




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.



NetAlly Network Testing Apps



AutoTest



Ping/TCP



Capture



Discovery



Wi-Fi



Path Analysis



Performance



iPerf



Link-Live



Cable

Contents

Contact Us	13
Introduction	14
How to Use this Guide	15
The PDF Reader App	15
Buttons and Ports	20
Charging and Power	24
PoE Charging	24
Safety and Maintenance	27
Legal Notification	30
Home and Android Interface	31
Home Screen	32
Navigating the Android System	34
Android Status Bar and Notifications ..	37
Notification Panel	37
Apps Screen and Store	40
Device Settings	43
Quick Settings Panel	44
Connecting to Wi-Fi	48
Sharing	52
Sharing Files to Link-Live	53

Sharing a Text String Comment to Link-Live	55
Saving a Screenshot	58
EtherScope nXG Settings and Tools .	59
Navigation Drawer	60
About Screen	62
Exporting Logs	63
EtherScope nXG General Settings	64
Wi-Fi	65
PoE	66
Management	67
Test and Management Ports	70
Configuring the Ports	70
Connection and Scanning Notifications	74
Test Port Notifications	74
Management Port Notifications	76
PoE and VNC	77
EtherScope nXG Icons	78
Floating Action Button (FAB) and Menu	79
Common Tools	81
Web Browser/Chrome	81
Camera and Flashlight	81

Software Management	83
Managing Files	84
Files Application	84
Using a Micro-SD Card	87
Using a USB Drive	88
Ejecting Storage Media	89
Using a USB Type-C to USB Cable	90
Updating Software	92
Remote Access	95
Resetting App Defaults	97
Saving a Default App Settings Configuration	100
Restoring Factory Defaults	101
EtherScope nXG Testing Applications	103
AutoTest App and Profiles	104
AutoTest Overview	106
Managing Profiles and Profile Groups ..	110
Factory Default Profiles	110
Adding New Profiles	112
Profile Groups	118
Creating New Profile Groups	122

Using the Main AutoTest Screen	126
Wired AutoTest Profiles	128
Wired Profile Results	131
PoE Test Results	133
Wired Link Test Results	136
Switch Test Results	138
Wired Profile FAB	142
Wired Profile Settings	145
PoE Test Settings	147
Wired Connection Settings	150
HTTP Proxy	152
Wi-Fi AutoTest Profiles	154
Wi-Fi Profile Test Results	157
Wi-Fi Link Test Results	159
Connect Log	168
Channel Test Results	169
AP (Access Point) Test	173
Wi-Fi Profile FAB	176
Wi-Fi Profile Settings	179
Wi-Fi Connection Settings	181
Advanced (Wi-Fi Connection)	183
Channel Test Settings	186

HTTP Proxy	189
DHCP, DNS, and Gateway Tests for Wired and Wi-Fi AutoTests	191
DHCP or Static IP Test	192
DNS Test	202
Gateway Test	207
Test Targets for Wired and Wi-Fi AutoTests	212
Adding and Managing Test Targets ..	213
Target Test Results Screens	217
AutoTest Ping Test	220
AutoTest TCP Connect Test	226
HTTP Test	230
FTP Test	242
Air Quality AutoTest Profiles	253
Air Quality Profile Settings	255
Air Quality Profile Results	258
Ping/TCP Test App	263
Ping/TCP Settings	264
Populating Ping/TCP from Another App	264
Configuring Ping/TCP Settings	267

Manually	
Running Ping/TCP Tests	270
Capture App	274
Capture Settings	275
Running and Viewing Captures	282
Discovery App	287
Introduction to Discovery	289
Using the Main Discovery List Screen ..	291
Filtering the Discovery List	295
Sorting the Discovery List	299
Refreshing Discovery	301
Uploading Discovery Results to Link- Live	302
Discovery Details Screens	304
Top Details Card	306
Lower Cards in Device Details	312
Problems	314
Addresses	315
Interfaces	316
SNMP	322
Connected Devices	324
Resources	325

VLANs	326
SSIDs	327
Using the Discovery FAB	329
Device Types	333
Routers	333
Switches	334
Unknown Switches	335
Network Servers	337
Hypervisors	338
Virtual Machines	339
Wi-Fi Controllers	340
Access Points (APs)	341
Wi-Fi Clients	342
VoIP Phones	343
Printers	344
SNMP Agents	345
NetAlly Tools	346
Hosts/Clients	348
Discovery Settings	350
SNMP Configuration	353
Active Discovery Ports	361
Extended Ranges	362

Devices Discovered Through Other	
Devices	367
Device Health Interval	373
Problem Settings	377
Wi-Fi Analysis App	381
Wi-Fi Analysis and Discovery	383
Using the Wi-Fi App Screens	384
Wi-Fi App List Screens	385
Filtering in the Wi-Fi App	388
Sorting in the Wi-Fi App	392
Uploading Wi-Fi Results to Link-Live ..	395
Wi-Fi Details Screens	397
Wi-Fi Problems Screen	400
RF and Traffic Statistics Overview ...	402
Channels Map	407
Channels Utilization	408
Channels Overlap	411
Channels	415
Channel Details	417
SSIDs	419
SSID Details	421
APs	424

AP Details	426
BSSIDs	428
BSSID Details	430
Clients	439
Client Details	441
Interferers	447
Interferer Details	449
Path Analysis App	451
Introduction to Path Analysis	452
Path Analysis Settings	453
Populating Path Analysis from Another App	453
Configuring Path Analysis Manually ..	453
Running Path Analysis	457
Path Analysis Results and Source EtherScope Cards	459
Layer 3 Hops	463
Layer 2 Devices	468
Uploading Path Analysis Results to Link-Live	474
Performance Test App	476
Introduction to Performance Testing ..	478

Performance Test Settings	480
Saving Custom Performance Tests ...	481
Configuring the Source EtherScope nXG	485
Configuring Performance Endpoints ...	501
OneTouch 10G Performance Peer ...	502
LinkRunner G2 Reflector	504
LinkRunner AT Reflector	506
NPT Reflector Software	508
Running a Performance Test	510
Performance Test Results	511
Performance Service Detailed Results	513
Uploading Performance Results to Link-Live	519
Running EtherScope as a Performance Peer	521
iPerf Test App	525
iPerf Settings	527
Saving Custom iPerf Settings	527
Populating a Test Accessory Address from Discovery	529
Configuring iPerf Settings Manually .	532

Running an iPerf Test	536
Uploading iPerf Results to Link-Live ..	539
Link-Live Cloud Service	542
Getting Started in Link-Live Cloud Service	544
Uploading Test Results	545
Unclaiming	546
Using the Link-Live App	548
Job Comment	550
Link-Live and Testing Apps	551
Cable Test App	555
Cable Test Settings	556
Running Cable Test	557
Open Cable TDR Testing	558
Terminated WireView Testing	561
Using the Tone Function	563
Specifications and Compliance	564
Specifications	565
General	565
Wireless	566
Environmental Specifications	572
Certifications and Compliance	573

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/EtherScope.

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.

To register, go to NetAlly.com/Registration.

Introduction

The EtherScope nXG Portable Network Export 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.

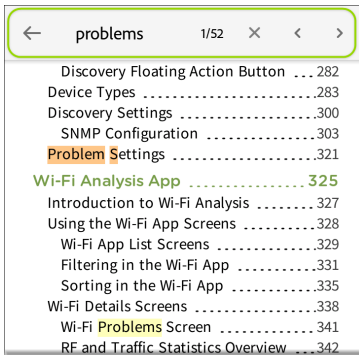
The EtherScope nXG may also be referred to as just "EtherScope" or the "unit" in this guide.

The PDF Reader App

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

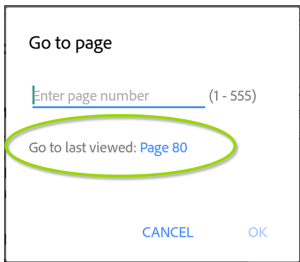
- Tap **blue links** to go to their destinations. [Underlined blue links](#) open external websites.
- Touch headings in the **Contents** list that starts on page 2 to go to the corresponding sections.
- Use the Search function  in the upper toolbar to find specific terms in the guide.



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."




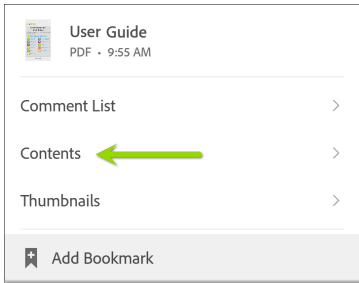
- To scroll quickly up or down in the guide, touch and drag the page number tab 141 at the right. Drag the tab to the very top of the screen to return to the [title page](#).


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



NOTE: You *cannot* touch the back buttons,  or , to go 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.




 **User Guide**
PDF • 9:55 AM

Comment List >

Contents ← >

Thumbnails >

 Add Bookmark

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

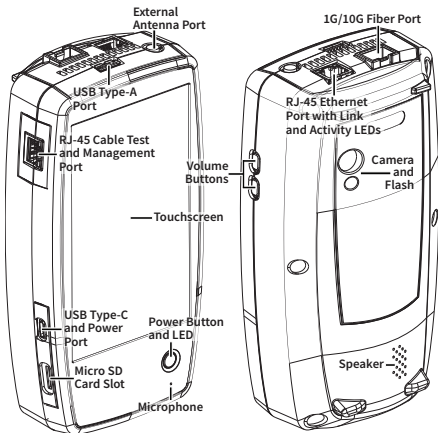
Contents	
Contact Us	
Introduction	>
Home and Android Interface	>
General Settings and Tools	>
Software Management	>
EtherScope nXG Testing Applications	

- 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 your PC, you can transfer the PDF file using one of the methods described in the [Managing Files](#) section, or go to [NetAlly.com/products/EtherScope](https://www.netally.com/products/EtherScope).

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

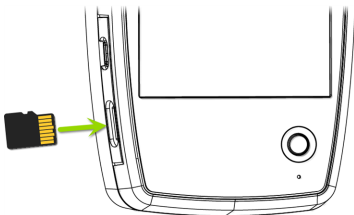
FEATURE	DESCRIPTION
Micro SD Card Slot	Used for removable storage expansion (See Inserting a Micro SD Card below.)
Volume Buttons	Increase or decrease the audio volume
Speaker	Produces audio

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

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

Inserting a Micro SD Card

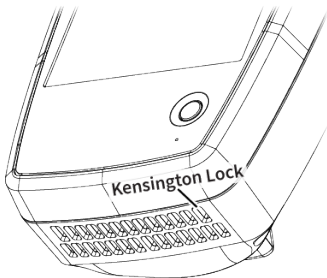
A Micro SD card must be inserted with the *metal contacts facing the front* (towards the touchscreen) of the unit, as shown below.



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 the USB-C charging port on the left side of the unit and an AC outlet. The Power LED button turns red when the unit is charging and goes 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.

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 for charging when the unit is connected to a

switch with Class 4 802.3at (25 W) and above. To charge with PoE, connect the top RJ-45 port on the unit to a network switch with PoE or a PoE injector.


To charge via PoE, the unit must be powered on or in display sleep mode and the "Charge battery via PoE" setting must be enabled in [General Settings](#).

The EtherScope must also run an [AutoTest Wired Profile](#) to detect PoE availability. 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

- Hold the power button on the front of the unit for approximately one second to start it up. The Power LED turns green when the EtherScope nXG is powered on.

- 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, hold the power button for one second until the “Power off” and “Restart” dialog box appears on the touch-screen, and then touch **Power off**.
- To perform a hard power off (without shutting down the software), press and hold the power button for five seconds. Only use this method if the unit is unresponsive to a normal power off.


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.
- There are no serviceable parts. Do not try to service the product.
- 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.

- 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 stiff-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 End User License Agreement 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.

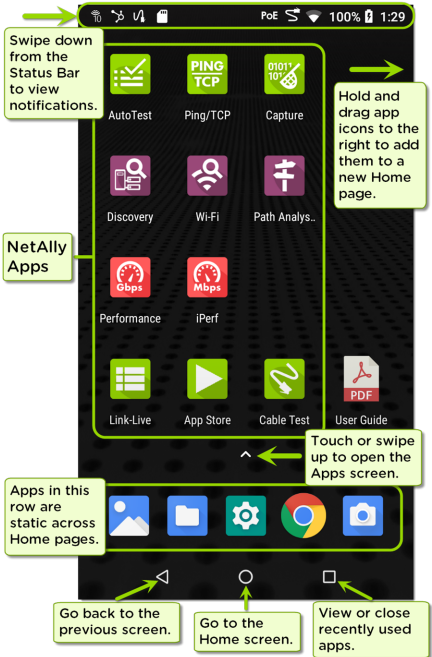
NetAlly reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.

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



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 in 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 them. This is also the screen where you can close, or stop, the open applications.

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

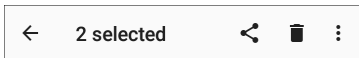
Swiping


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.



NOTE: 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.

TIP: You can use this feature to [attach a text string, as a comment](#), to test results uploaded to [Link-Live](#).

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.

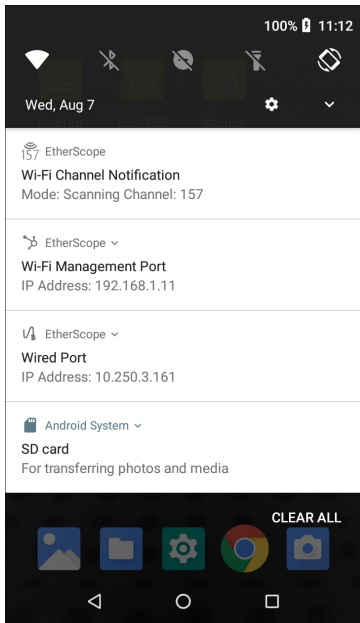
See [Connection and Scanning Notifications](#) for details about the notifications related to EtherScope nXG network testing and management.

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

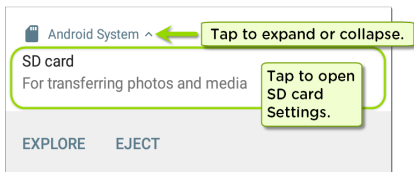
Notification Panel

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 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.




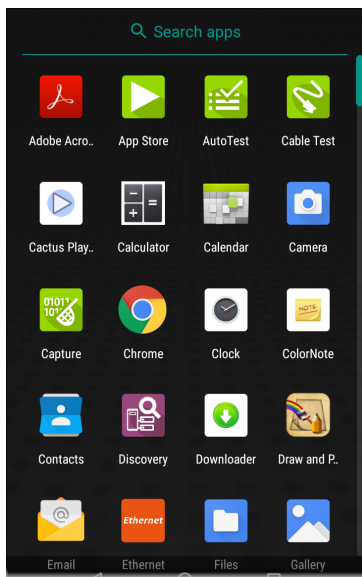
- Touch the title and down arrow \vee on a notification (or swipe down on it) to expand the box and view more details or options.



- 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 connection or scanning 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 .



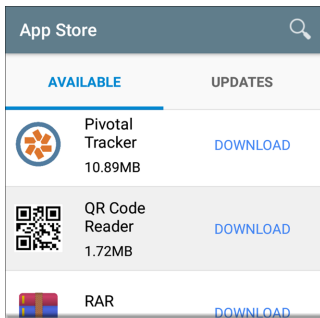
The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.

- 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.

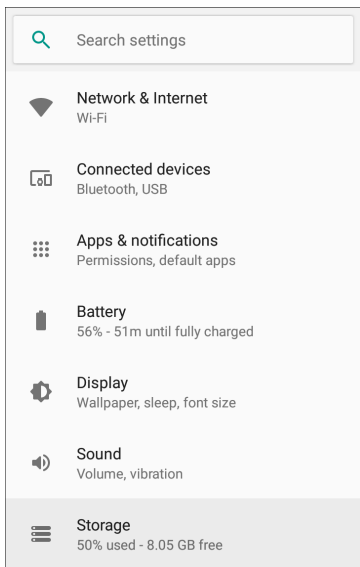


Touch the search icon to search for an App.

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 an App**.

Device Settings

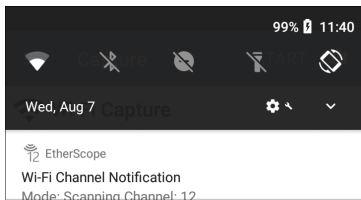
To access the Android system device settings, touch the Settings  icon at the bottom of the [Home screen](#).



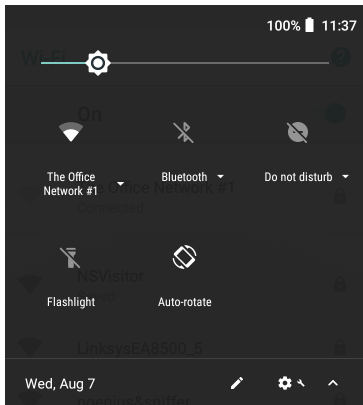
Use the device Settings screen to adjust the display, sound, and date/time; view installed applications and memory devices; [connect to Wi-Fi](#); or [reset to factory defaults](#).



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.



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**  options 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.

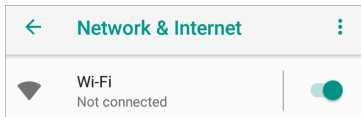
Connecting to Wi-Fi

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.

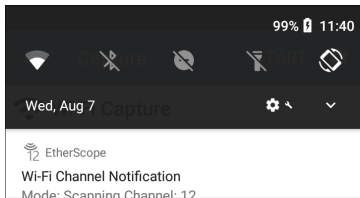
To connect your EtherScope to a Wi-Fi network, access the Android Wi-Fi [Device Settings](#) using either method below:

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

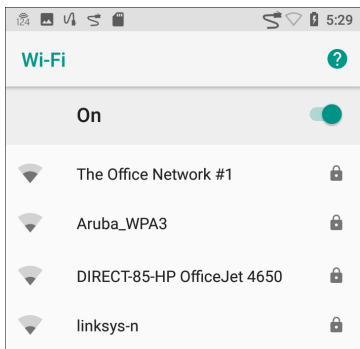


- Open device Wi-Fi settings from the [Quick Settings panel](#) by dragging down the [Status](#)

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

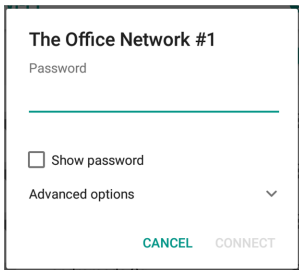


Either path opens the Wi-Fi settings screen.



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

2. Touch a discovered Wi-Fi network from the list.
3. Enter the network's credentials.

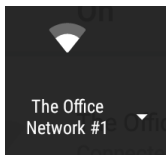



The screenshot shows a dialog box titled "The Office Network #1". Below the title is a "Password" label followed by a text input field with a blue underline. Underneath the input field is a checkbox labeled "Show password" which is currently unchecked. Below that is a label "Advanced options" with a downward-pointing chevron icon to its right. At the bottom of the dialog, there are two buttons: "CANCEL" in blue and "CONNECT" in grey.

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](#).



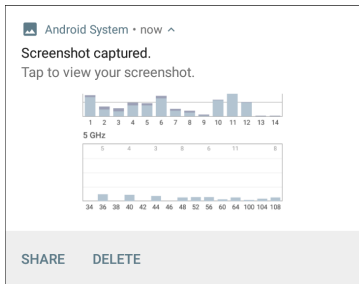
The [Status Bar](#) displays the Wi-Fi status icon  at the top right of the screen.

Sharing

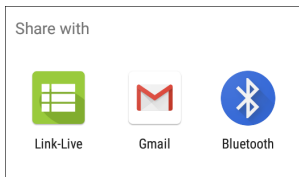
EtherScope nXG allows you to “share” images and files like you would on a smart phone.

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.



Touch **SHARE** to open the “Share with” pop-up dialog, where you can chose a sharing method, such as email, messaging, or uploading to [Link-Live](#).



Sharing Files to Link-Live

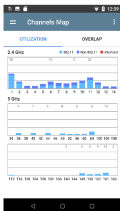
From the “Share with” dialog box (and other screens on the EtherScope), touch the **Link-Live**  option to share a file to Link-Live Cloud Service. Depending on the file type, files can be uploaded along with your last test result, analysis data, or individually to the Uploaded Files page in Link-Live.

The example image below shows the Link-Live screenshot upload screen.



Link-Live

by NetAlly



Comment

2nd Floor South

Job Comment

Union Hall



SAVE TO LAST TEST RESULT



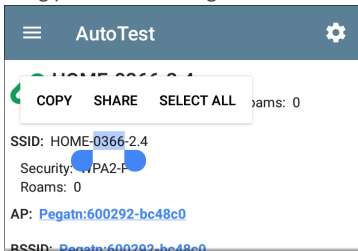
SAVE TO UPLOADED FILES

See the [Link-Live](#) chapter for more information on using Link-Live with your EtherScope nXG.

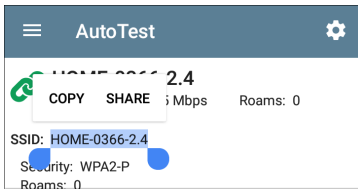
Sharing a Text String Comment to Link-Live

Attaching a text comment to test results sent to Link-Live will help you organize and search through your test data later.

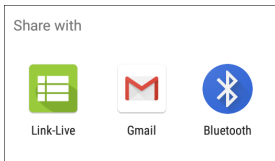
1. Long press a text string to select it.



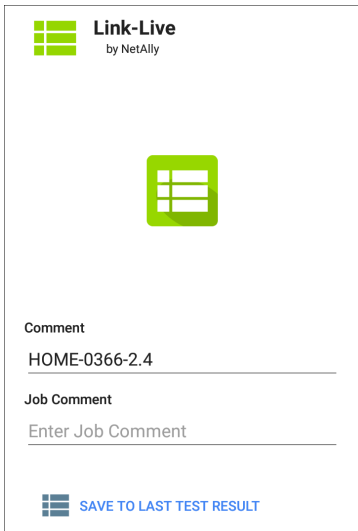
2. Touch **Select All** if needed.





3. Touch **SHARE**.



4. Select the Link-Live icon to open the [Link-Live sharing screen](#).




 **Link-Live**
by NetAlly



Comment
HOME-0366-2.4

Job Comment
Enter Job Comment

 **SAVE TO LAST TEST RESULT**

5. Format your comments as needed, and then touch **SAVE TO LAST TEST RESULT**.

TIP: Add a forward slash (/) to the front of the Comment to automatically create a Folder in

Link-Live and store the test result in the new folder.



Saving a Screenshot

On the EtherScope nXG, 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).

The EtherScope nXG emits a beep and displays the captured screenshot notification in the [Notification Panel](#) when it is successful. Open the notification to share the captured image via your Email app, Link-Live, or another method.

EtherScope nXG Settings and Tools


The EtherScope nXG features a common set of tools and **General Settings** that apply to multiple Apps and testing behavior throughout the unit. This chapter covers settings, icons, and notifications specific to EtherScope nXG.

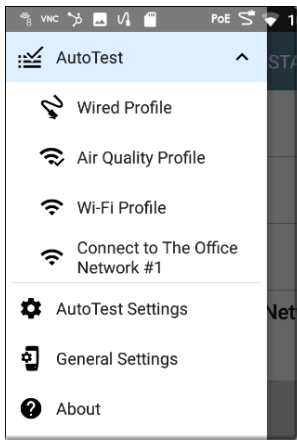
Access common settings and screens from the Left-Side Navigation Drawer  or the Settings  screen in the NetAlly apps.

Navigation Drawer

Each test app contains additional settings, tools, and information in a "navigation drawer" that slides out from the left side of the screen.

To open the navigation drawer:

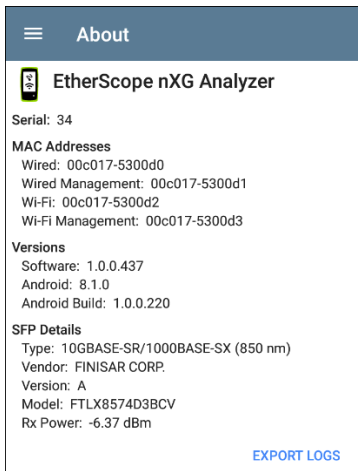
- Touch the menu icon  at the top left of the testing application screens.
- Touch and drag (swipe) to the right from the very left side of the app screens.




As an example, the AutoTest navigation drawer (above) provides access to the [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



About

 **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: 1.0.0.437
- Android: 8.1.0
- Android Build: 1.0.0.220

SFP Details

- Type: 10GBASE-SR/1000BASE-SX (850 nm)
- Vendor: FINISAR CORP.
- Version: A
- Model: FTLX8574D3BCV
- Rx Power: -6.37 dBm

[EXPORT LOGS](#)

The About screen displays the serial number, MAC addresses, software versions, and SFP details for your EtherScope nXG. This screen also contains the Export Logs functions, which allows you to save your unit's logs for analysis by NetAlly's technical support team.

Exporting Logs

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](#).)

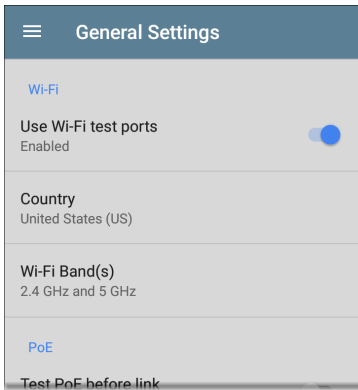
EtherScope nXG General Settings

The General Settings listed below control test and management-related connections that affect multiple test apps, including [AutoTest](#), [Discovery](#), and [Wi-Fi](#).

Access the General Settings from the [left-side navigation drawer](#) in the apps listed above.



General Settings



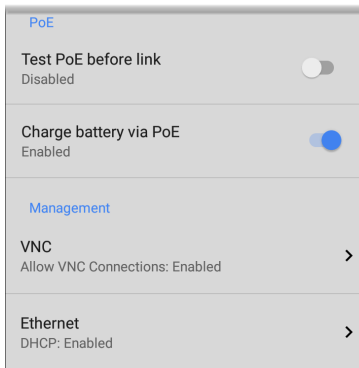
Wi-Fi

Use Wi-Fi test ports: 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 will transmit.

Wi-Fi Band(s): Select the wireless frequency bands the unit will scan, test, and measure.



PoE

Test PoE before Link: By default, an AutoTest [Wired Profile](#) performs the Link test before the PoE test is able to complete. Enable this setting to tell EtherScope to 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 to detect PoE availability before the unit can use it for charging.

See also [PoE Charging](#).

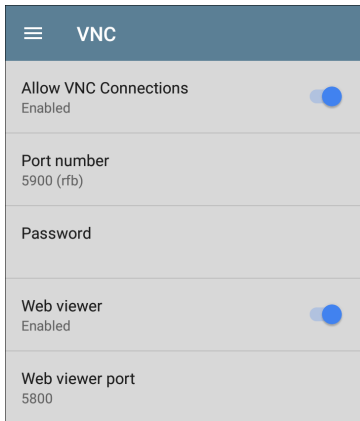
Management

The settings below affect the EtherScope's management port connections.

VNC

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

See [Test and Management Ports](#) and [Remote Access](#) for more information about connecting to a VNC client.



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

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

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

Web viewer: Touch the toggle to enable to disable web viewer access.

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

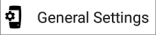
Ethernet


DHCP: This settings 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 addresses.

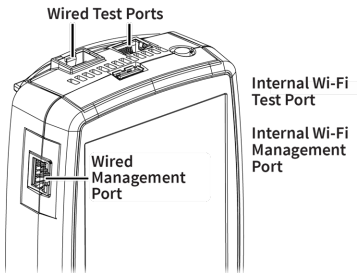
Test and Management Ports

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.

Configuring the Ports

The [General Settings](#)  control EtherScope's use of the test and management ports. General Settings appear in the left-side navigation drawer in the AutoTest, Discovery, and Wi-Fi apps.

The settings  within many of the individual NetAlly apps also let you choose which ports that app will use for its test or analysis.



Refer to [Buttons and Ports](#) and the technical [Specifications](#) if needed.

Test Ports

EtherScope runs Wired and Wi-Fi AutoTests, connection tests, 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](#). Both Wired Fiber connections and Wi-Fi Profiles must be started manually in the [AutoTest](#) app.

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 AutoTest, Discovery, and Wi-Fi 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 packet

captures, link speed, or other advanced connection tests.

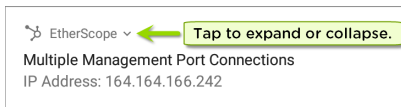
The Management Ports provide a more stable network connection than the Test Ports, as the Test Ports may frequently drop link and reconnect or resume scanning.

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

Connection and Scanning Notifications


EtherScope nXG shows notifications from the NetAlly testing apps and ports in the top Status Bar and drop-down [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.



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

Test Port Notifications

 A **Wired Test Port** connection, "Wired Port," for testing is established from 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.





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

- 
 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.
- 
 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.


 EtherScope
Wi-Fi Channel Notification


Mode: Scanning Channel: 104

- 
 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.

 EtherScope ^
Wi-Fi linked on channel 132
 SSID: NSVisitor
 Signal: -58 dBm
 Channel Width: 20 MHz
 IP Address: 192.65.49.107

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

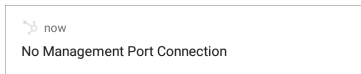


A **Wired Management Port** connection is established through the left-side RJ-45 Management [port](#). Its details are displayed under the Management Port notification.



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.



PoE and VNC



Your unit has access to Power over Ethernet (PoE) for power and charging.



A remote VNC connection is active with a VNC client.



EtherScope nXG 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

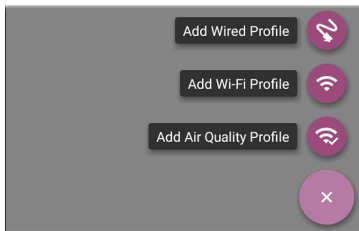


Directional Arrows (or Carets) - indicate the ability to "drill in," open a screen, or expand a panel for more detailed information, or to change the order of a list

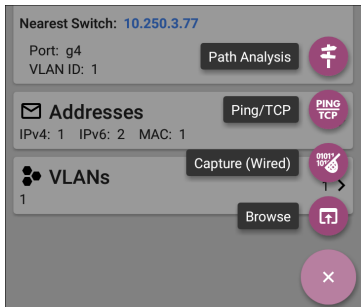
Floating Action Button (FAB) and Menu

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.



Floating action menus that appear in the testing applications are described more specifically in the relevant chapters. For example, see [Using the Discovery FAB](#) in the Discovery app chapter for a more detailed illustration.


Common Tools

Web Browser/Chrome

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

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 results to be uploaded to [Link-Live](#).

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

Software Management

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

Tap a link below to skip to your desired topic:

[Managing Files](#)

[Updating Software](#)

[Remote Access](#)

[Resetting App Defaults](#)

[Restoring Factory Defaults](#)


Managing Files

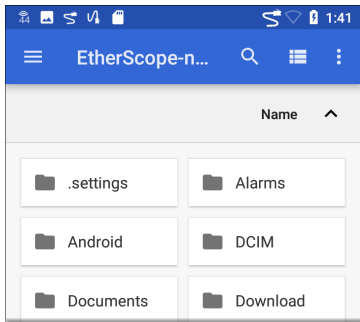
In EtherScope nXG's Android operating system, images, documents, and other files live in a folder hierarchy, where you can copy, move, and paste them between folders or to external storage locations.


See also [Navigating EtherScope nXG](#).



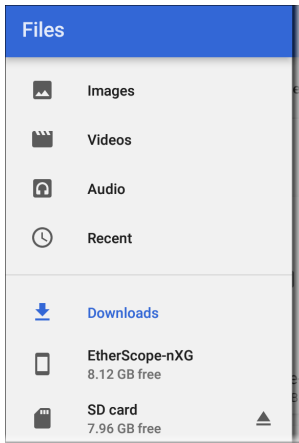
Files Application

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.



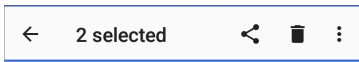
- Tap a folder or file to open it.
- **Long press** on folders or files to view additional file management operations.
- Tap the action overflow icon  in the Files app to see even more actions, such as to create a new folder, move a file, or delete an item.


- Open the left-side navigation drawer to easily navigate through the different folders.



To Move or Copy a file in the Files app, follow this process:

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.



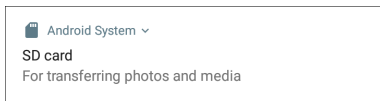
4. Navigate to the folder where you want to move or copy to.
5. Touch the **Move** or **Copy** button at the bottom of the screen.


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.




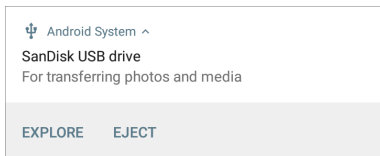
The **SD card** storage location is also available from the **Files**  application.


 **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.

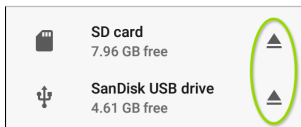


The **USB storage** location is now available from the **Files**  application.


⚠ 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.

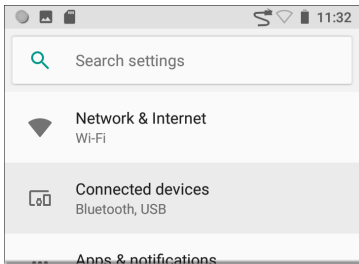
Ejecting Storage Media

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).

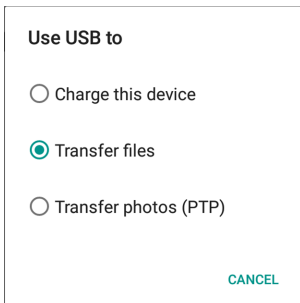


Using a USB Type-C to USB Cable

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.



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.

NOTE: You must create an account and "claim" your EtherScope nXG unit to the Link-Live Cloud Service 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.

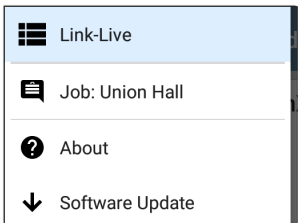
 Link-Live

Software Update Notification

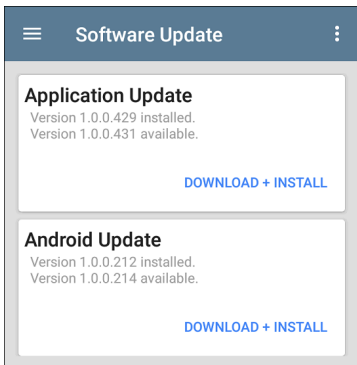
Software update available.

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.



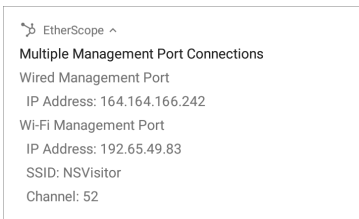
4. If both an Android and an Application Update are available, install the Android update first.
5. Touch **Download + Install** to update the Android operating system or the NetAlly Applications. Each update must be installed separately.

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

Remote Access

Remotely access the EtherScope nXG using a VNC client connection. While you can establish a VNC connection over the Wired or Wi-Fi Test Ports, the Management Ports provide more stable links. (See [Test and Management Ports](#).)

The top notifications are the quickest way to find assigned IP addresses for your EtherScope. Swipe down from the [Status Bar](#) to view them.



- 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.

See [General Settings > VNC](#) to configure VNC connections.

To connect to EtherScope using a VNC client:

1. Get the IP address of a connected 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](#).

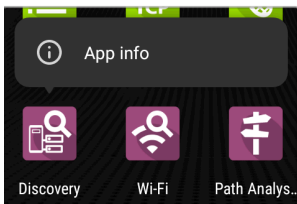
Resetting App Defaults

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

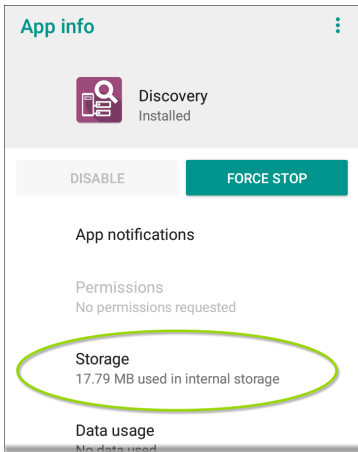
⚠ CAUTION: This operation will delete all saved settings, Profiles, and other saved application data.


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

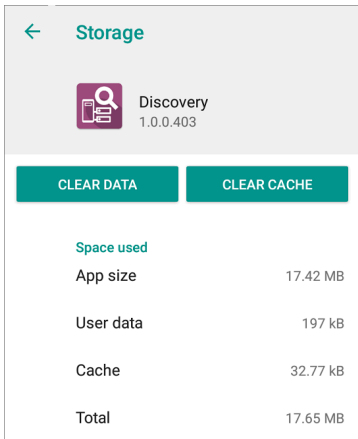
1. Access the **App Info** screen by long pressing (touch and hold) on a app's icon on the [Home](#) or [Apps](#) screen.




2. Tap the **App info** button.



3. 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

CLEAR DATA CLEAR CACHE


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 a Default App Settings Configuration

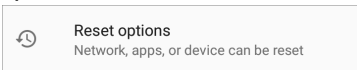
If you find you are frequently resetting app defaults, you can save  the default configuration of settings for later use within the NetAlly testing apps. Loading a saved default configuration in an app is faster than accessing the main device settings. This strategy would be most useful for [AutoTest Profiles](#), [Discovery](#) and [Problem Settings](#), and [Performance Test](#) configurations.

1. Go to an app's settings  screen.
2. With all settings still set to the defaults, tap the save button  and **Save As**.
3. Save a default configuration with an obvious name like "Default Wired Profile" or "Discovery Defaults."

Restoring Factory Defaults

 **CAUTION:** This operation will 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**.



4. On the Reset options screen, select an option based on which defaults you want restored. Whichever option you chose, 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 Ether-Scope's defaults.

The device restarts with factory default settings.



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

Managing Profiles and Profile Groups

Wired AutoTest Profiles

Wi-Fi AutoTest Profiles

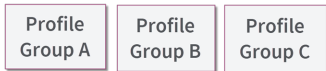
DHCP, DNS, and Gateway Test for Wired and Wi-Fi Profiles

Test Targets for Wired and Wi-Fi Profiles

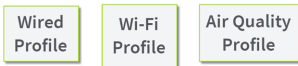
AutoTest Overview

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

Profile Groups



Profiles



Test Targets



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

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

A **Profile** contains a series of individual network tests. There 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.

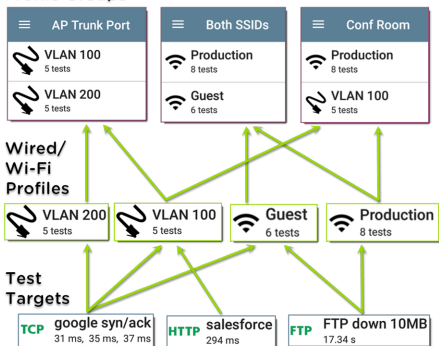
Here are some examples of useful Profile Grouping schemes:

- 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.

Profile Groups



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

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:

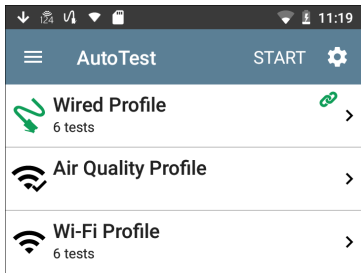
Wired Profiles test copper and fiber connections.


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 [Profile Groups](#) 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.

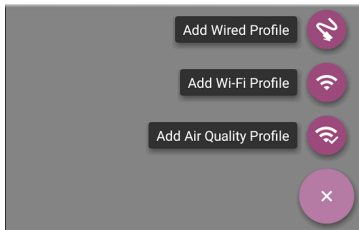
- The default **Air Quality Profile** runs when you touch **START** on the main AutoTest screen or the Air Quality screen.
- For the default **Wi-Fi Profile** to run successfully, you must select an SSID and enter security credentials before the EtherScope can connect to a network.




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.





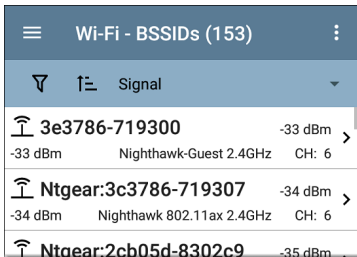
The profile's configuration screen appears after you select the type of profile you want to add. See the topic for each profile type for a description of its settings.


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.



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 2.4GHz

AP: Ntgear:3c3786-719306

BSSID: 3c3786-719307

802.11

Channel: 6

Types: ax, n, g, b

Signal: -32 dBm

SNR: 62 dB

Security Type: WPA2-P

Last Seen: 2:21:01 PM

↑↓ Rates and Capabilities **Connect**

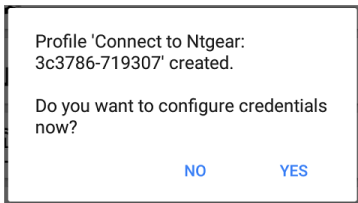
Clients **Capture (Wi-Fi)**

RF and Traffic Statistics

CH: 6 Utilization: 3%

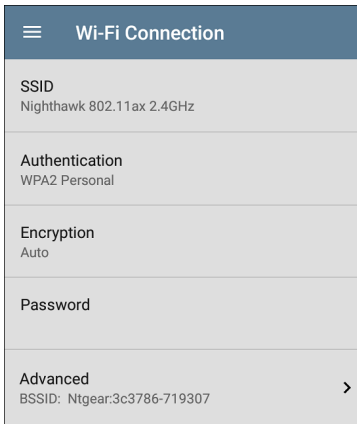
5. In the Floating Action Menu, touch **Connect**.


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



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.

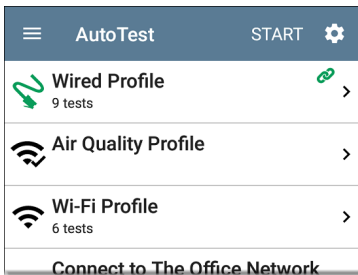


7. Enter any additional credentials (like the network Password), and touch the back button  to return to and run the Profile.

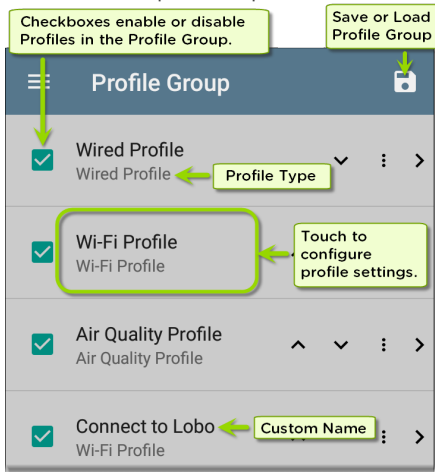
Profile Groups

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. 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).






The Profile Group screen opens.



On the Profile Group screen, you can perform these actions:

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

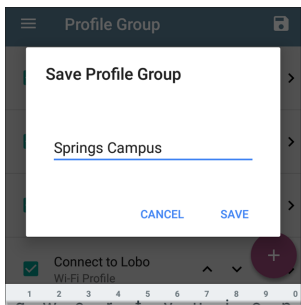
- Tap the up and down arrows  to reorder the saved test Profiles on this and the main AutoTest screen for the Profile Group.
- Touch the action overflow icon  to **Duplicate** or **Delete** a Profile.
CAUTION: When you delete a Profile, it is deleted from all Profile Groups. To remove a Profile from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

Each Profile Group can run one or many of the three Profiles types. Your saved Profiles are available across all of your saved Profile Groups.

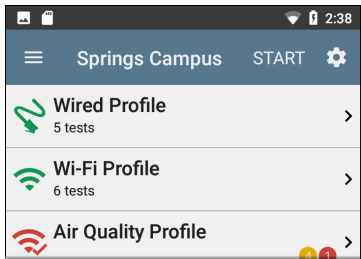
Custom Profile Group Names

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

In the example below, the user saves a custom Profile Group named "Springs Campus."







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




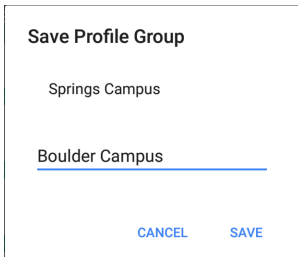
Creating New Profile Groups

To create a new Profile Group, follow these steps:

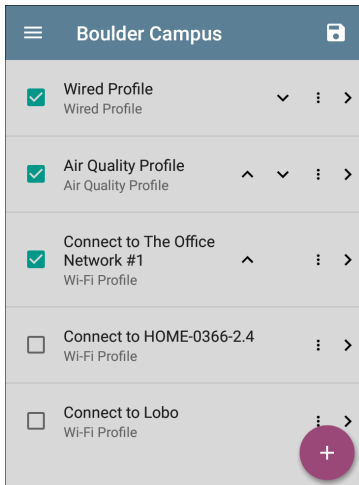
1. Go to the Profile Group screen by touching  on the main AutoTest screen.
2. Uncheck the boxes for any Profiles you do not want included in the new Profile Group.
3. Touch the FAB  to add new test Profiles to be included in your new Profile Group.
4. Tap the up and down arrows   to change the order in which the test Profiles

will run. Unchecked profiles will automatically move to the bottom of the list once you save the Profile Group.

5. Tap , and select **Save As**. A dialog box opens, where you can enter the new name.




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



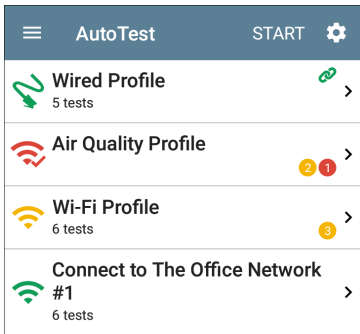
When running the "Boulder Campus" Profile Group shown above, AutoTest will first run the Wired Profile over the Ethernet connection, next scan the wireless channels for Air Quality results, and then connect to "The Office Network #1" and remain connected to that

network. This Profile Group will *not* connect to or test the "HOME..." or "Lobo" networks.

Using the 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:   (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.



Wired AutoTest Profiles

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

☰
AutoTest
START

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. The Switch test is not graded, so the icon stays black.

When Wired Profiles Run Automatically




- A single Wired AutoTest Profile runs automatically when the unit is powered on and EtherScope detects an active Ethernet connection in the top RJ-45 port.
- If there is more than one Wired Profile in the currently active Profile Group, the *last* Wired Profile in the list runs automatically.
- A Wired Profile will not run automatically over a fiber connection.
- A Wired Profile will not run automatically if the AutoTest app is open.

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 PoE, Wired Link, and Switch.

	53.15 V Class: 0 13.00 W	>
	10M/100M/1G RJ-45 HDx/FDx	>
	COS_DEV_SW1 Port: GigabitEthernet1/0/13	>

PoE, Wired Link, and Switch Results are described next.

Skip to [Wired Profile Settings](#).

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

Skip to [Test Targets](#).


Wired Profile Results

The image below shows a completed AutoTest Wired Profile.


The screenshot displays the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" with a gear icon on the right. Below the header is a list of test results for a "Wired Profile" (8 tests). Each result is shown in a white card with a green icon on the left and a right-pointing chevron on the right. The results are: 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), and HTTP google. A purple circular button with a white plus sign is located at the bottom right of the list.

Test Name	Value / Details
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 to view additional test information.
- Open the settings  from any individual test screen, like PoE or Link, to go directly to the settings for the current test.
- Touch the [blue underlined links](#) in the Wired test results to open a [Discovery](#) app Details screen populated with the selected name or ID and other characteristics.

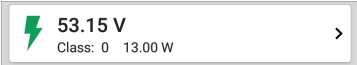
NOTE: You may need to [Configure SNMP](#) settings in the Discovery app to see all the available information about a network component, such as Interface Details for a Switch.


- 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

A rectangular card with a light gray border. On the left side, there is a green lightning bolt icon. To its right, the text "53.15 V" is displayed in a large, bold, black font. Below this, the text "Class: 0 13.00 W" is shown in a smaller, regular black font. On the far right side of the card, there is a black right-pointing chevron (>).

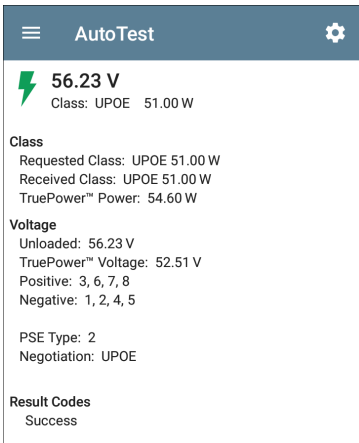
	53.15 V	>
	Class: 0 13.00 W	

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



☰ AutoTest ⚙️

 **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.




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

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



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

If the link icon turns yellow , the EtherScope has detected a downshift from the maximum advertised speed.

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

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



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

SFP Details (Fiber)

Rx Power: Link receive power

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

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



Switch Test Results

The results available for the Switch Test are based on Discovery Protocol advertisements

and SNMP system group information and statistics. See [Discovery Settings](#) for information about [SNMP configuration](#).



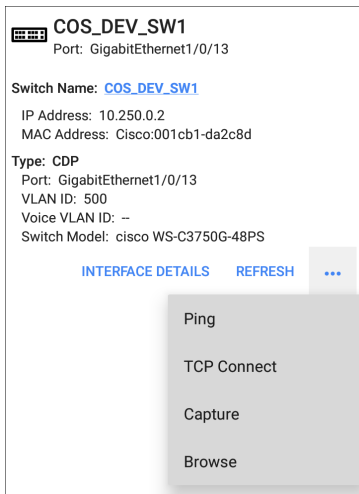
The Switch test card displays the discovered switch name and the port name. The Switch test is not graded, so the icon remains black.

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



Touch the card to open the Switch Test screen, where you can **REFRESH** the Switch test.

Switch Test Results Screen



The screenshot shows a network switch test result for 'COS_DEV_SW1'. It includes a keyboard icon, the switch name, port information, IP and MAC addresses, CDP type, and various configuration details. At the bottom, there are buttons for 'INTERFACE DETAILS', 'REFRESH', and a menu icon. A context menu is open over the menu icon, listing 'Ping', 'TCP Connect', 'Capture', and 'Browse'.

COS_DEV_SW1
Port: GigabitEthernet1/0/13

Switch Name: [COS_DEV_SW1](#)

IP Address: 10.250.0.2
MAC Address: Cisco:001cb1-da2c8d

Type: CDP
Port: GigabitEthernet1/0/13
VLAN ID: 500
Voice VLAN ID: --
Switch Model: cisco WS-C3750G-48PS

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

- Ping
- TCP Connect
- Capture
- Browse

If the EtherScope was unable to obtain switch information from an AutoTest run, touch **REFRESH** to capture and display the next port advertisement.

The switch results screen shows the following:

Switch Name: Name advertised by the switch

IP and MAC Addresses: Discovered switch addresses

Type: Discovery Protocol - CDP, LLDP, EDP, SNMP, or FDP

Port: Detected Port name

VLAN ID: Discovered VLAN ID number

Voice VLAN: Discovered Voice VLAN ID number

Switch Model: Discovered switch model name and number

Touch the action overflow icon **•••** to open other app or tools with the target (in this case, the switch) pre-populated. For example, **INTERFACE DETAILS** opens the Interface Details screen for the Switch in the [Discovery](#) app, and **Ping** opens the [Ping/TCP](#) app, populated with the switch's IP address.

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.

DHCP, DNS, and Gateway Results

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

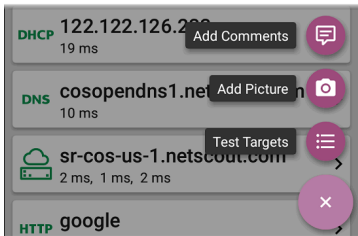
See [DHCP, DNS, and Gateway Tests for Wired and Wi-Fi](#).

PING FTP TCP HTTP Target Tests

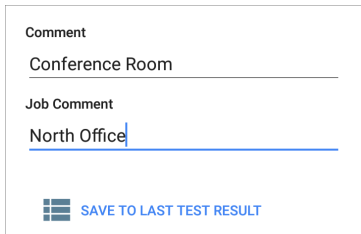
See the [Test Targets](#) topic for information on target test results.

Wired Profile FAB

The [Floating Action Button \(FAB\)](#) on AutoTest Profile screens allows you to attach comments and images to *your most recent AutoTest results* that are uploaded to [Link-Live Cloud Service](#).



When you touch **Add Comments**, the Link-Live [sharing](#) screen opens.



The screenshot shows a white rectangular area with a thin black border. At the top, the text "Comment" is displayed in a dark grey font. Below it, the text "Conference Room" is entered into a text field, with a horizontal line underneath. Further down, the text "Job Comment" is displayed. Below that, the text "North Office" is entered into another text field, with a blue horizontal line underneath and a blue vertical cursor at the end of the text. At the bottom left of the area is a blue icon consisting of three horizontal bars. To the right of this icon, the text "SAVE TO LAST TEST RESULT" is displayed in blue, all-caps font.

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

When you touch **Add Picture**, EtherScope lets you open the Gallery or Camera app to select or take a photo that is then uploaded and attached to your most recent test results.

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

Finally, touch the Test Targets option in the Floating Action Menu to open the [Test Targets](#) screen, where you can add Ping, TCP Connect,


HTTP, and FTP target tests to the current profile.

Wired Profile Settings

These settings control the wired test connection, PoE test, the thresholds for **Success/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 3, TruePower™ >
Wired Connection	Auto >
IP Configuration	DHCP: Enabled >
DNS Test	www.google.com >
Gateway Timeout Threshold	100 ms
Test Targets	3 target(s) >

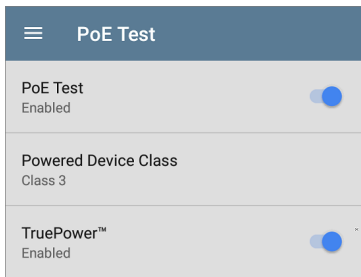
On the **Wired Profile** settings screen, touch each field described below as needed to configure the profile. Changed settings are automatically applied. When you finish configuring, tap the back button  to return to the profile.

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

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
- 802.3 at 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.

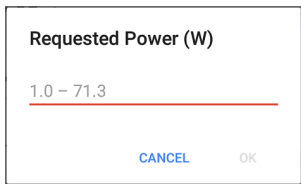
LLDP

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 a switch does not support LLDP and the LLDP setting is enabled,

LLDP negotiation will fail, but it will not affect the rest of the test.

Requested Power (W)

This setting appears if UPOE or PoE Injector are selected in the Powered Device Class setting shown above. 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.

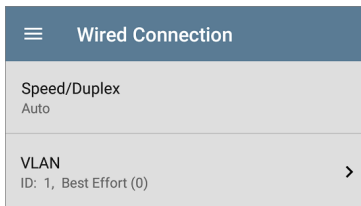
PoE General Settings

See the [PoE section in General Settings](#) for descriptions of the **Test PoE before Link** and **Charge Battery via PoE** settings, which also affect the PoE Test.

See also [PoE Charging](#).

Wired Connection Settings

Open **Wired Connection** settings to configure speed and duplex and VLAN. These settings control the [Wired Test Port](#) connection.



Wired Connection	
Speed/Duplex	Auto
VLAN	ID: 1, Best Effort (0) >

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.

VLAN

Touch to open the VLAN settings screen. Slide the toggle to the right to enable VLAN settings. 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.

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 for Wired and Wi-Fi Profiles](#).

HTTP Proxy

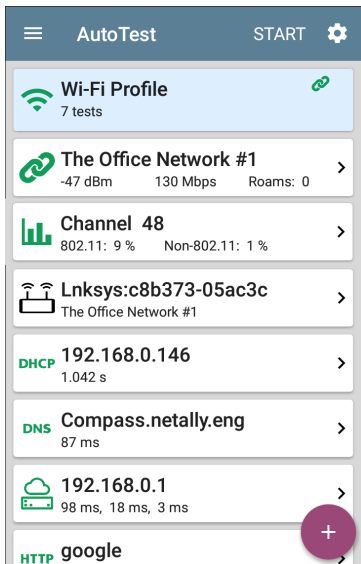
The Proxy control lets you specify a proxy server through which the connection will be established. These settings are only used if HTTP Proxy is enabled in an [HTTP](#) or [FTP](#) Test Target. Open the **HTTP Proxy** screen to enable proxy settings.

HTTP Proxy	
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 screenshot shows the AutoTest app interface. At the top, there is a blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" with a gear icon on the right. Below the header is a list of items:

- Wi-Fi Profile**: Includes a Wi-Fi icon, the text "7 tests", and a chain link icon.
- The Office Network #1**: Includes a chain link icon, signal strength "-47 dBm", speed "130 Mbps", and "Roams: 0".
- Channel 48**: Includes a bar chart icon, "802.11: 9 %", and "Non-802.11: 1 %".
- Lnksys:c8b373-05ac3c**: Includes a Wi-Fi router icon, "The Office Network #1", and a MAC address.
- DHCP 192.168.0.146**: Includes "DHCP" in green, the IP address, and "1.042 s".
- DNS Compass.netally.eng**: Includes "DNS" in green, the domain name, and "87 ms".
- 192.168.0.1**: Includes a cloud and server icon, the IP address, and "98 ms, 18 ms, 3 ms".
- HTTP google**: Includes "HTTP" in green and the domain name.


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

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:

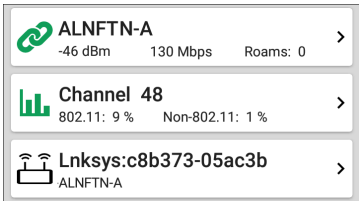
Success/Warning/Fail. The AP Test card shows the name and SSID of the connected AP. The AP test is not graded, so the icon stays black.

Wi-Fi Profiles do not run automatically.

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, , which also shows the connected channel.

Wi-Fi-Profile-Specific AutoTests

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



The screenshot shows three stacked status cards. The first card, titled 'ALNFTN-A', features a green link icon and displays '-46 dBm', '130 Mbps', and 'Roams: 0'. The second card, titled 'Channel 48', features a green bar chart icon and displays '802.11: 9%' and 'Non-802.11: 1%'. The third card, titled 'Lnksys:c8b373-05ac3b', features a Wi-Fi router icon and displays 'ALNFTN-A'. Each card has a right-pointing chevron icon.

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.

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



The screenshot shows a single status card titled 'SSID Not Set'. It features a red link icon and a right-pointing chevron icon.

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](#).

[Back to Title and Contents](#)

Wi-Fi Profile Test Results

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



The screenshot displays the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" and a gear icon on the right. Below the header, the main content area shows a list of test results for a Wi-Fi profile named "Connect to The Office Network #1".

- Connect to The Office Network #1**: 7 tests, with a yellow circle containing the number "1" in the bottom right corner.
- 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**: (partially visible).

A purple circular button with a white plus sign is located in the bottom right corner of the test results list.

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 screen, you can perform these actions:

- Touch any of the test result cards to view additional test information.
- Open the settings  from any individual test screen, like Link or Channel, to go directly to the settings for the current test.
- Touch the [blue underlined links](#) in the Wi-Fi test results screens to open a [Wi-Fi](#) app screen populated with the selected name or ID and other characteristics.
- 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 network connection is dropped, you may need to rerun the Profile to re-establish link and enable additional actions.



Wi-Fi Link Test Results

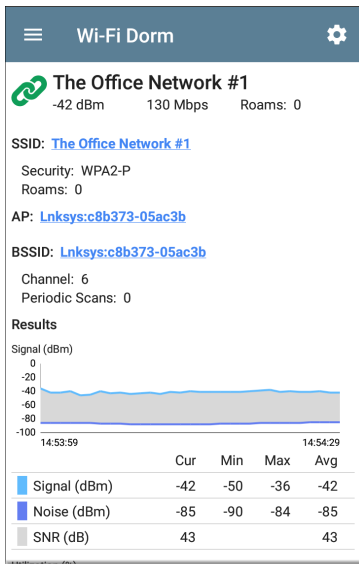
 **The Office Network #1** >
-42 dBm 130 Mbps Roams: 0

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



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 or IP address of the AP to which the Tester is connected

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.

SSID: NSVisitor

Security: WPA2-P

Roams: 2

AP: [lap-cos-us-4](#)

BSSID: [Cisco:0c2724-8f187e](#)

Channel: 56

Periodic Scans: 0

Last Roam From

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

BSSID: [Cisco:0c2724-8ecc2e](#)

Channel: 64

Periodic Scans: 1

This image shows an example Link test screen with roaming information.

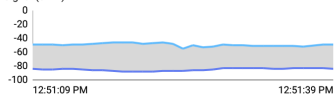
Last Roam From: If the EtherScope has roamed to a new AP, the previous AP's name, BSSID, and Channel display.

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.

Signal, Utilization, Retries, and TX Rate Graphs

Results

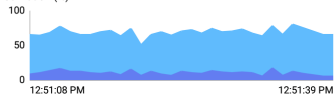
Signal (dBm)



	Cur	Min	Max	Avg
Signal (dBm)	-49	-55	-44	-48
Noise (dBm)	-84	-90	-83	-86
SNR (dB)	35			38

Signal (dBm)	-49	-55	-44	-48
Noise (dBm)	-84	-90	-83	-86
SNR (dB)	35			38

Utilization (%)



	Cur	Min	Max	Avg
802.11 %	60	44	68	59
Non-802.11 %	5	3	19	11
Total	65			70

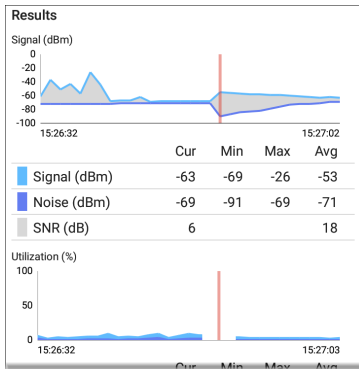
802.11 %	60	44	68	59
Non-802.11 %	5	3	19	11
Total	65			70

Results: These graphs, described below, update in real time for as long as the unit is still connected to the network and you are still viewing this screen. You can touch and drag (or swipe) left and right on each graph to move

backward and forward in time and view the recorded measurements. The graphs save and display data for up to 24 hours in the past if the unit stays linked.

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 you have been viewing the screen.

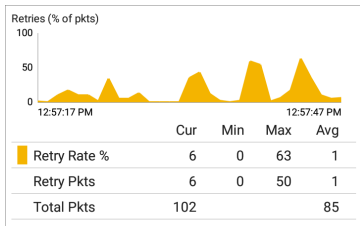
When the EtherScope roams to a new AP, each graph shows a **red** vertical line at the time the tester connected to the new AP.



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

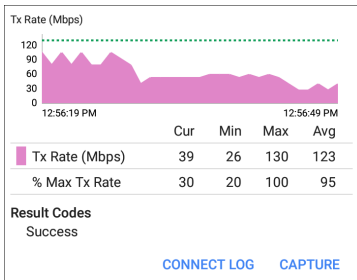
- Signal - The AP's signal strength in dBm
- Noise - The noise level in dBm on the channel used
- SNR - The network's signal-to-noise ratio, a measure of signal strength relative to noise, measured in decibels (dB)

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



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

- **Retry Rate %** - The AP's signal strength in dBm
- **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



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

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

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

Connect Log

Connect Log	
12:56:18.927 PM	Wireless: SSID The Office Network #1
12:56:19.124 PM	WPA2 Personal
12:56:21.793 PM	Link Down
12:56:21.794 PM	Scan AP: (208) c8:b3:73:05:ac:3b ch 6 -47 dBm
12:56:22.059 PM	Connecting to AP: c8:b3:73:05:ac:3b Chan 6
12:56:22.060 PM	Send Open Authentication Request
12:56:22.205 PM	Receive Open Authentication Success
12:56:22.256 PM	Send Association Request
12:56:22.300 PM	Wireless: WPA2 Info Element: Mcast=([2] TKIP) Ucast=([4] AES-CCMP) Auth=([2] PSK)
12:56:22.441 PM	Receive Association Success
12:56:22.442 PM	Wireless: Channel: 6 802.11n 20MHz
12:56:22.533 PM	Link Up: c8b373-05ac3b

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



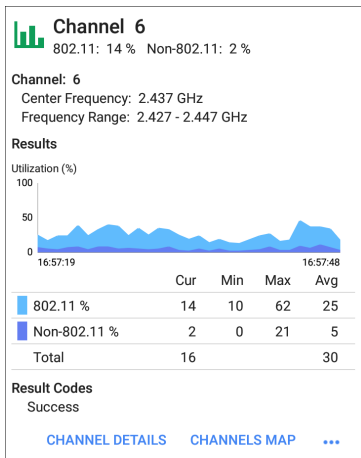
Channel Test Results



The Channel card shows the channel on which the AP is operating and the current 802.11 and Non-802.11 utilization.

Refer to [Channel Test Settings](#) if needed.

Channel Test Screen



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. Swipe left and right on the Utilization graph to move backward and forward in time and view the recorded measurements. The graph saves and displays data for up to 24 hours in the past if the unit stays linked.

The legend table displays the Current, Minimum, Maximum, and Average measurements.

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
- **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



Lnksys:c8b373-05ac3b


The Office Network #1



The AP card shows the AP's name and the SSID of the network it is supporting. The AP name shown is based on what the EtherScope is able to gather from the device.

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

AP Test Screen



Lnksys:c8b373-05ac3b
The Office Network #1

Device Name: [Lnksys:c8b373-05ac3b](#)

IP Address: 192.168.1.1
MAC Address: Lnksys:c8b373-05ac3b

SSID: The Office Network #1

Security: WPA2-P
Roams: 0

802.11
Channel: 1
Type: n
Supported Types: b, g, n

Client Associations: 3
Periodic Scans: 0

[CONNECT LOG](#) [CAPTURE](#)

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

Device Name: AP's name

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

MAC Address: The AP's MAC address

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

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 Wi-Fi packet **CAPTURE** on the connected channel and AP.

DHCP, DNS, and Gateway Results

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

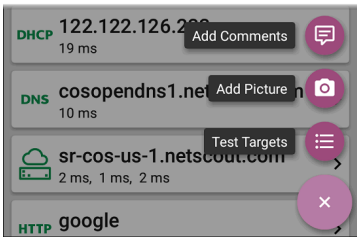
See [DHCP, DNS, and Gateway Tests for Wired and Wi-Fi](#).

PING FTP TCP HTTP Target Tests

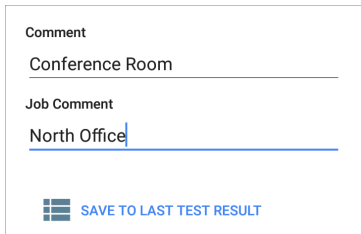
See the [Test Targets](#) topic for information on target test results.

Wi-Fi Profile FAB

The [Floating Action Button \(FAB\)](#) on AutoTest Profile screens allows you to attach comments and images to *your most recent AutoTest results* that are uploaded to [Link-Live Cloud Service](#).



When you touch **Add Comments**, the Link-Live [sharing](#) screen opens.



The screenshot shows a white rectangular area with a thin black border. At the top, the text "Comment" is displayed in a dark grey font. Below it, the text "Conference Room" is entered into a text field, with a horizontal line underneath. Further down, the text "Job Comment" is displayed. Below that, the text "North Office" is entered into a text field, with a blue horizontal line underneath and a blue vertical cursor at the end of the text. At the bottom left of the area is a blue icon consisting of three horizontal bars. To the right of this icon is the text "SAVE TO LAST TEST RESULT" in blue, all-caps font.

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

When you touch **Add Picture**, EtherScope lets you open the Gallery or Camera app to select or take a photo that is then uploaded and attached to your most recent test results.


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

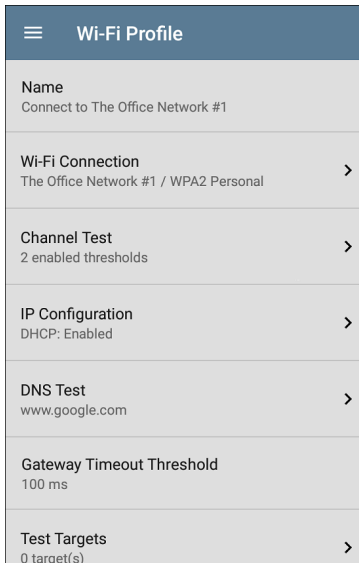
Finally, touch the Test Targets option in the Floating Action Menu to open the [Test Targets](#) screen, where you can add Ping, TCP Connect,

HTTP, and FTP target tests to the current profile.

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.



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.

Wi-Fi Connection	
SSID	The Office Network #1
Authentication	WPA2 Personal
Encryption	Auto
Password	*****
Advanced	BSSID: Any >

SSID

Enter an SSID or select from the list of discovered SSIDs.

Authentication

Open the **Authentication** screen to select the correct security type for the network, and enter all necessary authentication credentials for the

network, such as Encryption Type, Keys, EAP Type, Username, Certificates, and/or Password.

Encryption

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

Password

Touch the **Password** field to enter the network password.



Advanced (Wi-Fi Connection)

Advanced	
BSSID	Any
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.

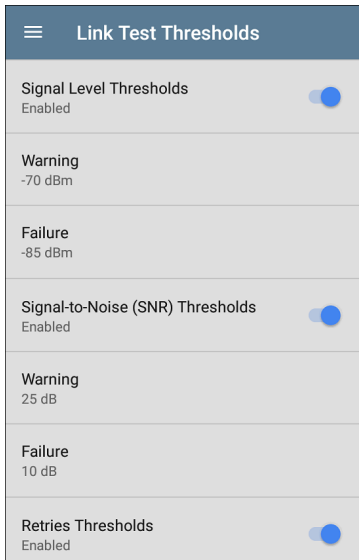
Roam Threshold

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.



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

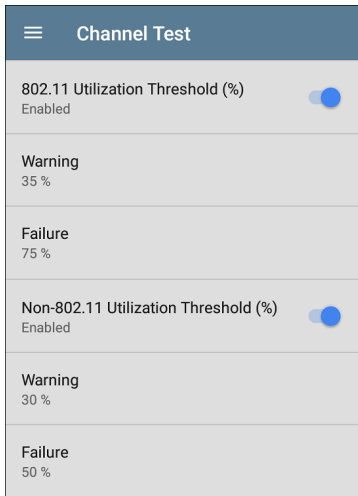
Transmit Rate (TX) Thresholds: Measured rate as a percentage of the AP's maximum throughput rate

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 (%)

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 connection will be established. These settings are only used if HTTP Proxy is enabled in an [HTTP](#) or [FTP](#) Test Target. Open the **HTTP Proxy** screen to enable proxy settings.


HTTP Proxy	
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.

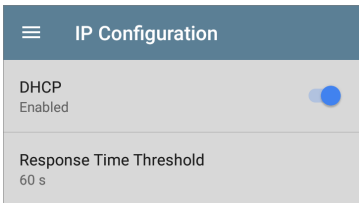
Touch [blue links](#) or the blue action overflow icon  on the test results screens for additional actions.

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.



By default, DHCP is enabled. Open **IP Configuration** to 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

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

The Static IP address fields for **Subnet Mask**, **Default Gateway**, and **Primary** and **Secondary DNS Servers** only appear if DHCP is disabled. 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.

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

50.0 %  Offer Acknowledge

Device Name: The discovered name of the Switch (Wired) or AP (Wi-Fi), 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 EtherScope

Subnet Mask: IP address of the subnet where EtherScope is testing

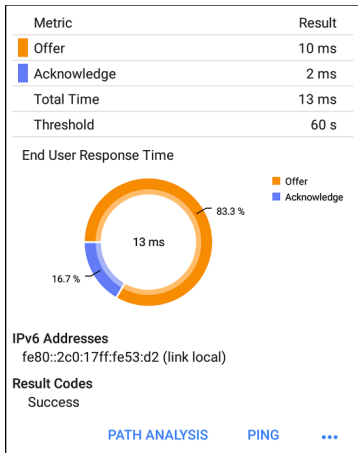
Subnet: Combination of the subnet mask and the offered IP address

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 graph: Breakdown of the times for the process of acquiring a DHCP IP address



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

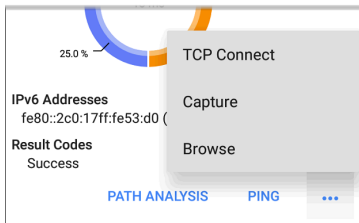
Total Time: Total amount of time consumed by the DHCP process

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 graph: A pie chart showing the Offer and Acknowledgment times as percentages

IPv6 Addresses: Addresses obtained via router advertisement

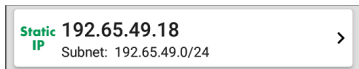
Results Codes: Final status of the test (Success or Failure)



The additional actions available on the DHCP test screen include opening the [Path Analysis](#), [Ping/TCP](#), or [Capture](#) app populated with the DHCP server address or browsing to the address in the web browser.

Static IP Test Results

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



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

Touch the card to open the test results screen.

The screenshot shows the AutoTest app interface. At the top is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and a gear icon on the right. Below the header is a white card with a thin black border. The card displays the following information:

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

The Static IP test screen displays the configured addresses.

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

Subnet Mask: IP address of the subnet where EtherScope is testing

Gateway: Name of the Gateway server

IP Address: IP address of the Gateway server

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

[Back to Title and Contents](#)

DNS Test

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	
Lookup Name	www.google.com
IP Protocol Version	IPv4
Lookup Time Threshold	1 s

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.



Touch the card to open the DNS test results screen.

DNS Test Results Screen

DNS **cosopendns1.net.com**

19 ms

Lookup Name: www.google.com

Threshold: 10 s

DNS 1: [cosopendns1.net.com](#)

Lookup IP: 172.217.1.196

Lookup Time: 19 ms

DNS 2: [cosopendns2.net.com](#)

Lookup IP: 172.217.1.196

Lookup Time: 13 ms

DNS 3: [cosdc-01.net.com](#)

Lookup IP: 172.217.1.196

Lookup Time: 2 ms

Result Codes

1: Success

2: Success

3: Success

[TEST AGAIN](#)

[PATH ANALYSIS](#)

[...](#)

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

Lookup Name: www.google.com

Threshold: 1 s

DNS 1: Compass.netally.eng

Lookup IP: 172.217.12.4
Lookup Time: 17 ms

DNS 2: 10.200.72.19

Lookup IP: 172.217.12.4
Lookup Time: 6 ms

DNS 3: 10.200.72.20

Lookup IP: 172.217.12.4
Lookup Time: 6 ms

DNS 4: 10.200.72.11

Lookup IP: 172.217.12.
Lookup Time: <1 ms

Result Codes

1: Success
2: Success
3: Success
4: Success

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

Ping
TCP Connect
Capture
Browse

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



Gateway Test

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

Gateway Timeout Threshold

Gateway Timeout Threshold


5 ms

10 ms

100 ms

1 s

10 s

Custom Value 

CANCEL **OK**

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

the gateway server before grading the test as a fail. 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](#).



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

Gateway Test Results Screen

The screenshot shows the AutoTest application interface. At the top is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and a gear icon on the right. Below the header is a white card with a green cloud icon and a server rack icon. The card displays the following information:

- 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

At the bottom of the card are three blue buttons: "TEST AGAIN", "PATH ANALYSIS", and "...".

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

IPv4 Address: Internal IPv4 address of the Gateway server

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)

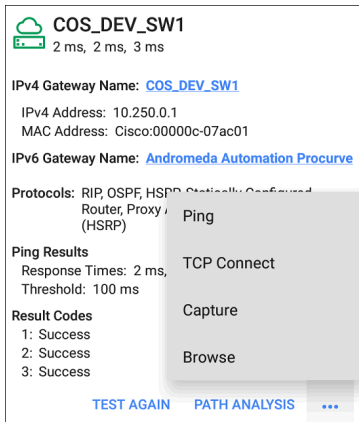
IPv6 Gateway Name: Name advertised by the IPv6 router (if available)



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_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 / (HSRP)

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

Result Codes
 1: Success
 2: Success
 3: Success

Context Menu:
 Ping
 TCP Connect
 Capture
 Browse

Bottom Buttons: TEST AGAIN PATH ANALYSIS ...

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 testing app, or **Browse** to the Gateway's IPv4 Address in your web browser.

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](#)

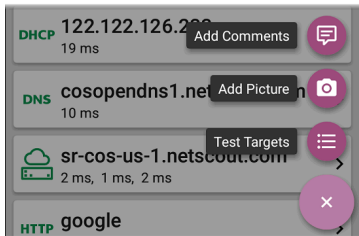
[TCP Connect](#)

[HTTP](#)

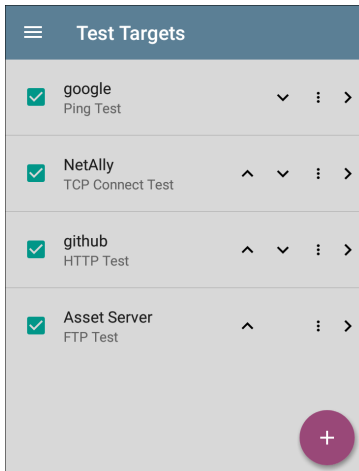
[FTP](#)

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.

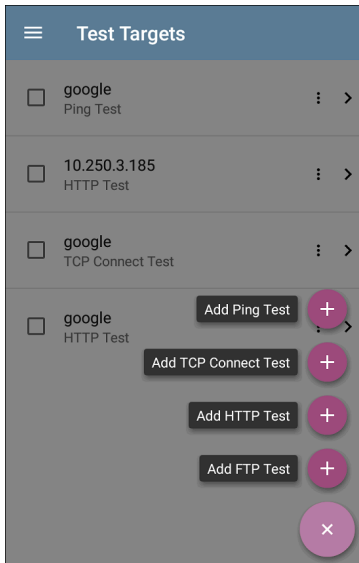


On the Test Targets screen, you can perform these actions:

- 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.

PING google
9 ms, 33 ms, --

Device Name: [172.217.1.196](#)

IPv4 Address: 172.217.1.196
MAC Address: --

Results
Lookup Time: 3 ms
Response Times: 9 ms, 33 ms, -- ●
Threshold: 250 ms

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

The third Response Time displays two dashes -- to indicate that no response was received, and

under the Results heading, the yellow dot points out the third Response Time as the reason for the Warning. Additionally, the third Result Code lists "Timeout error" as the reason for the Warning.

Additional Target Test Actions



TEST AGAIN PATH ANALYSIS ...

After the Target test has completed, 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

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

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.

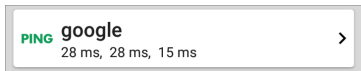
IP Protocol Version: IPv4 is used by default. Touch the field to switch between IPv4 and IPv6.

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



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

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

Device Name: Hostname or address of the target device

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

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

Results

- **Lookup Time:** How long it took to resolve the URL into an IP address
- **Response Times:** How long it took for the 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
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,
Threshold: 1 s

Result Codes
1: Success
2: Success
3: Success

TEST AGAIN PATH ANALYSIS ...

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, or **Browse** to the Ping target address in your web browser.

AutoTest TCP Connect Test

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

TCP Connect Test Settings

☰ TCP Connect Test	
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.

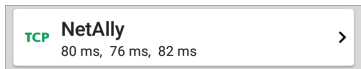
Device Name: Enter the IP address or URL of the target you want to test. If you enter an IP address, the DNS lookup portion of the test will be skipped.

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



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

AutoTest

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

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

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

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

Result Codes
1: Success
2: Success
3: Success

TEST AGAIN PATH ANALYSIS ...

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.

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

Name

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

URL

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

IP Protocol Version

IPv4 is used by default. 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	<input type="checkbox"/>

Response Must Contain

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

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 not found, the test fails with the return code: "HTML did contain expected content."

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



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

HTTP Test Results Screen

HTTP **github**
3.671 s





Device Name: [lb-192-30-253-113-iad.github.com](#)

IPv4 Address: 192.30.253.113

MAC Address: --

URL: <https://www.github.com>

Results

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

End User Response Time

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

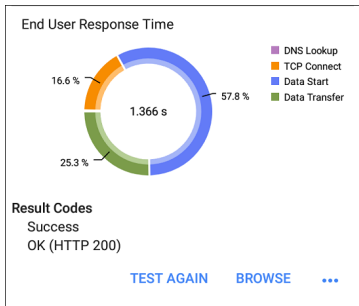
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, test will fail.

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

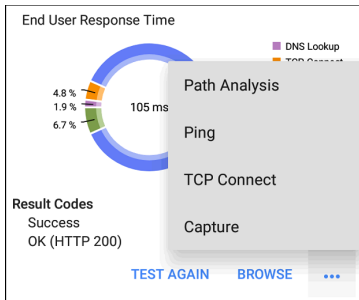
Rate (bps): The measured data transfer rate



End User Response Time graph: 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.

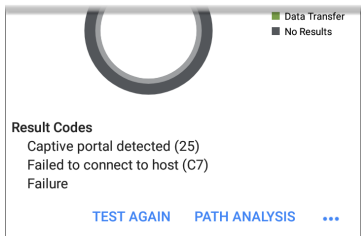


Touch [blue links](#) or the blue action overflow icon **...** at the bottom of the test results screens to run the HTTP **TEST AGAIN**, open another testing app, or **Browse** to the target address in your web browser.

Captive Portal Connections


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

If EtherScope detects that the network requires Captive Portal sign-in to connect, the "Captive portal detected" Result Code displays at the end of a failed HTTP test.



To connect to the Captive Portal, while still connected to the SSID and channel, tap the action overflow icon **...** on the HTTP test screen, and then select **Browse**.

A window opens in your default browser and allows you to enter the required credentials for the network.

When finished in the browser, hit the back button  to return to the HTTP test, and **TEST AGAIN** to connect and 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.

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

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	<input type="checkbox"/>

Username and Password

Enter these credentials to access the target server you specified. Enter "anonymous" as the username to establish an anonymous connection. The test 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

Metric	Result
FTP Asset Server	
171 ms	
Device Name: 10.250.2.218	
IPv4 Address: 10.250.2.218	
MAC Address: --	
Get File: /internal/iperf3	
Results	
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

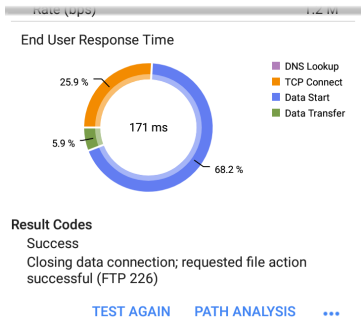
web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test will fail.

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



End User Response Time graph: 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

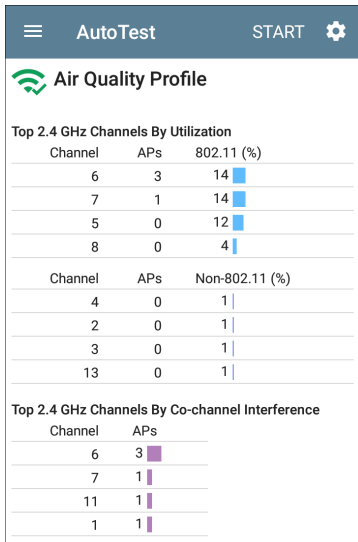
another testing app, or **Browse** to the FTP server in your web browser.



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.




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 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	<input checked="" type="checkbox"/>
Warning 35 %	
Failure 75 %	
Non-802.11 Utilization Threshold (%) Enabled	<input checked="" type="checkbox"/>
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

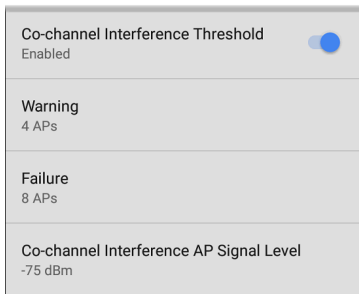
Touch the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Air Quality profile screen header.

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.

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.



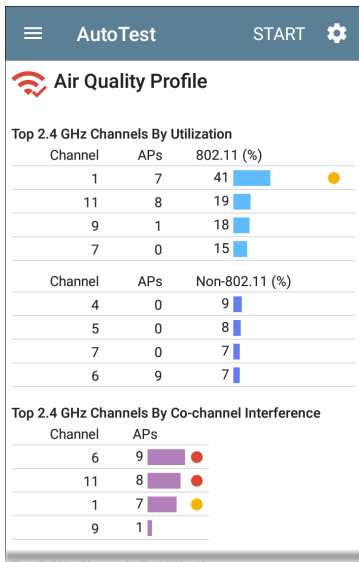
Co-channel Interference AP Signal Level

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.

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 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

☰
AutoTest
START

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

[CHANNELS MAP](#)

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.



Ping/TCP Test App

The Ping/TCP test app runs a continuous 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.

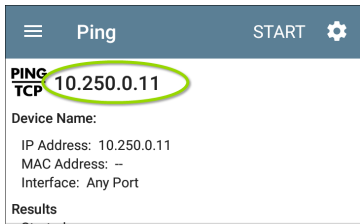
Populating Ping/TCP from Another App

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.

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

cos-lab-vm-cisco
Router
Name
SNMP: cos-lab-vm-cisco
Address
IPv4: 10.250.0.11 (Reachable)
MAC: Cisco:40f4ec-f47681
Protocols: Statically Configured Router
Attributes: Discovered via SNMP Switch, Port Aggregation
Path Analysis
Addresses → Ping/TCP
IPv4: 2 MAC: 1
VLANs
1, 196, 500, 508, 526, 560
Capture (Wired)
Browse
Interfaces
Up: 2 Down: 41
MIB SNMP

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



☰ Ping START ⚙️


PING
TCP 10.250.0.11

Device Name:

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

Results

Configuring Ping/TCP Settings Manually

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

Ping/TCP Settings	
Device Name	10.250.3.92
IP Protocol Version	IPv4
Interface	Wired Port
Protocol	Ping
Frame Size (bytes)	1024
Do Not Fragment	<input checked="" type="checkbox"/>
Timeout Threshold	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, Wired or Wi-Fi Test Port, or Wired or Wi-Fi Management Port.

See [Test and Management Ports](#) for explanations of the different ports.

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

Frame Size (bytes): This setting only appears if the **Ping** Protocol is selected. It specifies the total size of the payload and the header sent. Valid sizes are 64 bytes to 10000 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: This setting only appears if the **Ping** Protocol is selected. Touch the toggle button to enable.

Port: This setting only appears if the **TCP Connect** Protocol is selected. It indicates the port number 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.

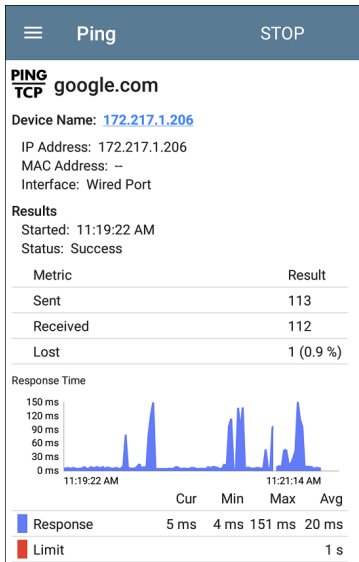
Timeout Threshold: This threshold controls how long the EtherScope waits for a response from the target the test is failed.

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**. The Ping/TCP app runs a continuous test to your selected target until you touch **STOP**.



Device Name: Hostname or address of the target device

IPv4 or IPv6 Address: IP address of the target

device

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

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

Interface: The 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: This graph plots the target device's response times in milliseconds. You can touch and drag (or swipe) left and right on the graph to move backward and forward in

time and view the recorded measurements. The graph saves and displays data for up to 24 hours in the past if the unit stays linked.

Response: This table displays the Current, Minimum, Maximum, and Average response time measurements.

Limit: This is 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.

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's details screens, 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 Wi-Fi app's BSSID details screen shown below contains the option to start a Wi-Fi Capture.

Wi-Fi - BSSID

 **Lnksys:c8b373-05ac3b**

BSSID

SSID: **The Office Network #1**

AP: **Lnksys:c8b373-05ac3c**



BSSID: c8b373-05ac3b



802.11


Channel: 6



Types: n, g, b
Signal: -39 dBm
SNR: 54 dB
Security Types: WPA2-P, WEP

Last Seen: 1:34:22 PM

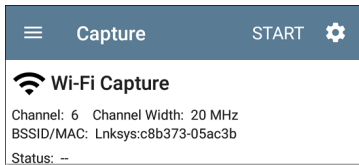
 **Problems** **Connect** 

Warnings: 1  **Capture (Wi-Fi)** 


↑↓ Rates and Capabilities 

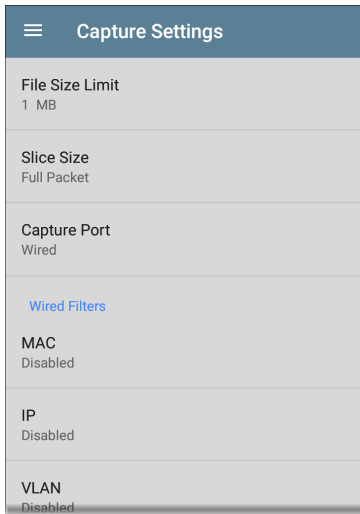
 **Clients** 

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



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.



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 **Wired** or **Wi-Fi**.

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 an 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.

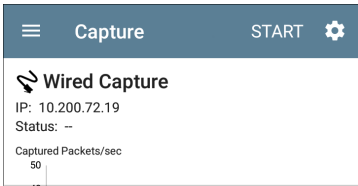
BSSID/MAC: Enter a BSSID to capture only packets going to or from the target device.

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.

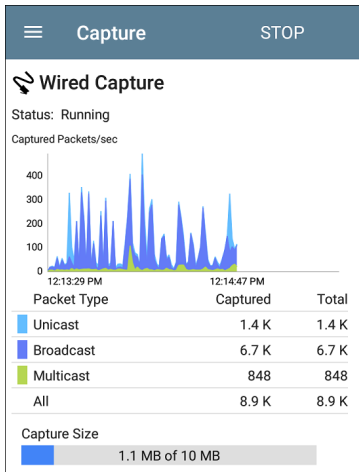
Running and Viewing Captures

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



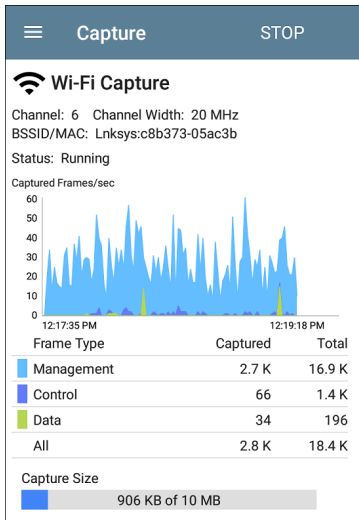
The current Status of the capture and any applied filters are shown under the capture type (Wired or Wi-Fi). The image above indicates that the app will only capture traffic for IP 10.200.72.19.

View the real time status of the capture as it is running, and tap **STOP** to stop the running capture before it reaches the File Size Limit from the settings.



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. Like other time-based graphs on the EtherScope, you can swipe left and right on the Captured Packets/sec graph to move backward and forward in time.

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

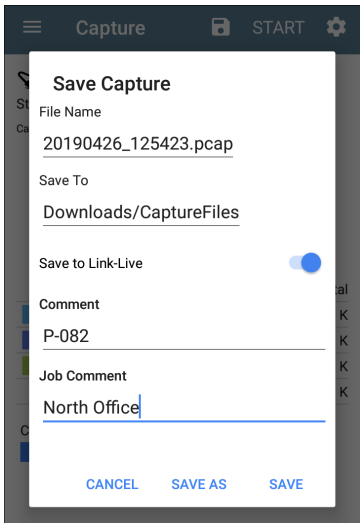


In this image, the app is capturing all three Wi-Fi Frame Types on channel 6 with the BSSID shown. The Total measurements in the table below the graph represent all frames seen,

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

CANCEL SAVE AS SAVE

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 chose 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](#)

[Using the Main Discovery List Screen](#)

[Discovery Details Screens](#)

[Device Types](#)

[Discovery Settings](#)

[Problem 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  at the top of the screen indicates that the EtherScope is scanning Wi-Fi channels to discover devices on the wireless network. Once a wired network connection (test or management) is available, wired discovery begins.

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

Using the Main Discovery List Screen

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

Discovery (589)		
  Name		
 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.)

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.

The screenshot shows the Discovery App interface with the following elements and callouts:

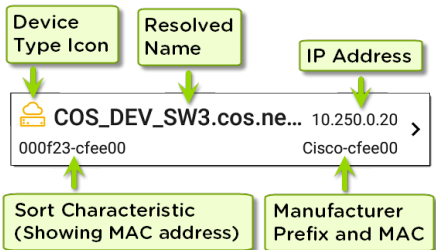
- Total number of discovered devices:** A callout box pointing to the text "Discovery (589)" in the header.
- Discovery Settings:** A callout box pointing to the hamburger menu icon on the left.
- Refresh Discovery:** A callout box pointing to the "Refresh Discovery" button in the top right.
- Filter:** A callout box pointing to the filter icon (funnel) above the list.
- Sort:** A callout box pointing to the "Name" dropdown menu.
- Touch a card to view device details:** A callout box pointing to the "Angela's EtherScope ..." device card.

The device list is as follows:

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


The information displayed on each device card varies depending on the selected Sort element

and the data the EtherScope was able to discover.



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

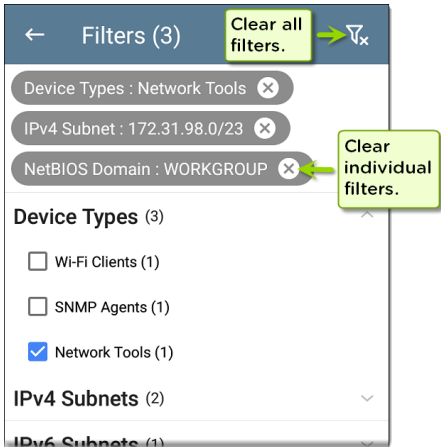
Filtering the Discovery List

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.

← Filters	
Device Types (13)	∨
IPv4 Subnets (63)	∨
IPv6 Subnets (1)	∨
VTP Domains & VLANs (2)	∨
NetBIOS Domains (4)	∨
SSIDs (76)	∨
Bands (2)	∨
Channels (22)	∨

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.

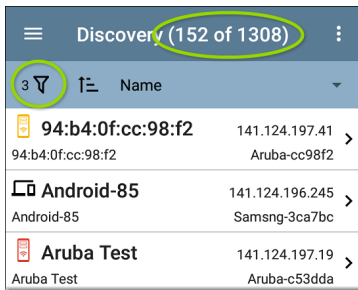
When filters are selected, those active filters are displayed at the top of the Filters screen.



- Tap the **X** 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.

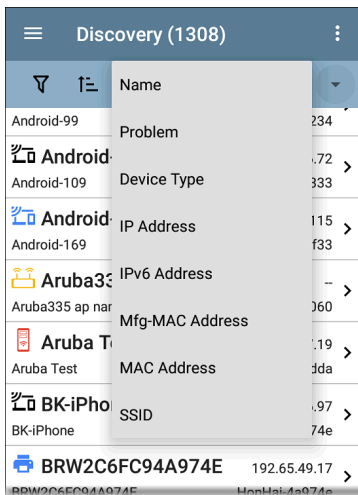


Back on the main Discovery screen, the screen title shows the number of filtered devices out of the total discovered devices (in the image above, 152 filtered devices out of 1308 total).

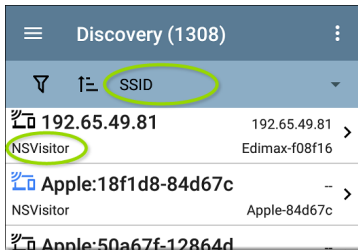
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

Sorting the Discovery List


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



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




The selected Sort option displays in the Sort bar above the device list, and the sort characteristic for each device is shown under the device type icon. In the image above, all the devices associated with the "NSVisitor" SSID are sorted together. Individual devices on the same SSID are sorted numerically and alphabetically.

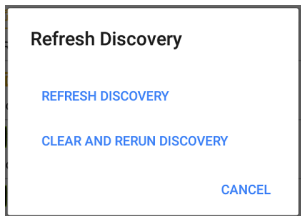
Tap the sort order icon  to switch the sort order between normal and reverse order.

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

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

Refreshing Discovery



Touch the action overflow icon  at the top right of the main Discovery screen, and select **Refresh Discovery** to refresh the Discovery process for both the Discovery and Wi-Fi apps.



REFRESH DISCOVERY restarts the 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.

**Link-Live**

by NetAlly



Discovery Snapshot Name

20190802_131842

Comment

1st Floor

Job Comment

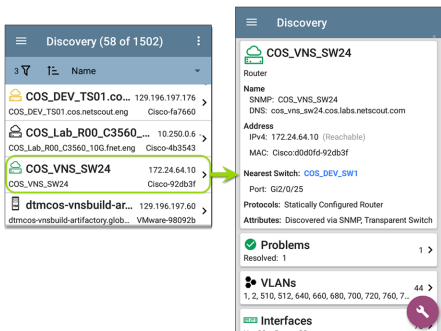
Psych Building**SAVE TO ANALYSIS FILES**

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


Discovery Details Screens


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


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





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


 **Discovery**


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

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

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

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

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




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

Each Details screen shows additional information about the selected device, any Problems detected by the 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 (Unassociated)
MAC: Aruba:186472-c53dda
Nearest Switch: [163.166.136.236](#)
Port: g1
Protocols: Statically Configured Router
Services: DHCP Server

The top of the card shows the device type 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).

 **Discovery**

 **Cisco3702**

Lightweight AP

Name
AP: Cisco3702
SNMP: Cisco3702

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

802.11
Channels: 1, 64
Type: 802.11ac

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

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

Last Seen: 5:23:20 PM

The 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 DNS, mDNS, SNMP, NetBIOS, AP, and Virtual Machine names if available.

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.

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

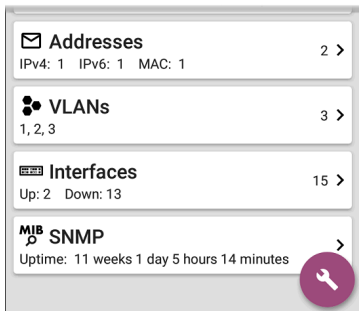
Guest OS: Operating system running on the virtual machine

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.



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

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

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

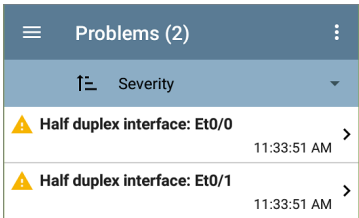
Remember, you can touch any card with a right pointing arrow ➤ to open a new screen with more information about the device or characteristic.

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.



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



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

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

☰ Problems - COS_DEV_TS... ⋮

⚠ Half duplex interface: Et0/0

First Detected: 11:33:51 AM

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

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

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

✉ **Addresses** 3 >

IPv4: 1 IPv6: 2 MAC: 1

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

Addresses (3)	
↑	Address
IPv4	10.250.0.120
	10.250.0.120
	10.250.0.0/22
	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.

Interfaces

Interface are discovered using SNMP.

 Interfaces	171 >
Up: 20 Down: 151	

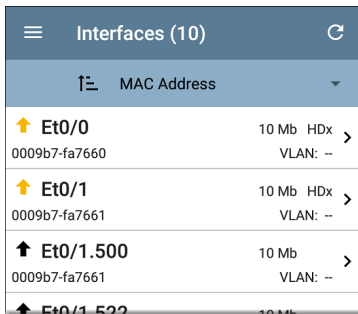
The Interfaces card shows the number of Up and Down interfaces and the total number of Interfaces to the right.

Tap the card to view the list of Interfaces.

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

Like other Discovery list screens, the Interfaces list provides a number of Sort options, and the selected sort option affects the type of information displayed. The image above shows Interfaces sorted by Status (up or down). The

image below shows Interfaces sorted by MAC Address, so each Interface's MAC address is displayed.



The screenshot shows a mobile application interface titled "Interfaces (10)". The header bar is dark blue with a hamburger menu icon on the left and a refresh icon on the right. Below the header, there is a sorting bar with a list icon, the text "MAC Address", and a dropdown arrow. The main content area displays a list of network interfaces. Each row includes an arrow icon (yellow for up, black for down), the interface name, its MAC address, speed, type, and a chevron icon. The visible rows are:

Sort Icon	Interface Name	MAC Address	Speed	Type	Action
↑	Et0/0	0009b7-fa7660	10 Mb	HDx	>
				VLAN: --	
↑	Et0/1	0009b7-fa7661	10 Mb	HDx	>
				VLAN: --	
↑	Et0/1.500	0009b7-fa7661	10 Mb		>
				VLAN: --	
↑	Et0/1.522		10 Mb		>

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

The screenshot shows the 'Et0/1' interface details screen. At the top, there is a blue header bar with a hamburger menu icon on the left, the text 'COS_DEV_TS01.cos.net...' in the center, and a refresh icon on the right. Below the header, the interface name 'Et0/1' is displayed with an upward-pointing arrow icon. The description reads 'DOT1Q Trunk to CISCO_3750_PoE COS_DEV_SW2 f...'. The status is 'up'. Below this, the following details are listed: Speed: 10 Mb, Duplex: HDx, and MTU: 1500. The connected device is 'COS_DEV_SW1' and the port is 'Gi2/0/30'. The address section shows the MAC address 'Cisco:0009b7-fa7661'. At the bottom, there are two expandable sections: 'Devices' with a folder icon and a count of '0', and 'Statistics' with a line graph icon and a right-pointing arrow. The statistics data shown is 'Util: 0.3 % Discards: 0.0 % Errors: 0.0 %'.

☰ COS_DEV_TS01.cos.net... ↻

↑ 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 >

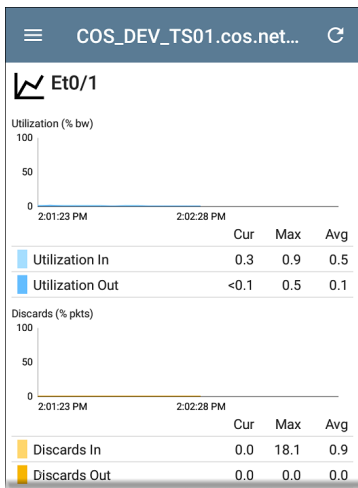
📈 Statistics >

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.

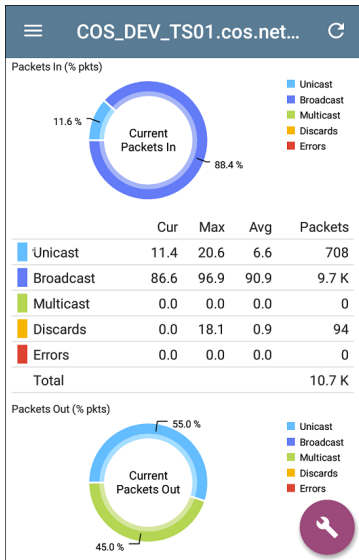
MTU: Maximum Transmission Unit, the maximum packet frame size configured on the interface port

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**.



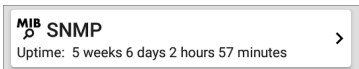
The Statistics screen displays real time Utilization, Packet Discards, Packet Errors, and

a pie chart breakdown of Packet transfers to and from the Interface.



SNMP

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



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



COS_DEV_SW34

MIB SNMP**SNMP System Group**

Uptime: 5 weeks 6 days 2 hours 58 minutes

Manufacturer: Cisco

Model: cat4500e

Serial Number: FOX1407GRJA

HW Version: V02

SW Version: 15.2(2)E7

Description:

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

Technical Support:

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

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

Compiled Wed 12-Jul-17 14:36 by

SNMP

Type: SNMP v1/v2/v3

Engine ID: 80000009030068efbd6f4b80

Communication: SNMP v2

Using: Default Community String: public

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

SNMP: SNMP versions the device supports, Engine ID (for v3), and how the 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 10.250.0.1	Gi1/0/38 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 10.250.3.32	-- NetAlly-02506e	>

Resources

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

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

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

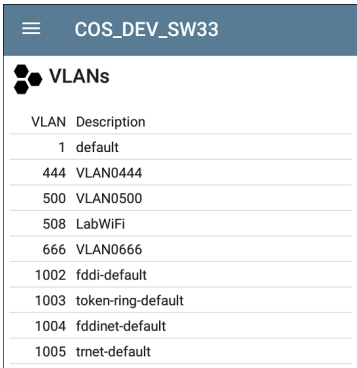
COS_DEV_SW34		
 Resources		
	Cur	Max
CPU %	12	12
Memory %	60	60
Last Update: 1:44:22 PM		

By default, 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.

VLANS

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

 VLANS	9 >
1, 444, 500, 508, 666, 1002, 1003, 1004, 1005	



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.

SSIDs

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



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

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

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



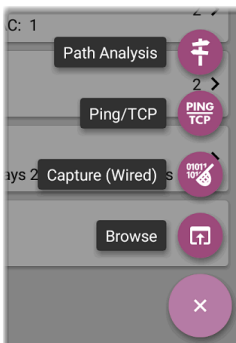
Using the Discovery FAB

The Floating Action Button (FAB) on Device Details screens offers additional actions depending on the device type and connection available.


Opening other apps, such as [Path Analysis](#), [Ping/TCP](#), or [Capture](#), from a Discovery


Details screen will auto-populate the app you open with the address and other device characteristics. In this way, 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.


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).

 **Discovery**

 **Rack5SW1.fnet.eng**
Router
Name
SNMP: Rack5SW1.fnet.eng
Address
IPv4: 10.250.3.207 (Reachable)
MAC: Cisco:00141c-8945c1
Nearest Switch: [COS_DEV_SW1](#)
Port: Gi2/0/39
Protocols: Statically Configured Router
Attributes: Discovered via SNMP, Transparent Switch

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

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

 **Interfaces** 
Up: 12 Down: 30

When a user opens the FAB and selects a different app, such as Path Analysis, only the address and name listed at the top 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

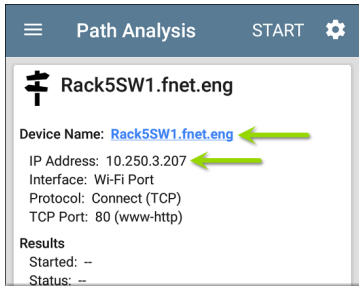
Path Analysis (button)

PING TCP (button)

Capture (Wired) (button)

Browse (button)

Close (button)



To open another screen or app with a different address, the user can touch 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.



 **Discovery**

 **cos-dev-sw18-poe**
Switch
Name
SNMP: cos-dev-sw18-poe
Address
IPv4: 10.250.3.216 (Reachable)
MAC: Cisco:503de5-220c43
Attributes: Discovered via SNMP, Transparent Switch

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

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

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

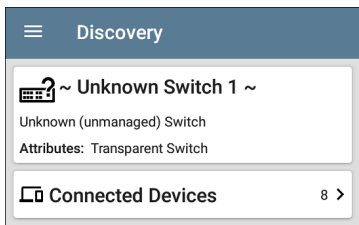
 **SNMP** 
Uptime: 27 weeks 2 days 7 hours 25 minutes

Unknown Switches

Unknown switches are detected indirectly 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.



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**

IP: 10.250.3.221 IPv6: 2001:c001:c0de:500:d1f5:d8e0:a81:3397 MAC: 000c29-13235b

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.

 **Discovery**

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

Hypervisor

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


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

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


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

Services: Hypervisor

Attributes: Port Aggregation

 **Addresses**


IPv4: 1 IPv6: 1 MAC: 1



Virtual Machines

VMware virtual machines are discovered by examining the VMware client table in VMware hypervisors that are SNMP enabled. Devices are also classified as Virtual Machines if they have a VMware MAC.

☰
Discovery



Cisco ACS 5.8 Linux

Virtual Machine

Name
Virtual Machine: Cisco ACS 5.8 Linux


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

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


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

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

Services: Virtual Machine




Addresses





IPv4: 1 IPv6: 2 MAC: 1


Wi-Fi Controllers


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.

 **Discovery**


 **Ntgear:3c3786-719307**
AP
Address
BSSID: [Ntgear:3c3786-719307](#)
802.11
Channels: 6, 36 (bonded)
Type: 802.11ax
Last Seen: 11:20:17 AM


 **Addresses** 2 >
BSSID: 2

See also [APs in the Wi-Fi analysis app](#).

Wi-Fi Clients

Wireless clients are discovered through wireless packet analysis and SNMP queries via 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.

 **Discovery**

 **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.

☰
Discovery



TOSHIBA e-STUDIO3005AC

Printer

Name

SNMP: TOSHIBA e-STUDIO3005AC

mDNS: MFP12073521


NetBIOS: MFP12073521

Address

IPv4: 143.131.143.43 (Reachable)

IPv6: fe80::280:91ff:feb8:3a31


MAC: Tokyo:008091-b83a31



Problems

1 >


Warnings: 1



Addresses

3 >


IPv4: 1 IPv6: 2 MAC: 1




Interfaces

2 >

Up: 2 Down: 0



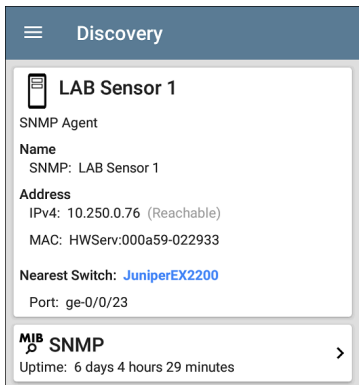
SNMP



SNMP Agents


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

NOTE: If 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](#).



The screenshot shows the 'Discovery' section of the app. At the top left is a hamburger menu icon. The title 'Discovery' is centered at the top. Below this is a card for 'LAB Sensor 1', which includes a mobile device icon, the title 'LAB Sensor 1', and the label 'SNMP Agent'. The card lists the following details: Name: SNMP: LAB Sensor 1; Address: IPv4: 10.250.0.76 (Reachable) and MAC: HWServ:000a59-022933; Nearest Switch: JuniperEX2200; Port: ge-0/0/23. Below this card is another card for 'MIB SNMP' with a right-pointing arrow and an uptime of 6 days 4 hours 29 minutes.

Discovery

 **LAB Sensor 1**
SNMP Agent

Name
SNMP: LAB Sensor 1

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

Nearest Switch: [JuniperEX2200](#)
Port: ge-0/0/23

MIB SNMP >
Uptime: 6 days 4 hours 29 minutes







See also [SNMP Details](#).

NetAlly Tools


The EtherScope can also identify other NetAlly network testers, including EtherScope nXGs,


AirCheck G2s, OneTouches, LinkRunners (AT and G2), and Test Accessories.


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


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	AirCheck G2	NetAlly-350593
 NetAlly:00c017-353246	AirCheck G2	NetAlly-353246
 10.250.2.117	LinkRunner G2	NetAlly-c50070
 10.250.2.132	Test Accessory	NetAlly-330e87

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

 **Discovery**

 **10.250.2.240**
LinkRunner G2
Address
IPv4: 10.250.2.240 (Reachable)
IPv6: fe80::2c0:17ff:fec5:88
MAC: NetAlly:00c017-c50088
Nearest Switch: [PV_Mike_NetgearGS110TP](#)
Port: g6
VLAN ID: 500

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


 **VLANs** 1 >
500

Hosts/Clients

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



Discovery

 ubuntu

Host/Client

Name

mDNS: ubuntu

Address

IPv4: 10.250.2.109 (Reachable)

IPv6: 2001:c001:c0de:500:b844:4388:4fb7:4506

MAC: ORICO:f01e34-1fbaa4

Nearest Switch: [PV_Mike_NetgearGS110TP](#)

Port: g3

VLAN ID: 500

 Addresses

4 >

IPv4: 1 IPv6: 3 MAC: 1


 VLANs

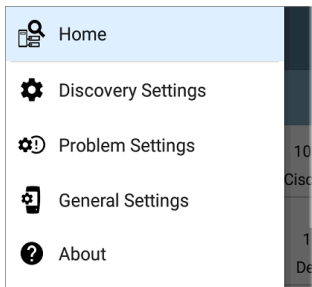
1 >

500

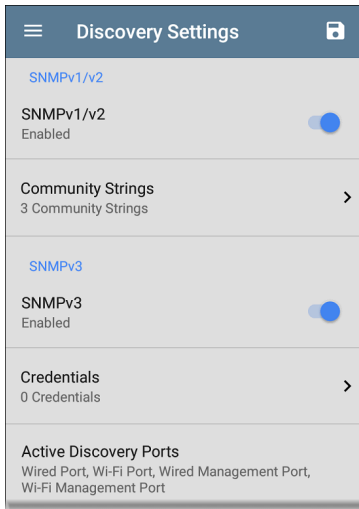
Discovery Settings

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](#) or back to [General Settings](#).)



To adjust Discovery Settings, follow these steps:

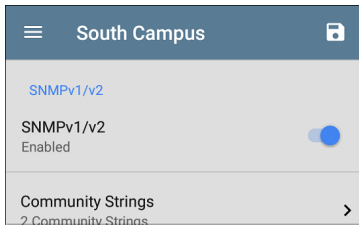
1. On the **Discovery Settings** screen, touch each field described in this topic, as needed, to select or enter your required configuration elements.

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 save 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.

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.



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

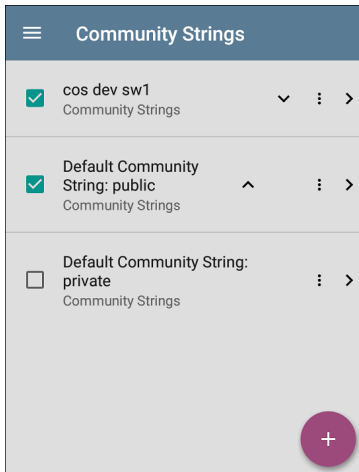
EtherScope uses to communicate with those devices.

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 String screen and add, edit, or remove 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.

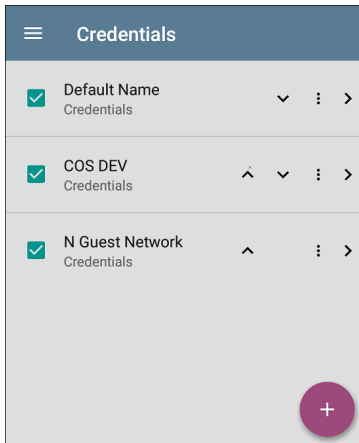
SNMPv3

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 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

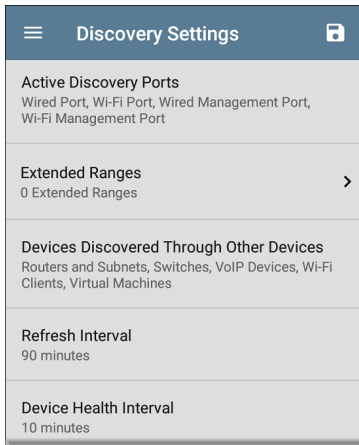
Touch to enter the SNMPv3 username.

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.



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

CANCEL

OK

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 Ether-Scope 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

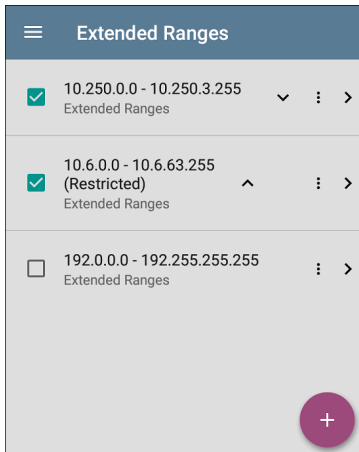
you want the Discovery process to run. Discovery sweeps all of the enabled Extended Ranges for devices, whether directly connected or off-net. The EtherScope performs Ping sweeps on subnets that are not directly connected and ARP sweeps on connected subnets.

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.

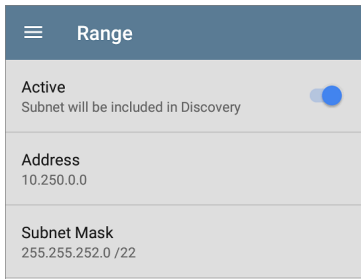
Configure both **SNMP Credential Sets** and **Extended Ranges** to ensure that the EtherScope always discovers management subnets, regardless of your network port connections.

Touch the field to open the Extended Ranges screen.



- Check or uncheck the boxes to include or exclude an extended range from the current Discovery configuration. Unchecked Extended Ranges do not affect the default Discovery behavior in the current configuration, but they may be used in other Discovery configurations (like Community Strings and Credentials).

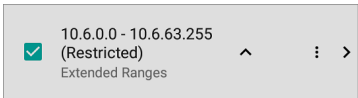
- Touch any Extended Range's row to edit its address and subnet.
- Touch the FAB  to add new extended ranges.



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

Active vs. Restricted Subnets

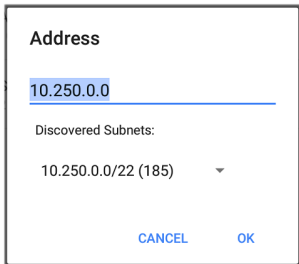
For each configured Extended Range, you can tap the toggle button to switch from **Active** to **Restricted**. Discovery is performed on Active Ranges. Setting a Range to **Restricted** disables the discovery process on that network or subnet, meaning the EtherScope will *not* communicate with devices within the restricted range.



- Restricted Ranges take precedence regardless of the order in which they are listed on the Extended Ranges screen.
- You can Restrict a part of a configured Active Extended Range.
- You can also restrict a single device, whether it is part of an Active Range or not. To enter a single device that you do not want discovered, enter its IP address in the Address field, and set the Subnet Mask field to 255.255.255.255.

Address

Tap the **Address** field to enter or select an IP address range.



Address

10.250.0.0

Discovered Subnets:

10.250.0.0/22 (185) ▼

CANCEL OK

Tap the drop-down menu to select a previously Discovered Subnet. The Address field 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

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

Routers and Subnets

When the Routers and Subnets checkbox is enabled, any discovered routers are included in discovery results. In addition, if Discovery has SNMP access to a discovered router, its routing tables are read, and the next hop routers are added to the Discovery list. If any local subnets are available in the routing tables, these are

also added to the Subnets list. This process continues until all the available SNMP credentials are tried for the added routers.

NOTES: Discovery does not sweep every discovered subnet; discovered subnets are only added to the subnets list. To perform discovery in a specific subnet, see **Extended Ranges** above.

If another site has routers you want to discover using this process, but there isn't a local next hop link from this site, you can add one of the routers of that site to discovery, 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.

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

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

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

CANCEL OK

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

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

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


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

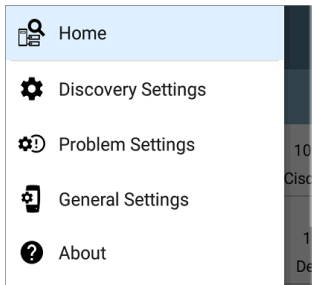
This function controls how long your EtherScope waits between SNMP queries to key tables that can cause CPU spikes in the SNMP agents, including the ARP cache, IP address table, routing tables, and FDB tables.

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.

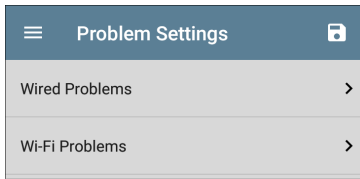
Problem Settings

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 configured Problem Settings by touching the save button  on this screen.




- **Load** opens a previously saved Problems configuration.
- **Save As** saves the current configuration with an existing name or a new custom name.


After you have saved a configuration, the custom name you entered appears in the title of the Problem Settings screen.

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	<input checked="" type="checkbox"/>	
Duplicate IP Address Enabled	<input checked="" type="checkbox"/>	
DHCP Server Not Responding Enabled	<input checked="" type="checkbox"/>	
EtherScope nXG Received Multiple DHCP Offers Enabled	<input checked="" type="checkbox"/>	
EtherScope nXG Received Used IP from DHCP Enabled	<input checked="" type="checkbox"/>	
EtherScope nXG Lost DHCP Lease Enabled	<input checked="" type="checkbox"/>	

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.



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 v1.0 can also detect and indicate the 802.11ax media type (also 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

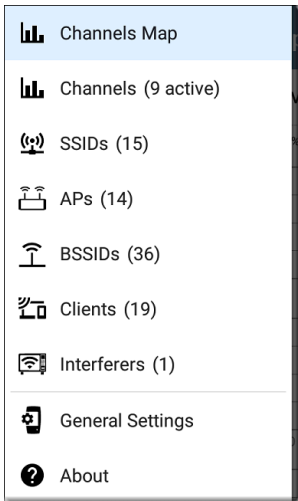
Wi-Fi Analysis utilizes the [Wi-Fi Test Port](#) to scan the channels and acquire information about your wireless networks. If the Wi-Fi Test Port is linked (for instance after running a [Wi-Fi AutoTest Profile](#)), the port unlinks and resumes scanning when you open the Wi-Fi Analysis app.

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.

Using the Wi-Fi App Screens


To switch between the different Wi-Fi app screens, tap the menu icon  (or swipe right) to open the left-side navigation drawer.



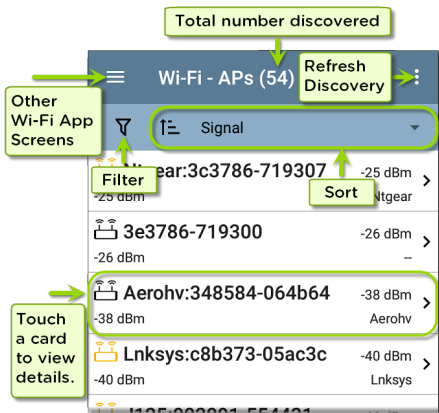
The Wi-Fi app's navigation drawer displays a real-time count (in parentheses) of each wireless component EtherScope has detected. Tap an option to open the corresponding screen.

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 view its details.

The example image below shows the APs screen with the common Wi-Fi app screen functions pointed out.

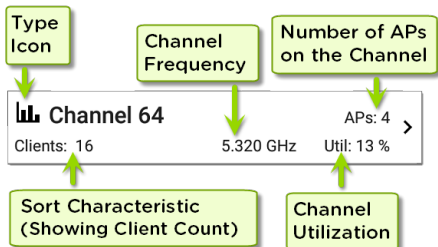


Like in AutoTest and other EtherScope screens, the icons in Wi-Fi analysis change color to indicate a **Warning** or **Failure** condition. The app also displays icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous 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 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.



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

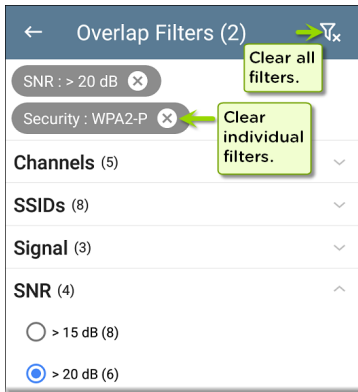
characteristics detected (for example, number of active Channels or detected Security types).

Touch a category to select filters by tapping the checkboxes or radio buttons.




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 **x** 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 .

Wi-Fi - Channels Map

UTILIZATION OVERLAP

2

CH 1 - 14 (2.4 GHz)
AP: Pegatn:600292-bc48c0 CH: 6

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).

Wi-Fi - APs (5 of 16)

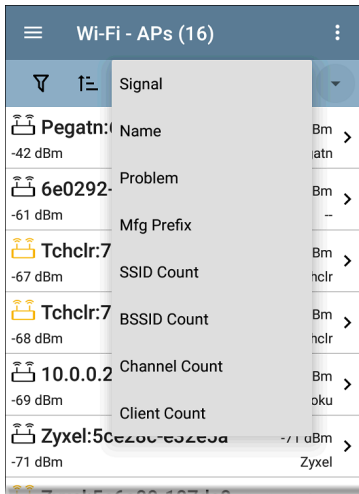
3 Signal

Pegatn:600292-bc48c0 -43 dBm >
-43 dBm Pegatn




6e0292-ba71f8 -60 dBm >

Sorting in the Wi-Fi App


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

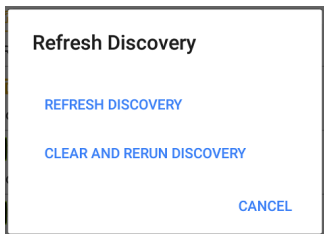
Tap the sort order icon  to switch the sort order between normal and reverse order.

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 Discovery



Touch the action overflow icon  at the top right of the screen, and select **Refresh Discovery** to refresh the Discovery process for both the Wi-Fi and Discovery apps.



REFRESH DISCOVERY restarts the Discovery process without clearing the already discovered devices.

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

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.

**Link-Live**

by NetAlly

**Wi-Fi Snapshot Name**20190812_210303

Comment3rd floor

Job CommentUnion Hall

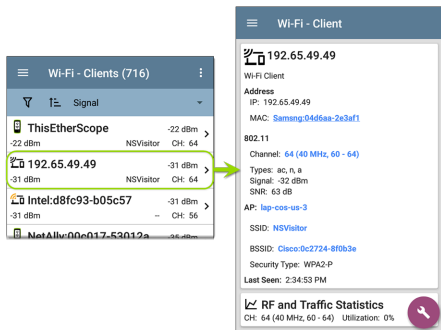
**SAVE TO ANALYSIS FILES**

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.





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.


 **Wi-Fi - Channel**


 **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	Filter	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.

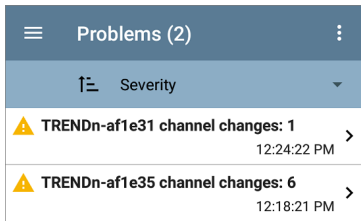
Wi-Fi Problems Screen

If any of the enabled Wi-Fi Problems are detected, the Problems card appears on the Wi-Fi Details screen.


The screenshot shows the 'Wi-Fi - AP' screen. At the top is a blue header with a hamburger menu icon and the text 'Wi-Fi - AP'. Below the header is a white card for the access point 'TRENDn:d8eb97-af1e2c'. The card contains the following information: an orange Wi-Fi router icon, the text 'AP', the AP ID 'TRENDn:d8eb97-af1e2c' (with a blue link), 'Mfg Prefix: TRENDn', '802.11', 'Types: ac, n, g, a, b', 'Security Type: WPA2-P', 'Signal: -54 dBm', and 'Last Seen: 3:47:10 PM'. Below this card is a 'Problems' card with a yellow warning triangle icon, the text 'Problems', 'Warnings: 2', and a '2 >' indicator. At the bottom is a partially visible 'SSIDs' card with a signal icon.

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.



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

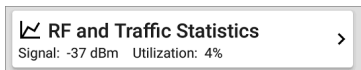
You can also tap the sort field to sort the list by **Severity** or by the time when the problem was **First Detected**. Touch the action overflow button  at the top right to **Clear Problems**.

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

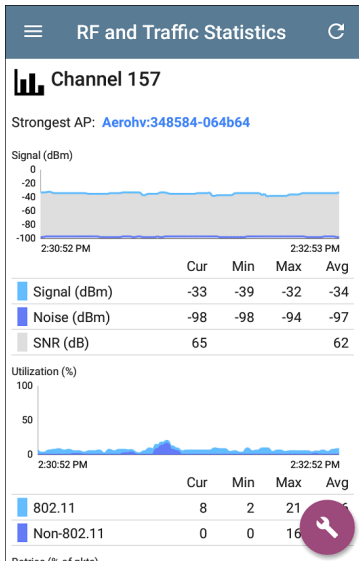
The Channel, BSSID, and Client Details screens can display RF and Traffic Statistics if any traffic is detected.

This section describes the common elements of the RF and Traffic Statistics screen. See the topic for each type of Details screen for differences.



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.



Strongest AP: The AP on the channel with the strongest signal

The graphs update in real time. You can touch and drag (or swipe) left and right on each graph

to move backward and forward in time and view the recorded measurements. The graphs save and display data for up to 24 hours in the past.

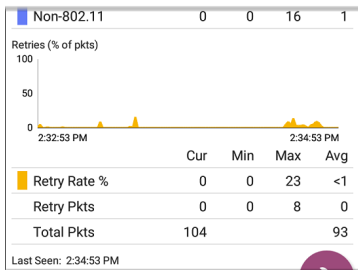
Under each graph, a legend table displays the Current, Minimum, Maximum, and Average measurements. The Current column contains measurements from the last second. Min, Max, and Avg columns show cumulative measurements gathered during the time the RF and Traffic screen has been open.

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)

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

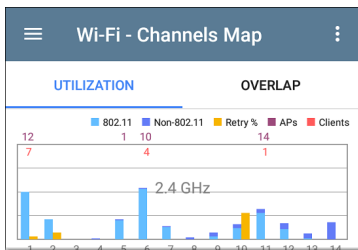


Retries (% of packets) graph: Plots percentage of transmitted packets that are retry packets

- **Retry Rate %** - The AP's signal strength in dBm
- **Retry Pkts** - The number of retry packets
- **Total Pkts** - The total number of transmitted packets

Channels Map

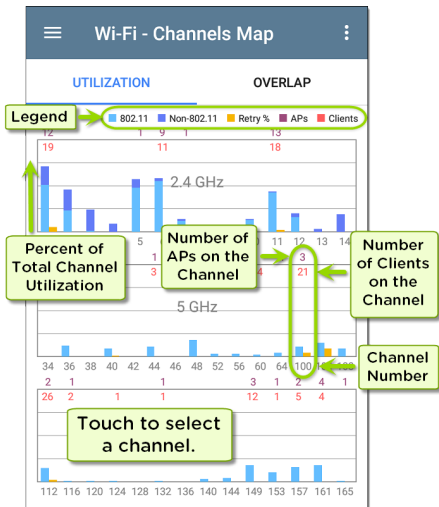
The Channels Map screens provide graphical representations of channel utilization, AP coverage, and overlap.



The Channels Map features two tabs: Utilization and Overlap. Touch the tab names to switch between the two screen types.

Channels Utilization

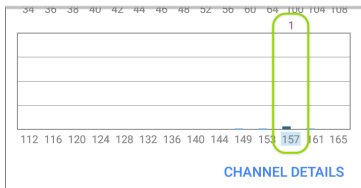
The Channels Utilization screen displays a bar graph of 802.11 and Non-802.11 utilization, retry percentage, and the number of APs and clients for each channel.



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.


APs are shown on their 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.

☰ **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** >



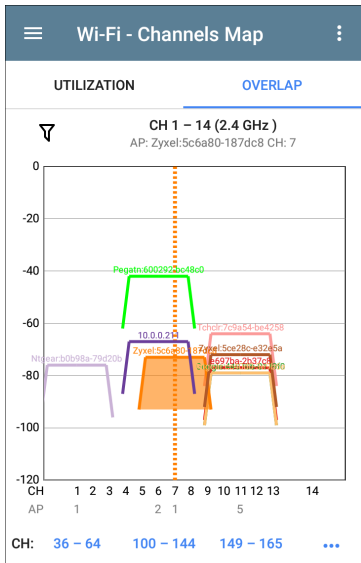
From the Channel Details screen, you can examine the addresses and devices operating on the channel and perform a deeper analysis.

See [Channel Details](#) for more about this screen.

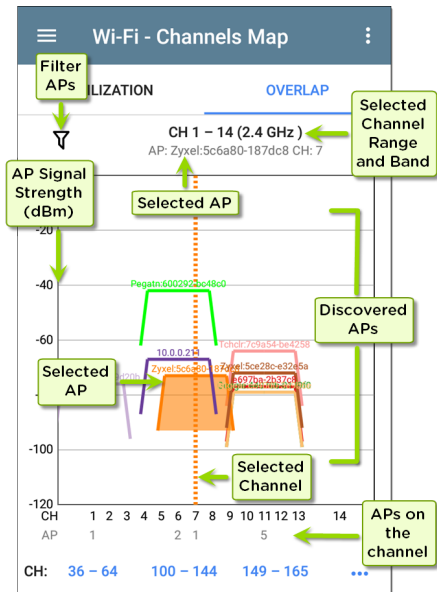
Channels Overlap

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.

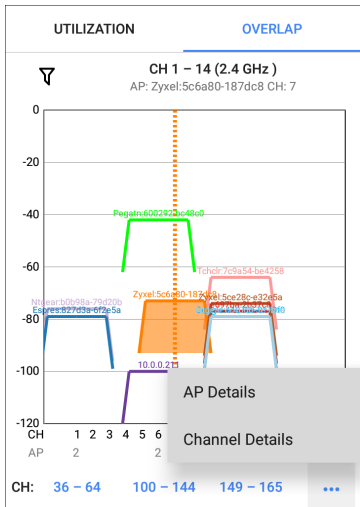
Each discovered AP is shown as a colored trapezoid and plotted on the graph based on its channel coverage (on the x-axis) and signal strength in dBm (on the y-axis).



- 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	Channel 7	2.442 GHz	APs: 0 Util: 0 %


Refer to [Using the Wi-Fi App Screens](#) if needed.


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.

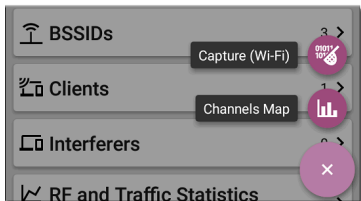
Dynamic Frequency Selection (DFS) channels also display an Attributes field that indicates DFS.

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)		
Filter	Sort	Signal
 Cisco WEP64 OA	-61 dBm	 APs: 1
 HNTNetgear2.4G	-61 dBm	 APs: 1
 Cisco 5G	-62 dBm	 APs: 2
 CiscoQATest-mañana	-62 dBm	 APs: 1
 Cisco WEP128 OA	-62 dBm	 APs: 1
 Cisco WEP128 SA	-62 dBm	 APs: 1
 Home-Guest-2.4G	-62 dBm	 APs: 1

Refer to [Using the Wi-Fi App Screens](#) 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


☰ Wi-Fi - SSID


 **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

 **APs** 1 >

 **BSSIDs** 1 >

 **Channels** 1 >

 **Clients** 0 >



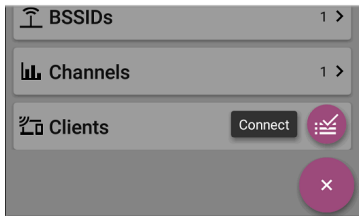
In addition to the Signal and Security Type, the SSID Details displays the AP on the network with the strongest signal, 802.11 Types that the

APs in the network support, and the time the EtherScope last detected activity on the network (Last Seen).

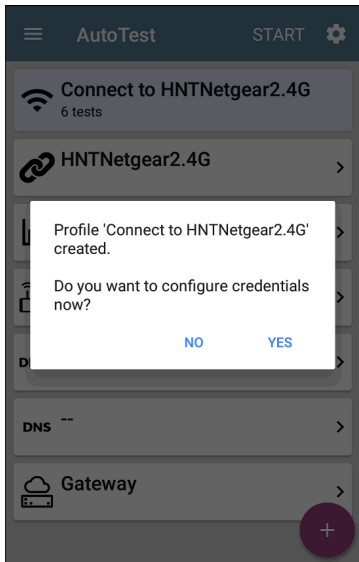
EtherScope nXG can detect and display 802.11 types a/b/g/n/ac/ax.

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]."




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.

Wi-Fi - APs (54)		
Filter	Sort	Signal
	Ntgear:3c3786-719307	-26 dBm > Ntgear
	3e3786-719300	-29 dBm > --
	Lnksys:c8b373-05ac3c	-39 dBm > Lnksys
	Aerohv:348584-064b64	-40 dBm > Aerohv
	J125:002091-554431	-46 dBm > J125
	Lnksys:c8d719-a51bcb	-48 dBm > Lnksys
	Cisco3702 Kris A	-50 dBm


Use the Filter  and Sort functions to determine which APs are shown and their order in the list. Refer to [Using the Wi-Fi App Screens](#) 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

☰ Wi-Fi - AP

 **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 802.11 ax 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	Nighthawk-Guest ...	CH: 6
 Ntgear:3c3786-719307	-28 dBm	Nighthawk 802.1...	CH: 6
 Ntgear:3c3786-719306	-37 dBm	Nighthawk 802.1...	CH: 36
 Aerohv:348584-064b64	-39 dBm	HNT 802.11ax	CH: 157
 Lnksys:c8b373-05ac3b	-42 dBm	The Office Netwo...	CH: 1
 Lnksys:c8d719-a51bcb	-48 dBm	Linksys15538	CH: 1
 1125-002091-554431	-49 dBm		


Refer to [Using the Wi-Fi App Screens](#) 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 2.4GHz**

AP: **Ntgear:3c3786-719307**

BSSID: 3c3786-719307

802.11

Channel: **6**

Types: ax, n, g, b

Signal: -37 dBm


SNR: 56 dB

Security Type: WPA2-P

Last Seen: 2:09:41 PM

↕ Rates and Capabilities >

📶 Clients 0 >

📈 RF and Traffic Statistics 

CH: 6 Utilization: 4%

In addition to the characteristics on the BSSID cards, the Details screen displays supported 802.11 Types, a Signal-to-Noise ratio (SNR)

measurement, the active Security Type, and the 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 Details 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.



Rates and Capabilities

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

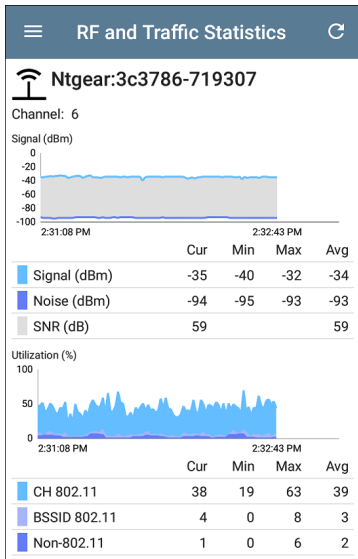
MU Cascading Support: false

Ack-Enabled Aggregation Support: false

DM Control Support: false

BSSID RF and Traffic Statistics

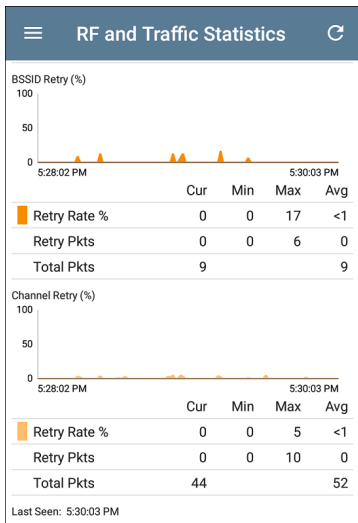
See [RF and Traffic Statistics Overview](#) in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.



The RF and Traffic Statistics screen for BSSIDs displays the BSSID and the channel number at the top of the screen.

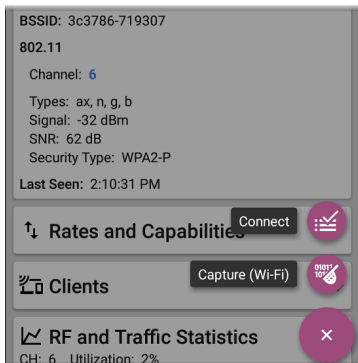
The Utilization graph shows separate measurements for Channel Utilization, BSSID Utilization, and Non-802.11 interference using different colors.

The screen also displays separate graphs for Channel Retries and BSSID Retries.



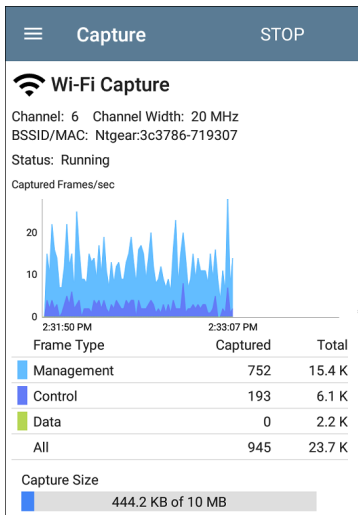
BSSID FAB

The FAB on the BSSID screen lets you **Connect** to the BSSID or record a packet **Capture** of the network traffic with the current BSSID on the connected channel.



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.





Clients


The Clients list screen displays the wireless clients the EtherScope has discovered connected to your wireless networks.

Wi-Fi - Clients (69)			
Filter	Sort	Signal	
	ThisEtherScope	-21 dBm	>
-21 dBm	ALNFTN-A	CH: 36	
	192.65.49.49	-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	
	UGSI:6c0b84-c1f09f	-46 dBm	>
-46 dBm	--	CH: 149	
	AzureW:485d60-71cb81	-49 dBm	>
-49 dBm	NSVisitor	CH: 11	

Refer to [Using the Wi-Fi App Screens](#) 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 show 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

☰ **Wi-Fi - Client**

 **192.65.49.49**

Wi-Fi Client

Address
IP: 192.65.49.49
MAC: [Samsng:04d6aa-2e3af1](#)

802.11
Channel: **11**
Types: n, g, b
Signal: -29 dBm
SNR: 66 dB


AP: [lap-cos-us-3](#)

SSID: [NSVisitor](#)

BSSID: [Cisco:0c2724-8f0b31](#)

Security Type: WPA2-P

Last Seen: 2:51:36 PM

 **RF and Traffic Statistics** 

CH: 11 Utilization: 0%


The top Client Details card for a connected Client displays the following information:

- Client's **MAC** address
- 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
- **Security** type of the network
- 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

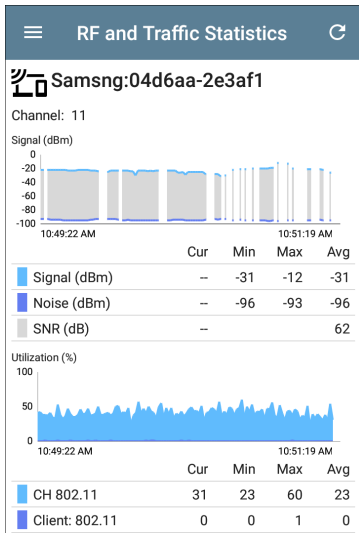
 **RF and Traffic Statistics** >

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.

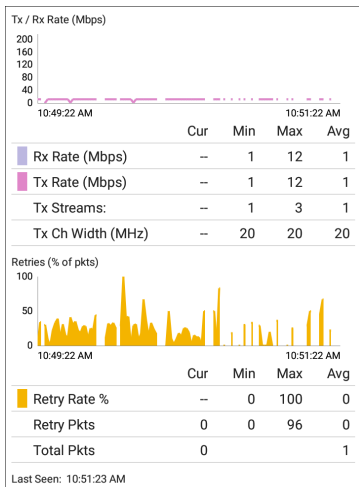
The RF and Traffic Statistics screen for Clients displays the Client's MAC or IP address and the channel number at the top of the screen.



The Utilization graph for Clients shows separate measurements for Channel (CH) Utilization and Client Utilization, using different colors.

The breaks in the Client RF and Traffic graphs occur because the Client is not consistently

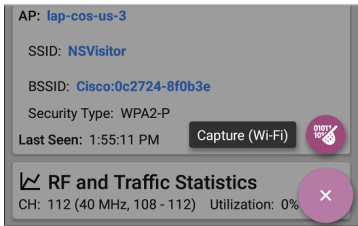
transmitting, so there is no data for EtherScope to display during those times.



The Clients RF and Traffic Statistics screen also displays a graph of Transfer (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 open the **Capture** app and record a packet capture of traffic going to and from the client.



When you open Capture from the Client Details FAB, the Capture app will be populated with the Channel number and MAC address of the client.

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 [Using the Wi-Fi App Screens](#) 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

 **Wi-Fi - Interferer**

 **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

CANCEL OK

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.

The screenshot displays the Path Analysis App interface. At the top, there is a blue header bar with a hamburger menu icon on the left, the text "Path Analysis" in the center, and "START" and a gear icon on the right. Below the header, the main content is organized into several cards:


- Test Card:** Features a flag icon, the domain "www.google.com", and latency values "10 ms, 6 ms, 11 ms". It lists "Device Name: www.google.com", "IP Address: 172.217.1.206", "Interface: Any Port", "Protocol: Connect (TCP)", and "TCP Port: 80 (www-http)". A "Results" section shows "Started: 2:26:58 PM" and "Status: Destination reached in 11 hops".
- Source Device Card:** Shows a smartphone icon, the name "ThisEtherScope", and a right-pointing chevron. Below it, it specifies "Out: Wired Port" and "1 Gb FDx".
- Layer 2 Path Card:** Includes a keyboard icon, the title "Layer 2 Path", and the text "No layer 2 devices discovered".
- Destination Card:** Shows a server icon, the domain "sr-cos-us-1.net.com", latency values "13 ms, 12 ms, 3 ms", and "Hop: 1" with a right-pointing chevron.
- IP Card:** Shows a cloud icon and the IP address "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
[UPLOAD TO LINK-LIVE](#)

The top Path Analysis results card shows the path's Destination address at the top, followed by the three response times from the TCP Connect, Ping, or Echo tests.

Device Name: Resolved DNS name or IP address of the destination entered in the settings

IP Address: IPv4 address of the target destination

Interface: The Interface option selected in the settings

Protocol: The Protocol selected in the settings (TCP, Ping, or Echo)

TCP Port: The port number used for a TCP Connect Protocol. This field does not appear for Ping or Echo Protocol results.

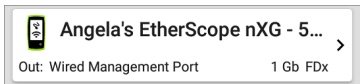
Results

Started: Time at which the Path Analysis began

Status: Current status of the Path Analysis test, including any error messages

UPLOAD TO LINK-LIVE: 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

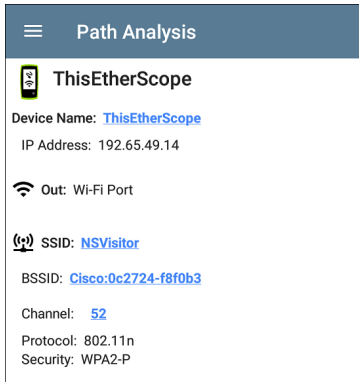


The source This EtherScope card displays the port from which the Path Analysis ran.

- 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.




The screenshot shows the Path Analysis App interface. At the top, there is a blue header with a hamburger menu icon on the left and the text 'Path Analysis' in white. Below the header, the device name 'ThisEtherScope' is displayed next to a small icon of a smartphone. The device name is followed by several lines of information: 'Device Name: ThisEtherScope', 'IP Address: 192.65.49.14', 'Out: Wi-Fi Port' (with a Wi-Fi icon), 'SSID: NSVisitor' (with a Wi-Fi icon), 'BSSID: Cisco:0c2724-f8f0b3', 'Channel: 52', 'Protocol: 802.11n', and 'Security: WPA2-P'. All the values for Device Name, SSID, BSSID, Channel, Protocol, and Security are highlighted in blue, suggesting they are clickable links.

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.


☰
Path Analysis



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

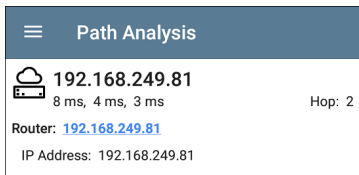
8 ms, 4 ms, 3 ms

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.



The screenshot shows a card titled "Path Analysis" with a hamburger menu icon on the left. Below the title, there is a cloud and server icon, followed by the IP address "192.168.249.81" in a large font. Underneath the IP address, the text "8 ms, 4 ms, 3 ms" is displayed. To the right of this text, it says "Hop: 2". Below these elements, the text "Router: [192.168.249.81](#)" is shown, with the IP address as a blue link. At the bottom of the card, it says "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.

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


Split Route

Path Analyses may obtain a "Split Route" result (as shown above), meaning that two or three

different routers within the same hop responded to the the three requests.

Tap a Split Route card to view the DNS names and IP addresses of the responding routers.

☰
Path Analysis



Split Route

41 ms, 25 ms, 34 ms

Hop: 8

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

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.

☰
Path Analysis




COS_DEV_SW1

13 ms, 12 ms, 13 ms

Hop: 3

Router: [COS_DEV_SW1](#)

IP Address: 192.168.249.82

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

Speed: 1 Gb

Duplex: FDx

Statistics

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



Tapping the [blue linked](#) switch name 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.

 **Path Analysis** START 



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

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



[UPLOAD TO LINK-LIVE](#)

 **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

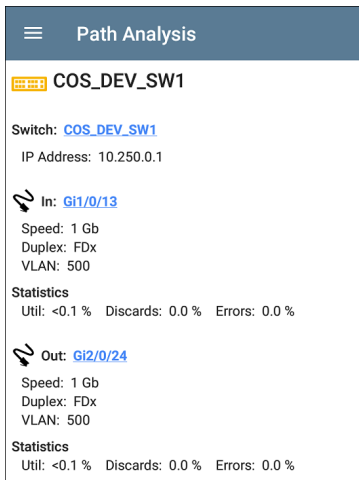
 **Cetus** 

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.



The screenshot shows a mobile application interface with a dark blue header containing a hamburger menu icon and the text "Path Analysis". Below the header, the device name "COS_DEV_SW1" is displayed with a yellow keyboard icon to its left. The main content area is white and contains the following information:

- 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.




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:

**Link-Live**

by NetAlly




Path Analysis Name

Comment

Job Comment



SAVE TO ANALYSIS FILES

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



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, 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 your saved 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 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 NPT Reflector software from NetAlly.com/support/downloads.

In this Chapter



Performance Test Settings

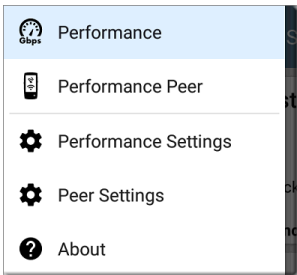
Running a Performance Test

Running EtherScope as a Performance Peer

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.

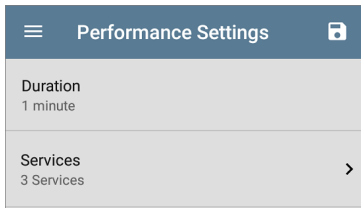
- **Services** include the Endpoint, Frame Size, Bandwidth, grading Thresholds, and Layer 2 and 3 Options. Services can be used in any number of saved Performance Tests.
- Saved **Performance Tests** contain a test Duration setting and the included Services.


For example, you can configure Services for multiple endpoints at different locations and

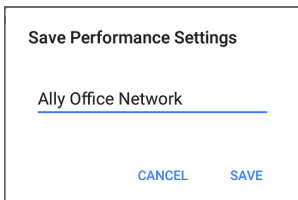
with different bandwidths. A user can also create multiple Services with different QoS priorities (using the Layer 3 options) to verify that loss does not occur over the higher priority stream.

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

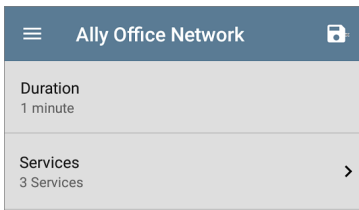
Open the Performance Settings screen  from the main Performance results screen or the left-side navigation drawer .



Touch the save icon , and select **Save As** to enter a new custom name for your currently configured Performance Test. Select **Load** to load a previously saved configuration.




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




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

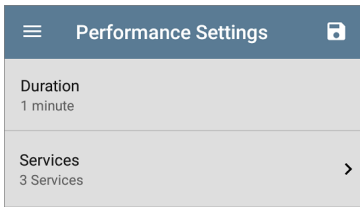
 **Ally Office Network**
Gbps


Duration: 1 minute
Started: 3:27:07 PM
Status: Next update in 26 seconds

	Loss	Latency	Jitter
 OneTouch 10G Peer >			
Up	--	--	--

Configuring the Source EtherScope nXG

Open the Performance Settings screen from the main Performance results screen  or the left-side navigation drawer .



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 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.

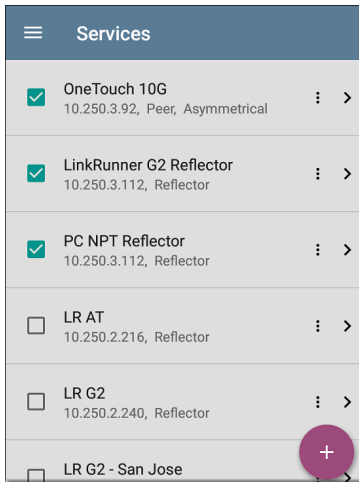
Services

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.


Touch the **Services** field in Performance Settings to open the Services screen.



On the Services 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	
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 TOS: Default (0)	>

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.

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

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

Communication UDP Port: If needed, 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 frame size or enter a custom value. The default is 512 Bytes.

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.



Bandwidth	
Upstream Target Rate	1 Mbps
Downstream Target Rate	10 Mbps

- If you are configuring a Reflector endpoint or you have selected Symmetrical Traffic Flow for a Peer endpoint, only one Target Rate is used.

- For a Peer with an Asymmetrical Traffic Flow configuration, you can select a different Upstream and Downstream Target Rate for each direction.

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.

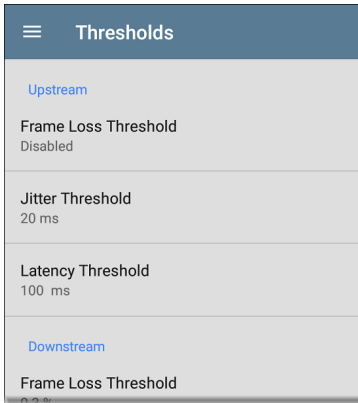
Thresholds

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.



Tap each Threshold field to select or enter the maximum value allowed. If a measured value exceeds the threshold value, the test fails.

Frame Loss Threshold: The Frame Loss Threshold is the percentage of frames that can

be lost before the test fails. The default is 0.3%. Tap the field to select or enter a new threshold or to disable grading based on frame loss altogether.

Jitter Threshold: Jitter is a measure of the variation in frame-to-frame latency in milliseconds. The default threshold is 20 ms.

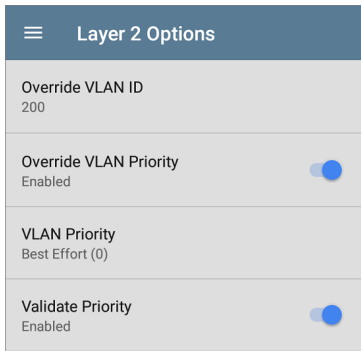
Latency Threshold: Latency is the amount of time it takes for a packet to go from the source to the endpoint and endpoint to source in milliseconds. The default threshold is 100 ms.

Layer 2 Options

The Performance Test runs over the [Wired Test Port](#) link established by an [AutoTest Wired Profile](#). Therefore, by default, the Performance Test runs using the VLAN ID configured in the settings of the Wired AutoTest Profile that established the link.

To test other VLANs, for example, those that make up a trunk port, configure the Layer 2 Options in your separate Services to test the corresponding VLANs.

Open **Layer 2 Options** in the Performance app settings to override the VLAN settings from AutoTest.



Override VLAN ID: 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.

Layer 3 Options	
QoS TOS With DSCP	
DSCP AF13 (14)	
Validate QoS Disabled	<input type="checkbox"/>

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.

Configuring Performance Endpoints

EtherScope nXG can run a Performance Test to any of the following Endpoints:

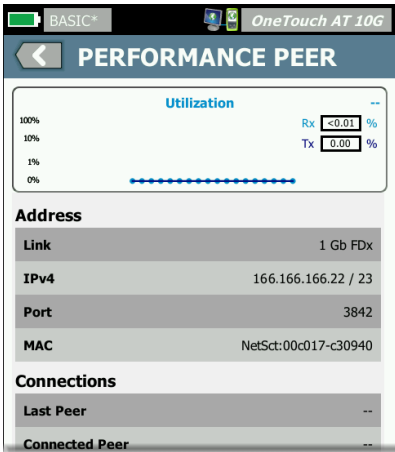
- Another EtherScope nXG (Peer)
- A OneTouch AT 10G (Peer)
- A LinkRunner G2 or LinkRunner AT (Reflector)
- NPT Reflector Software (Reflector)

See our website NetAlly.com for more information about [OneTouch](#) and [LinkRunner](#) and to download the free NPT Reflector PC application.

Using the EtherScope Performance Peer


To run an EtherScope nXG as a Performance Peer, see the [Running as a Performance Peer](#) topic.

OneTouch 10G Performance Peer



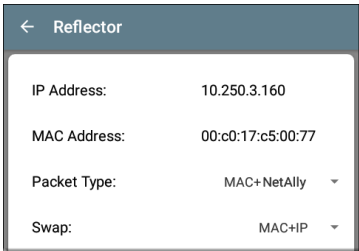
Follow these steps to set up a OneTouch 10G Performance Peer:

1. Ensure the OneTouch is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.


2. With the unit powered on, 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



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**  **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



Configure


1000
FDx

Start

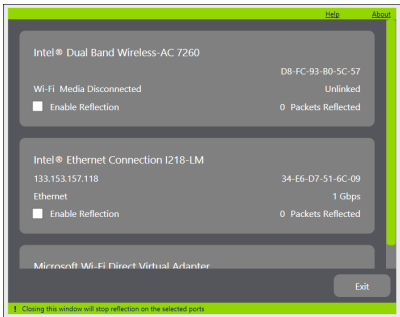
Follow these steps to set up a LinkRunner AT (2000) Reflector:

1. Ensure the LinkRunner is connected to an active network via the RJ-45 or Fiber test port and is plugged into AC power.
2. On the Home screen, select **Tools**.
3. In **General Configuration > Manage Power**, ensure the **Auto Shutoff Enabled** is unchecked to prevent the unit from powering down during the test. **Save** the changed setting.
4. In the Tools menu, select **Reflector**.

5. On the Reflector Screen, **Configure** the **Packet Type** and **Swap** settings as required. The default settings, **Packet Type: MAC + NetAlly** and **Swap: MAC + IP**, are recommended to avoid any undesired traffic on your network.
6. Select **Save** to apply any changed settings.
7. Select **Start** (F2) to run the Reflector.
8. The IP address of the Reflector is displayed at the top of the screen. Enter this address on the **Endpoint Device** screen in the 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



Follow these steps to set up the NPT Reflector PC application:

1. Download the software from [NetAlly.com/support/downloads](https://www.netally.com/support/downloads).
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

The screenshot shows the Performance Test App interface. At the top, there is a blue header bar with a menu icon, the word "Performance", a "START" button, a gear icon for settings, and a vertical ellipsis icon. Below the header, a white card displays the results of a "New Performance Test". The test duration is 1 minute, it started at 2:21:40 PM, and its status is "Success". Below this, a table lists the performance metrics for three services: OneTouch 10G, LinkRunner G2 Reflector, and PC NPT Reflector. The table has columns for Loss, Latency, and Jitter. OneTouch 10G shows 0% loss, 32 us latency, and <1 us jitter for both Up and Down directions. LinkRunner G2 Reflector shows 0.007% loss, 15 us latency, and <1 us jitter for Round Trip. PC NPT Reflector shows 0.057% loss, 464 us latency, and 101 us jitter for Round Trip.

	Loss	Latency	Jitter
OneTouch 10G			
Up	0 %	32 us	<1 us
Down	0 %	32 us	<1 us
LinkRunner G2 Reflector			
Round Trip	0.007 %	15 us	<1 us
PC NPT Reflector			
Round Trip	0.057 %	464 us	101 us

The Performance Test results update every 30 seconds, unless you are running a 10 second test, in which case, all results display after 10 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

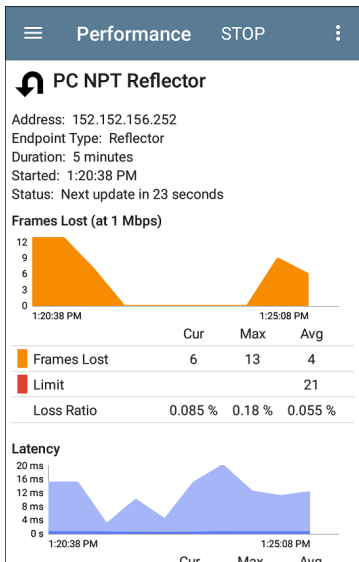
Started: Time at which the test began

Status: Current status of the test, including any error messages

Each card beneath corresponds to a configured Service and displays the Up, Down, Up and Down, or Round Trip measurements for 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



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

Loss, Latency, and Jitter Graphs

The graphs described in this section update in real time 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. If the test is long enough, you can touch and drag (or swipe) left and right on each graph to move backward and forward in time and view the recorded measurements.

Under each graph, a legend table indicates the meanings of the colors that correspond to different measurements.

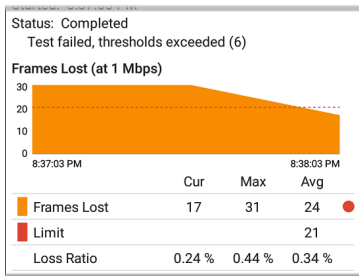
	Cur	Max	Avg
 Peak Latency Down	26.4 us	26.6 us	
 Latency Down	24.7 us	24.7 us	24.7 us
 Limit			100 ms

The table also displays the Current, Maximum, and Average measurements. The Current

columns contain measurements from the last interval. Performance test intervals are typically 30 seconds, unless you are running a 10-second test; then, there is only one interval of 10 seconds. The Min, Max, and Avg columns show cumulative measurements gathered during the test duration.

Peer endpoints display separate Up and Down measurements for Frames Lost, Latency, and Jitter, while Reflector endpoints display one round trip measurement for each.

Loss



Frames Lost (Up/Down) (at Target Rate):

Frame loss is quantified by the number of frames received subtracted from the number of frames sent.

The Target Rate from the Performance Settings is shown in parentheses next to the Frames Lost heading. In the image above, the configured Target Rate is 1 Mbps.

Limit: This is the Frame Loss Threshold for one interval (usually 30 seconds). 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).

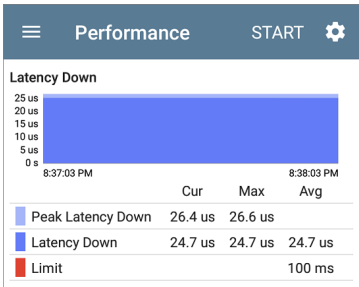
In the image above, the test has failed because Frame Loss was above the Limit.

Loss Ratio: The percentage of total frames that were lost

NOTE (for 10G 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

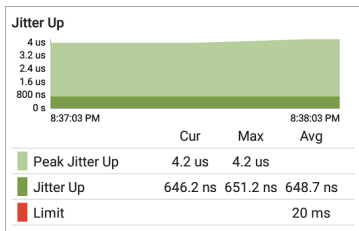


Latency (Up/Down): Latency is the amount of time it takes for a packet to go from the source to the endpoint or from the endpoint to the source (in milliseconds). Latency is calculated

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. 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).





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. 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).

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.

**Link-Live**

by NetAlly


**Comment****Job Comment**

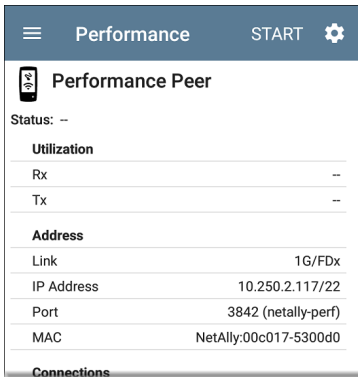
SAVE TO LINK-LIVE

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**.



The screenshot shows the Performance app interface. At the top, there is a dark blue header with a menu icon (three horizontal lines), the word "Performance", the word "START", and a gear icon for settings. Below the header, there is a section titled "Performance Peer" with a small icon of a mobile device. Underneath, the status is shown as "Status: --". There are two sections: "Utilization" and "Address". The "Utilization" section has two rows: "Rx" and "Tx", both with "--" values. The "Address" section has four rows: "Link" with "1G/FDx", "IP Address" with "10.250.2.117/22", "Port" with "3842 (netally-perf)", and "MAC" with "NetAlly:00c017-5300d0". At the bottom, there is a section titled "Connections".

Utilization	
Rx	--
Tx	--

Address	
Link	1G/FDx
IP Address	10.250.2.117/22
Port	3842 (netally-perf)
MAC	NetAlly:00c017-5300d0

Connections

The [Wired Test Port](#) must be linked (by running an [AutoTest Wired Profile](#)) for the Performance Peer function to run. If the port is not linked, a Status message displays, "The wired test port is not linked."

Performance Peer Setting


The only setting for the Performance Peer function is the **Communication UDP Port**.

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		STOP
	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



iPerf Test App

iPerf is a standardized network performance tool used to measure UDP or TCP capacity and throughput.

The iPerf App runs an iPerf3 performance test using a NetAlly Test Accessory or an iPerf server endpoint installed on a PC.



The NetAlly Test Accessory runs network connection tests, uploads results to [Link-Live Cloud Service](#), and acts as an iPerf server endpoint for iPerf tests run by other NetAlly handheld testers.

Learn more about the Test Accessory from [NetAlly.com/products/TestAccessory](https://www.netally.com/products/TestAccessory).

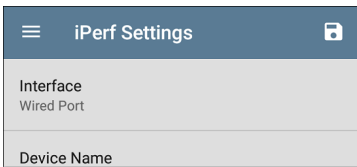
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the EtherScope iPerf test. You can download iPerf server software from <https://iperf.fr>.


iPerf Settings

To run an iPerf test, you must configure your EtherScope unit to communicate with your iPerf endpoint. You can manually enter its address or select a NetAlly Test Accessory from the [Discovery app](#) if the unit is discoverable.

Saving Custom iPerf Settings

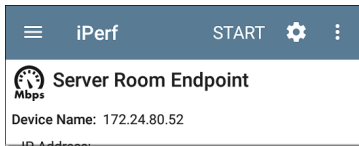
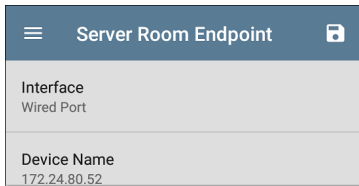
The iPerf app allows you to save a configuration of settings for running an iPerf test to the same endpoint later.



Touch the save icon , and select **Save As** to enter a new custom name for your currently configured settings. Select **Load** to load a previously saved configuration.

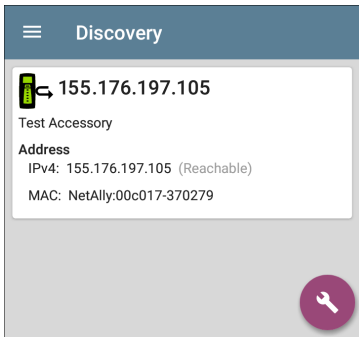
Once you save a settings configuration, the custom name you entered appears at the top of

the iPerf settings and results screens. In the example images here, the user has saved a custom iPerf configuration called "Server Room Endpoint."



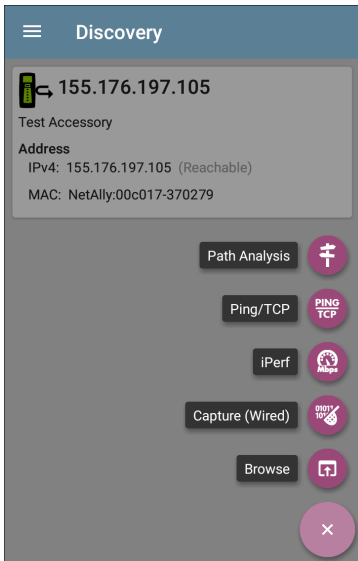
Populating a Test Accessory Address from Discovery

1. Open the Discovery app, and select an active **Test Accessory** from the main Discovery list to open the device details screen.



2. Open the Floating Action Button (FAB) menu.





3. Then, select the **iPerf** app button.

The iPerf app opens with the IP address populated from the Test Accessory selected in Discovery.



iPerf

START



New iPerf Test

Device Name: [155.176.197.105](#)


IP Address: 155.176.197.105


Interface: Wired Management Port

Results

Configuring iPerf Settings Manually

To configure the iPerf test settings manually, open the settings  on the iPerf screen.

iPerf Settings 	
Interface	Wired Port
Device Name	172.24.80.52
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, Wired or Wi-Fi Test Port, or Wired or Wi-Fi Management Port. See [Test and Management Ports](#) for explanations of the different ports.

Device Name: Enter the IP address or DNS name of the target iPerf server. Only IPv4 addresses are allowed for iPerf testing.

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.

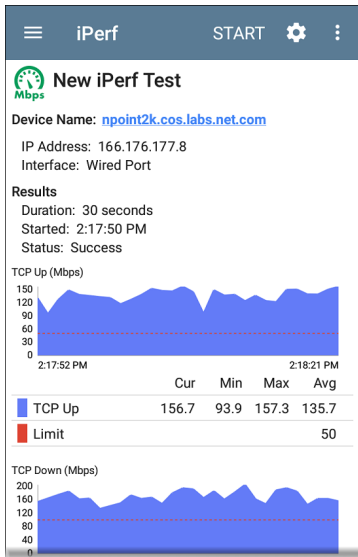
Upstream and Downstream Thresholds: Thresholds are the values the EtherScope uses to grade the test as **Pass** or **Fail**. iPerf thresholds are throughput rates. The default is

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.



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 speed.

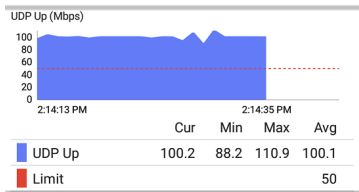
Device Name: Hostname or address of the iPerf server/Test Accessory

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 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.

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**.

**Link-Live**

by NetAlly

**Iperf Result Filename**

20190619_134743


Comment

Room 302

Job Comment

Union Hall

**SAVE TO LINK-LIVE**

The Link-Live sharing screen opens and allows you to revise the auto-generated filename and attach comments to the iPerf result, which will be displayed on the Results  page on Link-Live.

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



Link-Live Cloud Service

The screenshot displays the Link-Live Cloud Service interface. On the left, a list of test results is shown, each with a folder icon, a name, and a timestamp. The main area shows detailed information for a specific test: 'Angela's LinkRunner G2 - C50077' performed on Feb 15, 2018 at 12:32 PM. The interface is divided into several sections:

- Test:** Provides basic device information: MAC (00CE17-C50077), Device (LinkRunner G2), IPv6 (False), Type (Ethernet), Profile (Link-Live), and Firmware (1.80.25.20180129).
- Port:** Lists port statistics: Unloaded (53.3 V), Rxq Power (139W Class 0), Rxd Power (139W Class 0), Pair (Pos: 3.6 Neg: 1.2), PSE Type (Type1/2), and Present (True).
- Link:** Shows link status: Speed (1000), Adv Speed (10/100/1000), Duplex (FDx), Adv Duplex (FDx/TDx), Rk Pair (All), Polarity (Normal), and Optical (False).
- Switch:** Details switch information: Model (Cisco WS-C3750-48PS), IP/MAC (13.250.0.2), Port (GigabitEthernet1/0/19), VLAN (300), and Type (CDP).
- DHCP:** Lists IP (10.250.3.265) and Server (10.250.0.2).
- DNS:** Lists DNS 1 (10.250.3.221) and response times (25.7 ms, 1.1 ms, 1 ms).

Link-Live Cloud Service is a free, online system for collecting, tracking, organizing, analyzing, and reporting your test results, which 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 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 Link-Live apps, including Discovery, Wi-Fi Analysis, Path Analysis, Line Rate Performance Test, 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.

In Link-Live

1. The first time you sign in to Link-Live, a pop-up window appears, prompting you to claim a device.

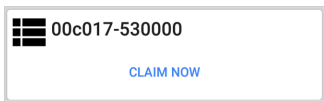
If you already have a user account and other devices claimed to Link-Live, navigate to the **Units** page from the left side navigation drawer, and click the **Claim Unit** button at the lower right corner of the screen.



2. Then, select the EtherScope nXG image, and follow the claiming instructions on the Link-Live website.

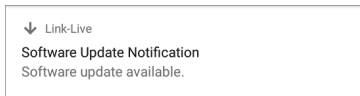
On the EtherScope nXG Unit

1. Open the Link-Live app. Your unit's MAC address is displayed.



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.





See [Updating Software](#) for more information.

Uploading Test Results

Once your EtherScope is claimed to the Link-Live Cloud, 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 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 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 .

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.

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**.



About



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: --

[UNCLAIM](#)

[EXPORT LOGS](#)

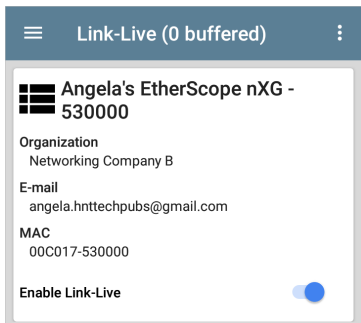
Copyright 2019

NetAlly

Using the Link-Live App



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 uploads as needed.

Link-Live App Screen Details



The "(# buffered)" in the Link-Live screen header indicates the number of test results stored in the device memory when no active network connection is available. These will

upload to Link-Live once your EtherScope is connected to an active network.

The EtherScope unit's name that displays in Link-Live is shown to the right of the Link-Live icon . You can change this name on the Link-Live 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 website. The fields displayed in EtherScope's Link-Live app are informational.

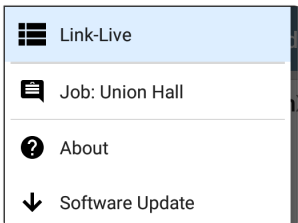
The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the EtherScope cannot upload test results or check for software updates. The **Upload to Link-Live** options will not appear in the other testing apps.

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.

To enter or change the Job Comment in the Link-Live app, follow these steps:

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](#).

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.

If your unit is not claimed to [Link-Live.com](https://link-live.com) or if Link-Live is disabled on the app screen, the

links and buttons for uploading to Link-Live in the testing apps 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.

**Link-Live**

by NetAlly

**Wi-Fi Snapshot Name**

20190429_122109

Comment



Conference Room B

Job Comment

North Office



SAVE TO ANALYSIS FILES

The Link-Live sharing screen for a screenshot or other image allows you to attach it to the most recent test result on the Results  page or just to the Uploaded Files  page on Link-Live.com.



Link-Live

by NetAlly



Comment

Conference Room B

Job Comment

North Office



SAVE TO LAST TEST RESULT



SAVE TO UPLOADED FILES

Remember, the regular **Comment** field uploads only to the current result or file, while the **Job Comment** field uploads with all results and files until you change it.




Cable Test App

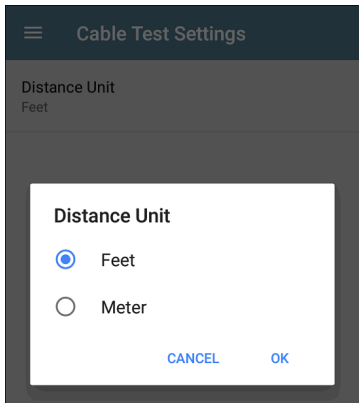
EtherScope nXG's Cable Test can help you determine cable length and fault status, verify wiremapping of patch and structured cabling, and locate cable connections using toning. The cable testing port is the RJ-45 port on the left side of the EtherScope unit. Connect a cable to this port for testing and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

Cable Test Settings

The settings for the Cable Test app are simply Distance Unit settings: Feet or Meters.

To change Cable Test settings, touch the menu  icon on the Cable Test app screen, and select **Cable Test Settings**.

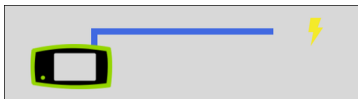
Tap the **Distance Unit** field, and select either **Feet** or **Meter** as needed, then touch **OK**.



Running Cable Test

Refer to EtherScope nXG's [Buttons and Ports](#) as needed.

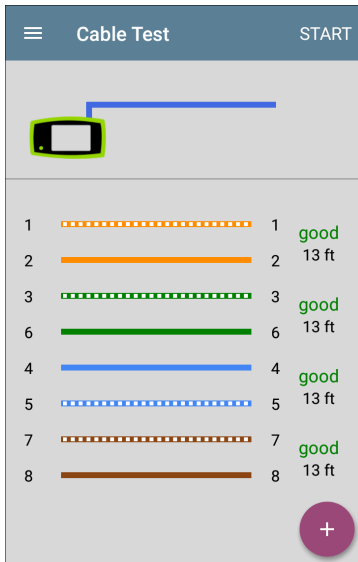
- With an [open or unterminated](#) cable connected to the RJ-45 cable test port (left side of the unit), you can measure length, identify shorts and splits, and locate opens.
- Using a cable terminated with a [WireView Cable ID accessory](#), you can measure cable length and identify shorts, opens, 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.



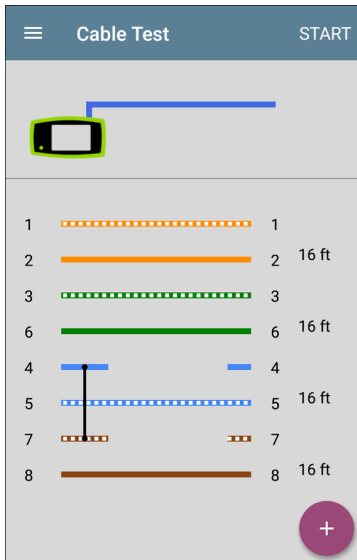
To start the cable test, tap **START** at the top right of the Cable Test app screen.

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.



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.



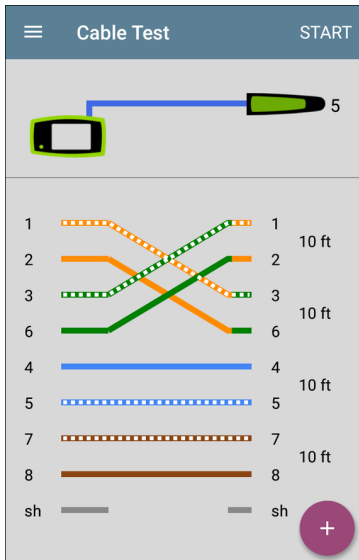
This unterminated cable test image shows a shorted cable between pins 4, 5, and 7.

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.

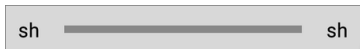
To run a terminated cable test, connect the left side RJ-45 port to a cable terminated with an external WireView Cable ID accessory.

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.

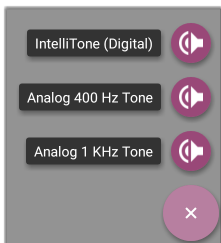
The last row of WireView results indicates whether the cable is shielded: an unbroken line between **sh** means a shielded cable is detected.



Using the Tone 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.

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, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)

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.



Conforms to relevant European Union directives.



Conforms to relevant Australian Safety and EMC standards.



Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.



Listed by the Canadian Standards Association.

Industry Canada Class A emission compliance

statement: This Class A digital apparatus complies with Canadian ICES-003. Avis de conformité à la réglementation d'Industrie Canada Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This device is not capable of transmitting in 5600-5650 MHz. This restriction is for the protection of Environment Canada's weather radars operating in this band.

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 ELEC-
tromagnetic 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, 7.2V 6.4 Ah

Wi-Fi: 2412 MHz-2472 MHz, 5180 MHz-5240 MHz, 5725 MHz - 5875 MHz

Bluetooth/BLE: 2402 MHz - 2480 MHz
