+NetAlly

Swap: MAC+IP

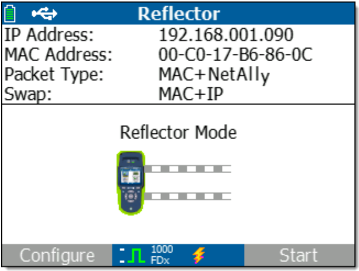
Follow these steps to set up a LinkRunner G2 Reflector:

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 touching the NetAlly logo at the bottom of the screen.

3. In the testing app, open the left-side navigation drawer by touching 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 EtherScope nXG'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

Reflector Mode

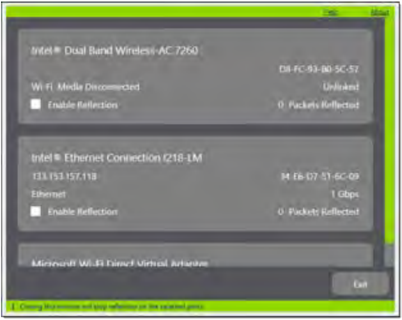
Follow these steps to set up a LinkRunner AT (2000) Reflector:

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 EtherScope nXG'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



Intel® Dual Band Wireless-AC 7260

D8-FC-93-B0-5C-57

Wi-Fi Media Disconnected   Unlinked

□ Enable Reflection   0 Packets Reflected

Intel® Ethernet Connection I218-LM

133.153.157.118   34-E6-D7-51-6C-09

Ethernet   1 Gbps

□ Enable Reflection   0 Packets Reflected

Microsoft Wi-Fi Direct Virtual Adapter

Closing this window will stop reflection on the selected ports

Follow these steps to set up the NPT Reflector PC application:

1. Download the software from NetAlly.com/support/downloads. Select EtherScope nXG 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 EtherScope nXG's Performance Test Services settings.

Refer to the **Help** in the NPT Reflector software for additional information.

Running a Performance Test

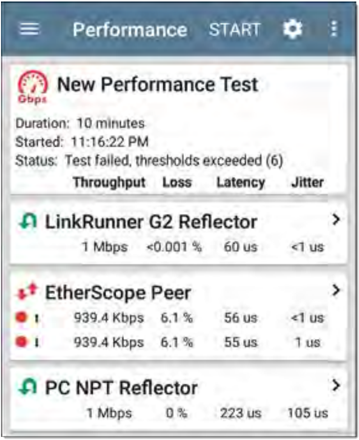
Note the following before running:

- 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 will fail with the Status message, "Too many services enabled (56)."

- Newly configured Services may not display on the main Performance Test screen until you touch START.

To run your configured Performance Test, touch **START** on the main Performance screen.

Performance Test Results



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 EtherScope nXG 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

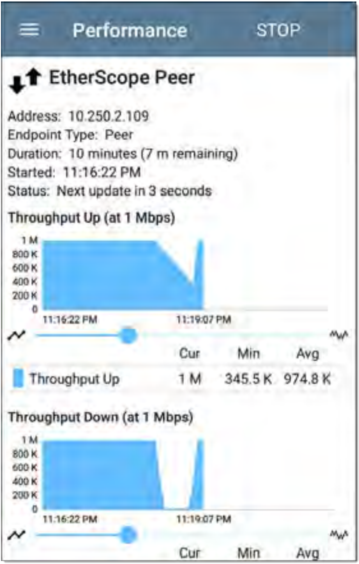
Started: Time at which the test began

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.

Touch a Service card to view more details.

Performance Service Detailed Results



EtherScope Peer

Address: 10.250.2.109
Endpoint Type: Peer
Duration: 10 minutes (7 m remaining)
Started: 11:16:22 PM
Status: Next update in 3 seconds

Throughput Up (at 1 Mbps)

	Cur	Min	Avg
Throughput Up	1 M	345.5 K	974.8 K

Throughput Down (at 1 Mbps)

The Service results screen displays detailed test characteristics and graphs of performance.

Address: IP address of the endpoint

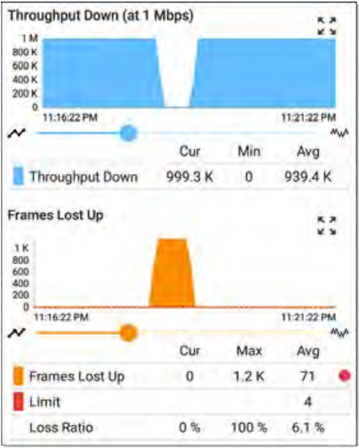
Endpoint Type: Peer or Reflector

Status: Current status of the test, including any error messages

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.



Throughput Down (at 1 Mbps)

	Cur	Min	Avg
🟦 Throughput Down	999.3 K	0	939.4 K

Frames Lost Up

	Cur	Max	Avg	
🟧 Frames Lost Up	0	1.2 K	71	●
🟥 Limit			4	
Loss Ratio	0 %	100 %	6.1 %	

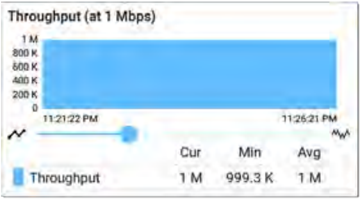
Touch and drag (or swipe) left and right on each graph to move backward and forward in time, and double tap or move the slider to zoom in and out. See the Trending Graphs topic for an overview of the graph's pan and zoom controls.

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

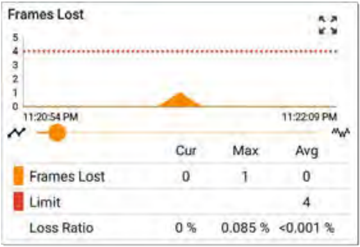


	Cur	Min	Avg
🟦 Throughput	1 M	999.3 K	1 M

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



	Cur	Max	Avg
🟧 Frames Lost	0	1	0
🟥 Limit			4
Loss Ratio	0 %	0.085 %	<0.001 %

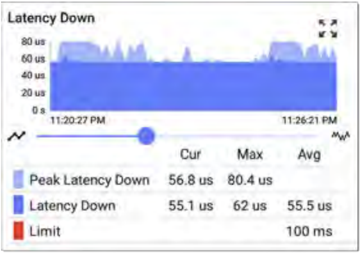
Frames Lost (Up/Down): Frame loss is quantified by the number of frames received subtracted from the number of frames sent.

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 user's clothing or interference from electrical appliances or 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

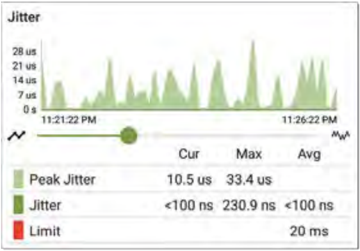


	Cur	Max	Avg
🟦 Peak Latency Down	56.8 us	80.4 us	
🟦 Latency Down	55.1 us	62 us	55.5 us
🟥 Limit			100 ms

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.



	Cur	Max	Avg
🟩 Peak Jitter	10.5 us	33.4 us	
🟩 Jitter	<100 ns	230.9 ns	<100 ns
🟥 Limit			20 ms

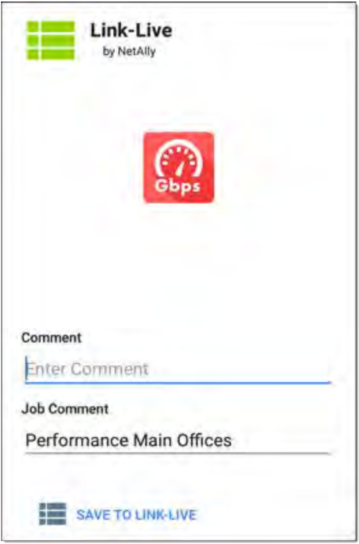
Jitter (Up/Down): Jitter is a measure of the variation in frame-to-frame latency in milliseconds.

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 Performance Results to Link-Live

Touch 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.



Comment

Enter Comment

Job Comment

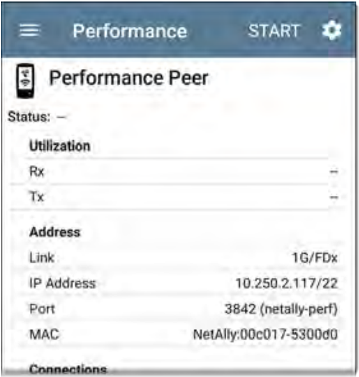
Performance Main Offices

See the Link-Live chapter for more information.

Running EtherScope as a Performance Peer

In addition to running a Performance Test as the controlling source device, EtherScope nXG can also act as a Peer for another EtherScope nXG or a OneTouch AT 10G acting as the source and controller.

To access the EtherScope Performance Peer, tap the menu button ☰ in the Performance app and select **Performance Peer**.



Performance Peer

Status: –

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

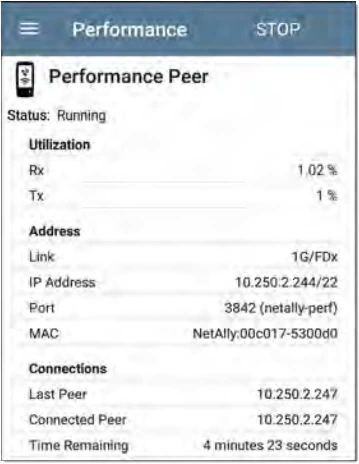
The only setting for the Performance Peer function is the **Communication UDP Port**.

Touch 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 Peer

Status: Running

Utilization

Rx 1.02 %

Tx 1 %

Address

Link 1G/FDx

IP Address 10.250.2.244/22

Port 3842 (netally-perf)

MAC NetAlly:00c017-5300d0

Connections

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 EtherScope to be entered into the controlling source device

Port: UDP Communication port in use by the peer

MAC: The EtherScope's MAC address

Connections

Last Peer: Address of the previous peer that was connected to the EtherScope

Connected Peer: Address of the peer that is currently connected to the EtherScope

Time Remaining: Amount of time left for the current test

Back to Title and Contents

iPerf Test App

iPerf is a standardized network performance tool used to measure UDP or TCP throughput and loss.

The iPerf app runs an iPerf3 performance test to a NetAlly Test Accessory or an iPerf server endpoint.

The NetAlly Test Accessory runs network connection tests, uploads results to Link-Live Cloud Service, and acts as an iPerf server endpoint for iPerf tests run by other NetAlly handheld testers.

Learn more about the Test Accessory from NetAlly.com/products/TestAccessory.

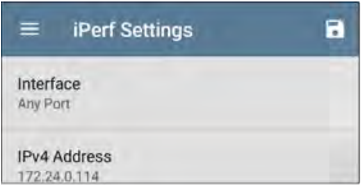
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the EtherScope iPerf test. You can download iPerf server software from https://iperf.fr.

iPerf Settings

To run an iPerf test, you must configure your EtherScope 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.



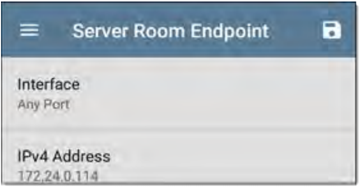
iPerf Settings

Interface
Any Port

IPv4 Address
172.24.0.114

Touch the save icon 💾 to load, save, import, and export configured settings. See Saving App Settings Configurations for more instructions.

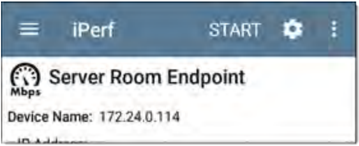
Once you save a settings configuration, the custom name you entered appears at the top of the iPerf settings and results screens. In the example images here, the user has saved a custom iPerf configuration called "Server Room Endpoint."



Server Room Endpoint

Interface
Any Port

IPv4 Address
172.24.0.114



Server Room Endpoint

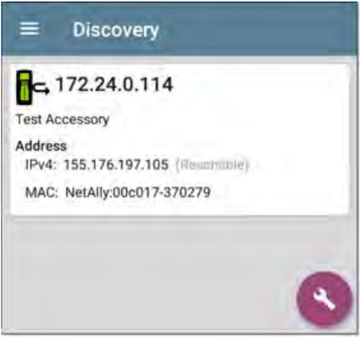
Device Name: 172.24.0.114

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.



172.24.0.114

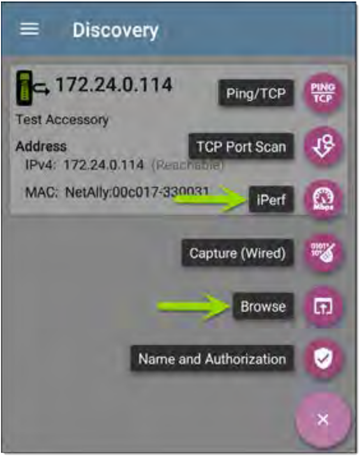
Test Accessory

Address

IPv4: 155.176.197.105 (Reachable)

MAC: NetAlly:00c017-370279

2. Open the floating action button (FAB) menu.



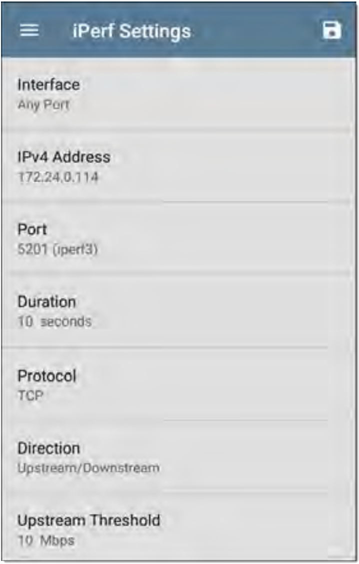
NOTE: You can select **Browse** in the floating action menu to open the Test Accessory's Web Interface, where you can view its status and configure its settings.

3. Then, select the **iPerf** app button.

The iPerf app opens with the IP address populated from the Test Accessory in Discovery.

Configuring iPerf Settings

To configure the iPerf test settings manually, open the settings ⚙ on the iPerf screen.



Interface
Any Port

IPv4 Address
172.24.0.114

Port
5201 (iperf3)

Duration
10 seconds

Protocol
TCP

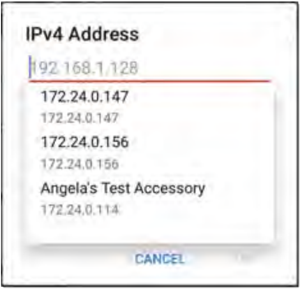
Direction
Upstream/Downstream

Upstream Threshold
10 Mbps

Touch 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 determines the EtherScope port from which the test runs. Touch the field to select Any Port, Wired or Wi-Fi Test Port, or Wired or Wi-Fi Management Port. See Test and Management Ports for explanations of the different ports.

IPv4 Address: Touch the field to enter or select the IPv4 address of the target iPerf server. Only IPv4 addresses are allowed for iPerf testing.



IPv4 Address

192.168.1.128

172.24.0.147
172.24.0.147

172.24.0.156
172.24.0.156

Angela's Test Accessory
172.24.0.114

A drop-down list in the IPv4 Address dialog shows all the Test Accessories the EtherScope has discovered through the discovery process, as well as any Test Accessories that are claimed to the same Link-Live organization as your EtherScope.

> NOTE: Clear the address field in the dialog to see the full list of discovered Test Accessory addresses.

Port: The default iPerf3 port number is 5201. Tap the field to enter a different port number.

> NOTE: The iPerf port number entered here must match the port number used by your iPerf server. If needed, consult the Test Accessory User Guide (NetAlly.com/products/TestAccessory).

Duration: This setting is the length of time for one direction, Upstream or Downstream, of the iPerf test. If the Direction setting below is set to both Upstream/Downstream, the total test time will be 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. Touch this field to set the test for only one direction.

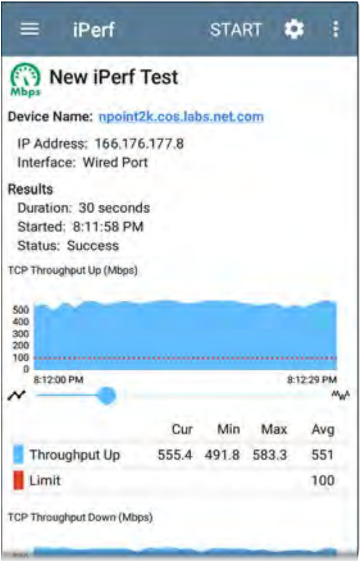
Upstream and Downstream Bandwidth: These fields only appear if the **UDP Protocol** is selected. They specify the desired target bandwidth for the iPerf Test using the UDP protocol.

Upstream and Downstream Thresholds: Thresholds are the values the EtherScope 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 or Management Port) from which you are running the iPerf test. Wired and Wi-Fi test ports require that an AutoTest Wired or Wi-Fi Profile has run to establish link. The AutoTest Wired Profile runs automatically, but you must open the AutoTest app to run a Wi-Fi Profile and link on the Wi-Fi test port. Management ports link automatically if a connection is available.

Tap the **START** button on the main iPerf screen to begin testing.



New iPerf Test

Device Name: npoint2k.cos.labs.net.com

IP Address: 166.176.177.8
Interface: Wired Port

Results
Duration: 30 seconds
Started: 8:11:58 PM
Status: Success

TCP Throughput Up (Mbps)

	Cur	Min	Max	Avg
🟦 Throughput Up	555.4	491.8	583.3	551
🟥 Limit				100

TCP Throughput Down (Mbps)

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 EtherScope Test or Management Port from which the test is running

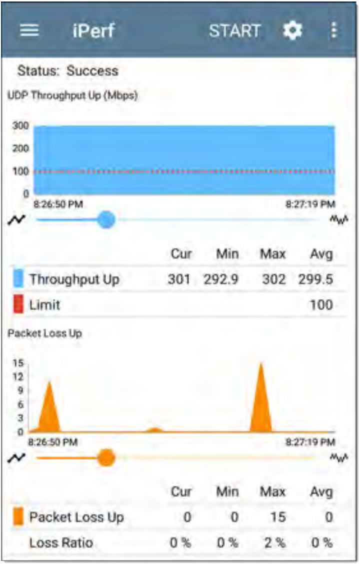
Results

- **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.



Status: Success

	Cur	Min	Max	Avg
🟦 Throughput Up	301	292.9	302	299.5
🟥 Limit				100

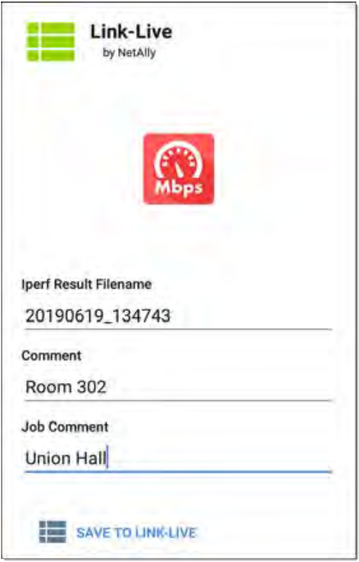
	Cur	Min	Max	Avg
🟧 Packet Loss Up	0	0	15	0
Loss Ratio	0 %	0 %	2 %	0 %

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 iPerf Results to Link-Live

To send your iPerf results to the Link-Live website, touch the action overflow button ⋮ at the top right of the iPerf screen, and then touch **Upload to Link-Live**.



Iperf Result Filename
20190619_134743

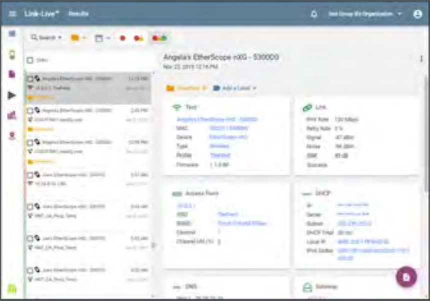
Comment
Room 302

Job Comment
Union Hall

The Link-Live sharing screen opens and allows you to revise the auto-generated filename and attach comments to the iPerf result, which will be displayed on the Results ☰ page on Link-Live.com.

Back to Title and Contents

Link-Live Cloud Service



Link-Live Cloud Service is a free, online system for collecting, tracking, organizing, analyzing, and reporting your test results. AutoTest results are automatically uploaded once your EtherScope nXG is claimed.

The comprehensive EtherScope nXG offers more features for analyzing your network in Link-Live than previous testers. Claim your EtherScope to Link-Live.com to access these functions:

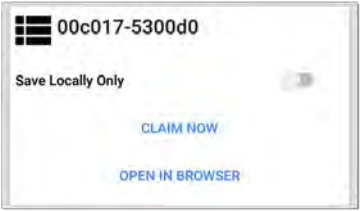
- Check for software updates and update your EtherScope nXG software.
- Download third-party applications from the NetAlly App Store to use on your EtherScope.
- Automatically upload AutoTest results each time you run AutoTest.
- Attach test and Job comments to Link-Live uploads, and automatically sort your results and files into folders in Link-Live.
- Upload test, discovery, and analysis results from the NetAlly apps, including Discovery, Wi-Fi, Path Analysis, AirMapper, Performance, and iPerf. See Link-Live and Testing Apps for more about uploading.

Getting Started in Link-Live Cloud Service

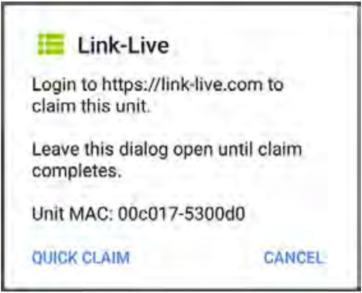
To start, create a user account at Link-Live.com, and sign in. You can open the Link-Live website in the EtherScope's web browser to create and manage your account.

Quick Claiming on the Unit

1. Open the Link-Live app ▤, and touch **CLAIM NOW** on the app screen.



2. In the Link-Live claiming dialog, touch **QUICK CLAIM**.



Link-Live

Login to https://link-live.com to claim this unit.

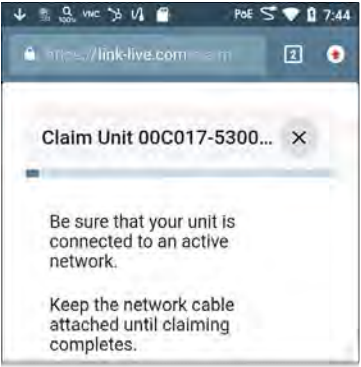
Leave this dialog open until claim completes.

Unit MAC: 00c017-5300d0

A web browser window opens to the Link-Live.com website.

3. Sign in if you haven't already.

   Once you are signed in, Link-Live attempts to claim your unit. You do not need to enter the MAC.

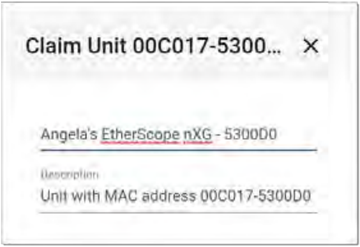


Claim Unit 00C017-5300... ✕

Be sure that your unit is connected to an active network.

Keep the network cable attached until claiming completes.

4. If an Update is available, note the updating instructions, and touch **CONTINUE**.
5. If desired, revise the name and description of your EtherScope unit.



Claim Unit 00C017-5300... ✕

Angela's EtherScope nXG - 5300D0

Description

Unit with MAC address 00C017-5300D0

Otherwise, touch the ✕ to finish the claiming process.

Claiming Manually

On Link-Live.com

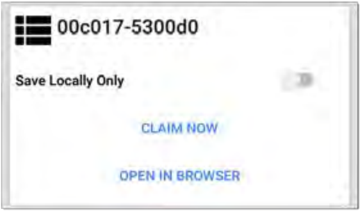
1. The first time you sign in to Link-Live.com, a pop-up window appears, prompting you to claim a device.

   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 click the **Claim Unit** button at the lower right corner of the screen .

2. Then, select the EtherScope nXG image, and follow the claiming instructions on the Link-Live website.

On the EtherScope nXG Unit

1. Open the Link-Live app. Your unit's MAC address is displayed.



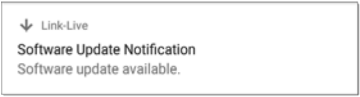
00c017-5300d0

Save Locally Only

2. Touch **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 EtherScope nXG 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.



Link-Live

Software Update Notification

Software update available.

See Updating Software for more information.

After Claiming

Once your EtherScope is claimed to the Link-Live Cloud Service, it will automatically upload your AutoTest results each time you run AutoTest. You can also upload a test comment and a picture with your test results using the AutoTest Wired and Wi-Fi Profile's floating action buttons (FABs), and you can automatically sort your results into folders in Link-Live using test and Job comments.

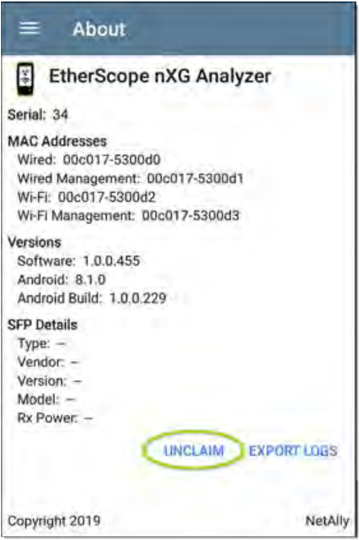
If your EtherScope is not connected to an active network, any test results, comments, or images are stored in memory (buffered) and uploaded once a connection is established.

For more information on how to the use the Link-Live.com website, click or touch the navigation menu icon ☰ at the top left of the Link-Live.com pages, and select ? Support.

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 any information to Link-Live.com.

To unclaim your EtherScope from Link-Live from your unit, open the About screen from the left-side navigation drawer in the Link-Live app, and touch **UNCLAIM**.



EtherScope nXG Analyzer

Serial: 34

MAC Addresses
Wired: 00c017-5300d0
Wired Management: 00c017-5300d1
Wi-Fi: 00c017-5300d2
Wi-Fi Management: 00c017-5300d3

Versions
Software: 1.0.0.455
Android: 8.1.0
Android Build: 1.0.0.229

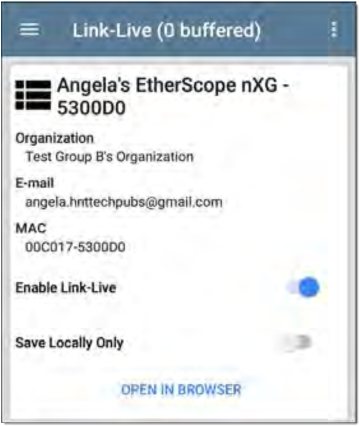
SFP Details
Type: –
Vendor: –
Version: –
Model: –
Rx Power: –

Copyright 2019 NetAlly

Link-Live App Features

The main Link-Live app screen on your EtherScope nXG 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



Angela's EtherScope nXG - 5300D0

Organization
Test Group B's Organization

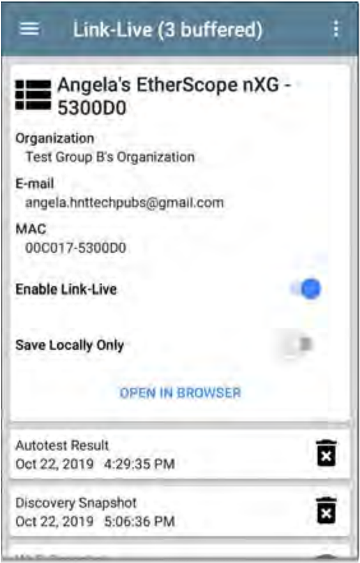
E-mail
angela.hnttechpubs@gmail.com

MAC
00C017-5300D0

Enable Link-Live ●

Save Locally Only ○

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 (3 buffered)

Angela's EtherScope nXG - 5300D0

Organization
Test Group B's Organization

E-mail
angela.hnttechpubs@gmail.com

MAC
00C017-5300D0

Enable Link-Live ●

Save Locally Only ○

OPEN IN BROWSER

Autotest Result
Oct 22, 2019 4:29:35 PM

Discovery Snapshot
Oct 22, 2019 5:06:36 PM

These will upload to Link-Live.com once your EtherScope is connected to an active network.

The EtherScope 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 EtherScope's Link-Live app are informational.

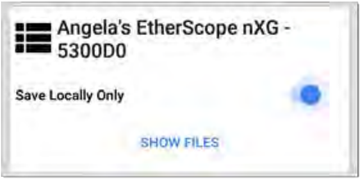
The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the EtherScope cannot upload test results or check for software updates. The **Upload to Link-Live** options will not appear in the testing apps.

Touch the OPEN IN BROWSER link to open Link-Live.com on the EtherScope's web browser.

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 EtherScope as JSON files.

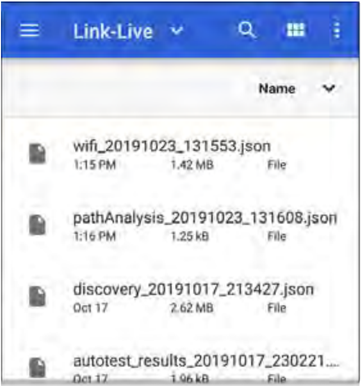
Touch the **Save Locally Only** toggle field in the Link-Live app to save the JSON files to your unit.



Angela's EtherScope nXG - 5300D0

Save Locally Only

Select **SHOW FILES** to open the Files app. The .json files are saved in the **Downloads > TestResults** folder.



wifi_20191023_131553.json
1:15 PM 1.42 MB File

pathAnalysis_20191023_131608.json
1:16 PM 1.25 kB File

discovery_20191017_213427.json
Oct 17 2.62 MB File

autotest_results_20191017_230221...
Oct 17 1.96 kB File

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 EtherScope.

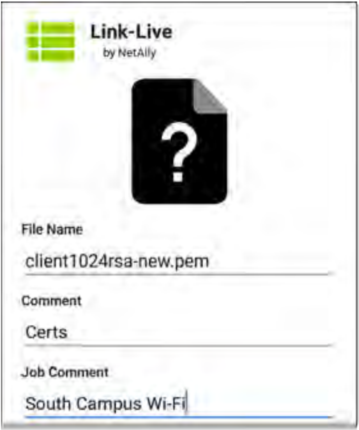
With **Save Locally Only** enabled, options for uploading or saving to Link-Live (described in the Link-Live and Testing Apps section below) will still display in the NetAlly testing apps.

However, the results will be 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 or Wi-Fi AutoTest profiles 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:



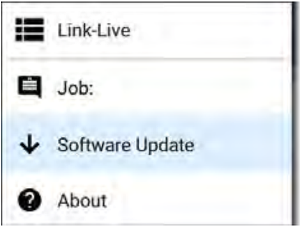
File Name
client1024rsa-new.pem

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, touch the menu icon ☰ or swipe right from the left side of the screen.



2. Touch the **Job:** field.
3. Enter a comment in the dialog box.
4. Touch **SAVE**.

Note that the **Job Comment** field appears in other Link-Live sharing screens, allowing you to change it from multiple locations on the EtherScope. 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.

Link-Live and Testing Apps

Once your unit is claimed, the Link-Live app works with several of the testing apps to upload test results, discovery and analysis data, comments, and images to the Link-Live website. Link-Live.com categorizes the uploads from different apps on corresponding webpages, as shown below:

LINK-LIVE WEBPAGE	APP UPLOADS
Results	AutoTest, Performance, iPerf, and Cable Test results Images, Connection Logs, and other files when saved to a test result
Uploaded Files	Captures, Images, Connection Logs, and other file types
Analysis	Discovery, Wi-Fi, and Path Analysis results
AirMapper	AirMapper Heatmaps

If your unit is not claimed to Link-Live.com or if Link-Live is disabled on the app screen, the links and buttons for uploading to Link-Live in the testing apps will not appear.

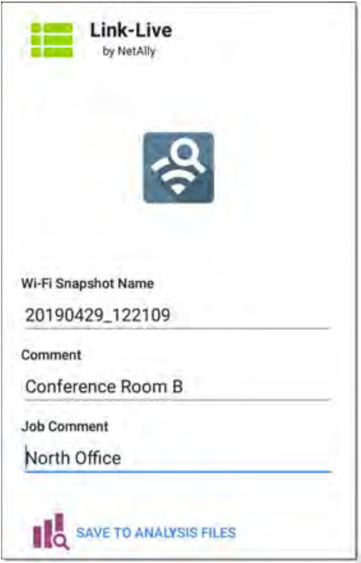
Link-Live Sharing Screens

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 or Wi-Fi app data allows you to upload to the Analysis page on Link-Live.com.



Wi-Fi Snapshot Name

20190429_122109

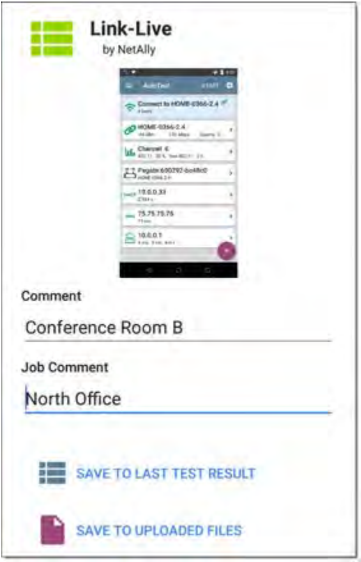
Comment

Conference Room B

Job Comment

North Office

The Link-Live sharing screen for a screenshot or other image allows you to attach it to the most recently run (AutoTest, Performance, iPerf, or Cable) test result on the Results ☰ page, or just to the Uploaded Files 📄 page on Link-Live.com.



Comment

Conference Room B

Job Comment

North Office

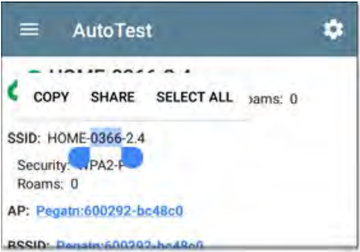
Remember, the regular **Comment** field uploads only to the current result or file, while the **Job**

Comment field uploads with all results and files until you change it.

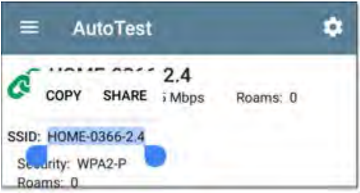
Sharing a Text File to Link-Live

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.

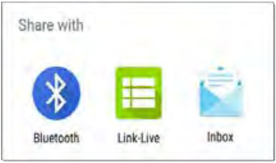
1. Long press a text string to select it.



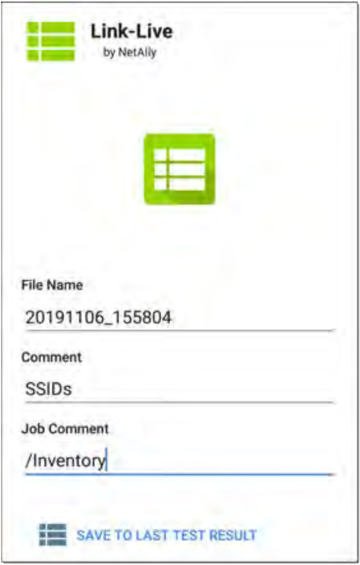
2. Touch **Select All** if needed.



3. Touch **SHARE**.



4. Select the Link-Live icon to open the Link-Live sharing screen.



File Name

20191106_155804

Comment

SSIDs

Job Comment

/Inventory

5. Format any comments as needed, and then touch **SAVE TO LAST TEST RESULT**.

Back to Title and Contents

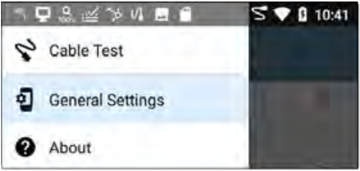
Cable Test App

EtherScope nXG'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 EtherScope 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, touch the menu ☰ icon on the Cable Test app screen, and select **General Settings**.

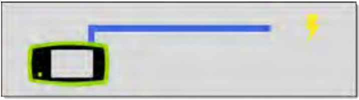


2. Scroll to the bottom of the Settings list under the **Preferences** heading.
3. Tap the **Distance Unit** field, and select either **Feet** or **Meters** as needed, then touch **OK**.

Running Cable Test

Refer to EtherScope nXG's Buttons and Ports as needed.

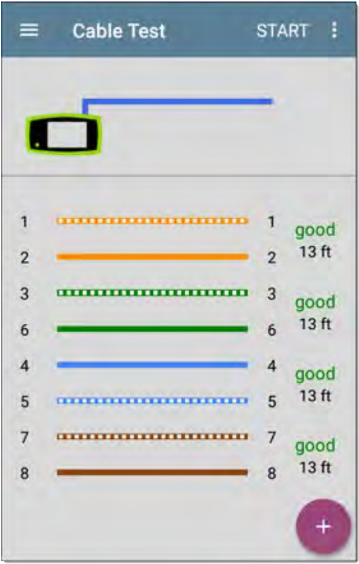
- With an open or unterminated cable connected to the RJ-45 cable test port (left side of the unit), you can measure length, identify shorts and splits, and locate opens.
- Using a cable terminated with a WireView Cable ID accessory, you can measure cable length and identify shorts, opens, split pairs, crossover cables, normal or negative pair polarity, and shielded cables.
- EtherScope nXG 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

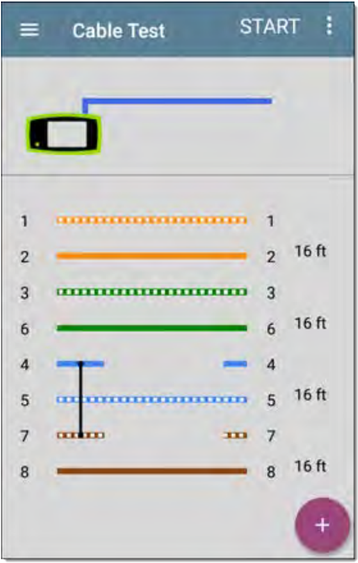
EtherScope nXG can measure the length of a cable and detect some faults by measuring the electrical reflections of the cable using Time Domain Reflectometry (TDR). Connect an open cable (unterminated) into the RJ-45 port on the left side of the EtherScope unit to measure its length and view any shorts,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



Cable Test START

1	1	good 13 ft
2	2	
3	3	good 13 ft
6	6	
4	4	good 13 ft
5	5	
7	7	good 13 ft
8	8	

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.



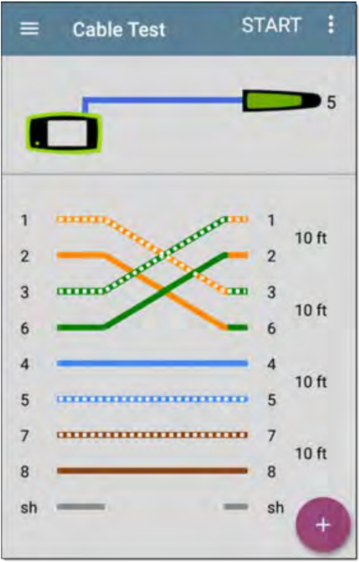
This unterminated cable test image shows a shorted cable between pins 4, 5, and 7.

Terminated WireView Testing

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

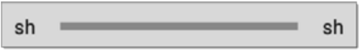
To run a terminated cable test, connect the left side RJ-45 port to a cable terminated with an external WireView Cable ID accessory.

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



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

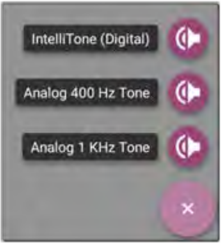
The last row of WireView results indicates whether the cable is shielded: an unbroken line between **sh** means a shielded cable is detected.



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, touch the FAB, and select the appropriate Tone option for your probe. The EtherScope nXG 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 Cable Test Results to Link-Live

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

See the Link-Live chapter for more information.

Specifications and Compliance

Required compliance information is contained in this chapter.

Specifications

General

Dimensions	4.05 in x 7.67 in x 2.16 in (10.3 cm x 19.5 cm x 5.5 cm)
Weight	1.677 lbs (0.76 kg)
Battery	Rechargeable lithium-ion battery pack (7.2 V, 6.4 Ah, 46 Wh)
Battery Life	Typical operating life is 3-4 hours (infinite on PoE). Typical charge time is 3 hours.
Display	5.0-inch color LCD with capacitive touchscreen (720 x 1280 pixels)
Host Interfaces	RJ-45 Cable Test and Management Port USB Type-A Port USB Type-C On-the-Go Port
SD Card Port	Supports Micro SD card storage
Memory	Approximately 8 GB available for storing test results and user applications
Charging	USB Type-C 45-W adapter: AC Input Power 100-240 V, 50-60 Hz; DC Output Power 15 V (3 A) RJ-45: 802.3at and 802.3bt PoE

Media Access	Copper: 10M/100M/1G/2.5G/5G/10G Fiber SFP Adapters: 1G/10GBASE-X
Supported IEEE Standards	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
Cable Test	Pair lengths, opens, shorts, splits, crossed, straight through, and WireView ID
Tone Generator	Digital tone: [455 KHz]; Analog tones: [400 Hz, 1 KHz]
LEDs	2 LEDs (Activity and Link Indicators)

Wireless

EtherScope nXG has two internal Wi-Fi Radios:

Wi-Fi Testing – 4x4 Dual-band 802.11ac Wave 2 wireless radio

Android System Wi-Fi, Bluetooth, and Management – 1x1 Dual-band 802.11ac Wave 2 + Bluetooth 5.0 and BLE wireless radio

Both are IEEE 802.11a/b/g/n/ac compliant.

4x4 Wi-Fi Radio for Testing

Applicant's Name	NetAlly
Model Number	BCM43465
Manufacturer	LITE-ON Technology Corporation
Manufacture Date	2017
Country of Origin	Taiwan
Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X (TKIP, AES)
Regulatory Domain	World Mode
Antenna Gain	1.1 dBi peak in the 2.4-GHz band; 3.2 dBi peak in the 5-GHz band

Data Rates

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11b**: 1, 2, 5.5, 11 Mbps
- **802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11n 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11n 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150 Mbps
- **802.11ac 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11ac 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 Mbps
- **802.11ac 80 MHz**: 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433 Mbps
- **802.11ac 160 MHz**: 65, 130, 260, 390, 520, 585, 650, 780, 867 Mbps

Operating Frequencies

The EtherScope nXG receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country for which it is currently configured in General Settings.

These are the center frequencies of the channels that the Wi-Fi radio supports.

- **2.4-GHz band**: 2.412 – 2.484 GHz (channels 1 through 14)
- **5-GHz band**: 5.150 – 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112,

Modulation

- **802.11b**: DBPSK (1 Mbps), DQPSK (2 Mbps), CCK (5.5 and 11 Mbps)
- **802.11g/n**: DBPSK, DQPSK, OFDM, BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM (proprietary)

Receive Sensitivity

- **6 Mbps**: -90 dBm
- **54 Mbps**: -71 dBm
- **802.11n 20 MHz**: -89 dBm (MSC 0/8)
- **802.11n 40 MHz**: -86 dBm (MSC 0/8)
- **VHT20 MCS 8**: -63 dBm
- **VHT40 MCS 9**: -60 dBm
- **VHT80 MCS 9**: -57 dBm

Android 1x1 Wi-Fi/Bluetooth Adapter for Management

Applicant's Name	NetAlly
Model	BLUE bean
Manufacturer	8devices
Manufacture Date	2019
Country of Origin	United States

Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X (TKIP, AES)
Regulatory Domain	World Mode
Antenna Gain	1.1 dBi peak in the 2.4-GHz band; 3.2 dBi peak in the 5-GHz band

Data Rates

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11b**: 1, 2, 5.5, 11 Mbps
- **802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11n 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11n 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150 Mbps
- **802.11ac 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11ac 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 Mbps
- **802.11ac 80 MHz**: 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 Mbps

Operating Frequencies

The EtherScope nXG receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country for which it is currently configured in General Settings.

These are the center frequencies of the channels that the Wi-Fi radio supports.

- **2.4-GHz band**: 2.412 – 2.484 GHz (channels 1 through 14)
- **5-GHz band**: 5.150 – 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)

Modulation

- **802.11a**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM
- **802.11n/ac**: BPSK (MCS0), QPSK (MCS1 and MCS2), 16 QAM (MCS3 and MCS4), 64 QAM (MCS5, 6, and 7), OFDM
- **802.11ac**: 256 QAM (MCS8 and MCS9), OFDM
- **802.11b**: DBPSK, BPSK (1 and 2 Mbps), QPSK (2 Mbps), CCK (5.5 and 11 Mbps)
- **802.11g**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM

Bluetooth v5 and BLE

- **Frequency Range**: 2.402 – 2.480 GHz
- **Max TX power**: 14 dBm (4 dBm BLE)

External Directional Antenna Accessory

Minimum gain: 5.0-dBi peak in the 2.4-GHz band and 7.0-dBi peak in the 5-GHz band

Reverse-polarity SMA plug

Antenna frequency range: 2.4 – 2.5 and 4.9 – 5.9 GHz

External antenna port is receive-only (no transmit).

Environmental Specifications

Operating Temperature	32°F to 113°F (0°C to +45°C) NOTE: The battery will not charge if the internal temperature of the unit is above 113°F (45°C).
Operating relative humidity (% RH without condensation)	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)

Storage Temperature	-4°F to 140°F (-20°C to +60°C)
Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	IEC 61010-1:2010: Pollution degree 2
Altitude	Operating: 4,000 m; Storage: 12,000 m

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.

CE	Conforms to relevant European Union directives.
✓	Conforms to relevant Australian Safety and EMC standards.
FC	Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.
CSA® C US	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.

U-NII devices operating in the 5.25-5.35 GHz and 5.47-5.725 GHz band, without radar detection are restricted to use indoors.

Contains FCC IDs	WA7-43465, WA7-9377
Contains IC IDs	6627C-43465, 6627C-9377

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.

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s).

L’émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d’Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.
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.

Absorption Rate (SAR) information: This device meets the government's requirements for exposure to radio waves. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons regardless of age or health.

FCC RF Exposure Information and Statement: The SAR limit of USA (FCC) is 1.6 W/kg averaged over one gram of tissue. This device was tested for typical body-worn operations with the back of the handset kept 0 cm from the body. To maintain compliance with FCC RF exposure requirements, use accessories that maintain a 0 cm separation distance between the user's body and the back of the handset. The use of belt clips, holsters and similar accessories should not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

Body-worn Operation: This device was tested for typical body-worn operations. To comply with RF exposure requirements, a minimum separation distance of 0 cm must be maintained between the user's body and the handset, including the antenna. Third-party belt-clips, holsters, and similar accessories used by this device should not contain any metallic components. Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided. Use only the supplied or an approved antenna.

EMC	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.

EU Compliance

This device complies with the following EU Directives: Directives 2014/53/EU, 2014/35/EU, and 2014/30/EU.

This device complies with RF specifications when the device is used at 0 mm from your body. Maximum measured SAR was 2.21 W/kg body; EU limit is 4.0 W/kg.

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

Wi-Fi: 2412 MHz-2472 MHz, 5180 MHz-5240 MHz, 5725 MHz - 5875 MHz

Bluetooth/BLE: 2402 MHz - 2480 MHz

เครืองโทรคมนาคมและอุปกรณ์นี้ มีความสอดคล้องตามข้อกำหนดของ กสทช. (This telecommunication equipment conforms to the requirements of NBTC.)