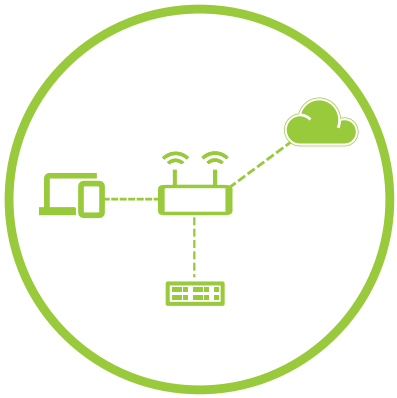
netAlly®



Link-Live™ Discovery Difference

Application Note

netAlly

The fastest, simplest, easiest way to generate network discovery snapshots.

Link-Live Discovery Difference

INTRODUCTION

Throughout the lifetime of a network many changes will happen. Sometimes you will have the need of installing more access points, maybe you will need to install new switches, or provision a PC for a new employee. But how often do you keep track and document those changes? Not knowing what devices are connected to your network and where they are located could make it a lot more difficult and time consuming to identify the root cause of network problems or possible security issues. It could also make it more difficult to upgrade an aging network.

More importantly, how about unauthorized changes made by someone else? Many times, employees will bring their own network devices to the office while attempting to work around production network safeguards. Other times, disgruntled personnel or hackers may try to gain access to your corporate data, or customer and employee information. Unauthorized or rogue devices on your network are a major security concern.

So, how can you keep track of network changes while at the same time detecting unauthorized devices connected to your network? The answer is simple! The Discovery Difference Analysis in the NetAlly Link-Live™ cloud service simplifies the process of documenting network changes or identifying unauthorized devices by comparing network discovery data collected by EtherScope® nXG or LinkRunner® 10G* (with AllyCare support) and automatically highlighting new or missing devices on your network.

In this application note we will start by explaining how to use these tools to generate network discovery snapshots, and then use Link-Live to generate a discovery difference analysis. Lastly, we will share with you how to identify new or missing network devices with either Discovery Analysis or Topology Mapping.

*In this document we will refer to discovery being conducted by the EtherScope nXG network analyzer. However, this process also applies to LinkRunner 10G units that have AllyCare support – an active support contract enables the discovery feature.

COLLECTING DISCOVERY DIFFERENCE DATA

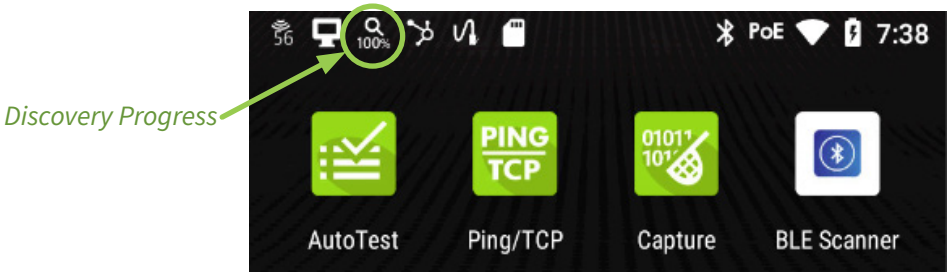
For Link-Live to be able to highlight what has changed over time in terms of new or missing devices you need to run two discovery tests at different times with your EtherScope nXG.

The initial discovery test will provide a baseline or snapshot of the original state of your network, and the second discovery test, conducted at a later time or date, will provide a snapshot of the current state of your network. Link-Live will compare the two snapshots and then highlight what has changed. That includes new devices that were not originally part of your network, and devices that were removed.

EtherScope® nXG
Portable Network Expert

Performing the Initial Discovery Test

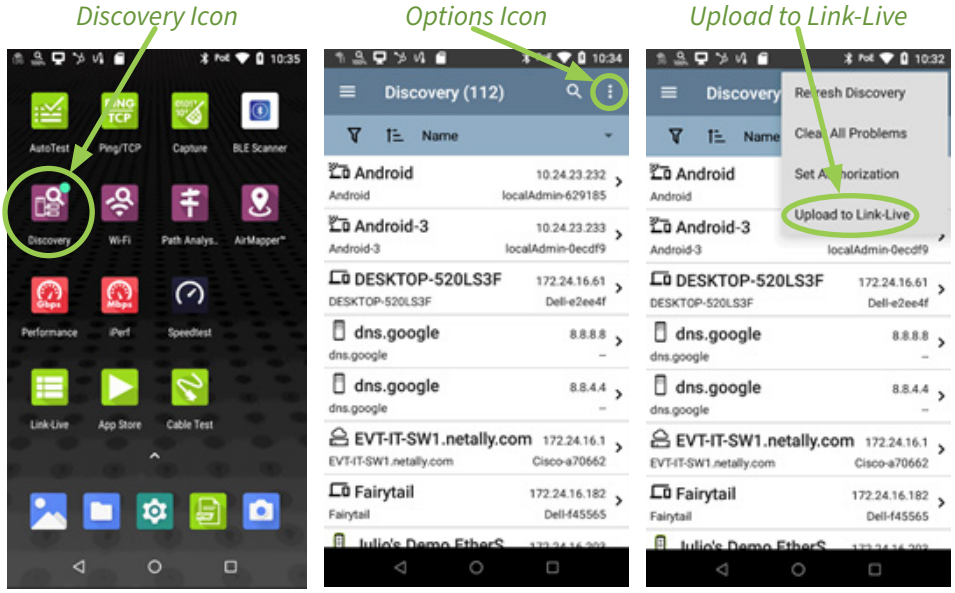
The EtherScope nXG will automatically perform a network discovery test upon connecting to a wired or wireless network and inform you of the progress it has made. You can see the progress made by the discovery test in the notification bar:



The EtherScope nXG can be configured with specific IP subnet ranges for discovery, or specified subnets can be excluded. It will discover all devices connected to the current subnet in addition to the subnets assigned. Please refer to the product user guide for information on configuring discovery settings.

Depending on the size of your network, the discovery process could take between a few seconds to a few minutes. After the discovery progress reaches 100% you are ready to upload the test results to Link-Live. To do that:

1) Select the “Discovery” icon on the EtherScope nXG home screen
2) Tap on the ellipsis (three dots) on the upper right of the screen
3) Select the “Upload to Link-Live” option



Performing the Second Discovery Test

When the second discovery test will be performed depends on your needs:

1) Network Security – You may want to run a discovery test on a regular basis to ensure no new unauthorized devices are connected to your network
2) Network Mapping – You may want to run a discovery test any time network changes are made. This will help you keep your network documentation up to date

To perform the second discovery test, follow the same process that was used while performing the first discovery test and upload your test results to Link-Live. (Be sure to use the same discovery settings as in the initial scan. Specific settings can be saved as a profile for later use – refer to the user manual.)

Link-Live
Complimentary Cloud
Service

ANALYZING DISCOVERY DIFFERENCE DATA

Now that both network discovery test results have been uploaded to Link-Live it is time to analyze the data. You have the option to analyze discovery difference data visually by using a “Topology” map, or you could look at device details through the “View Analysis” tabular data.

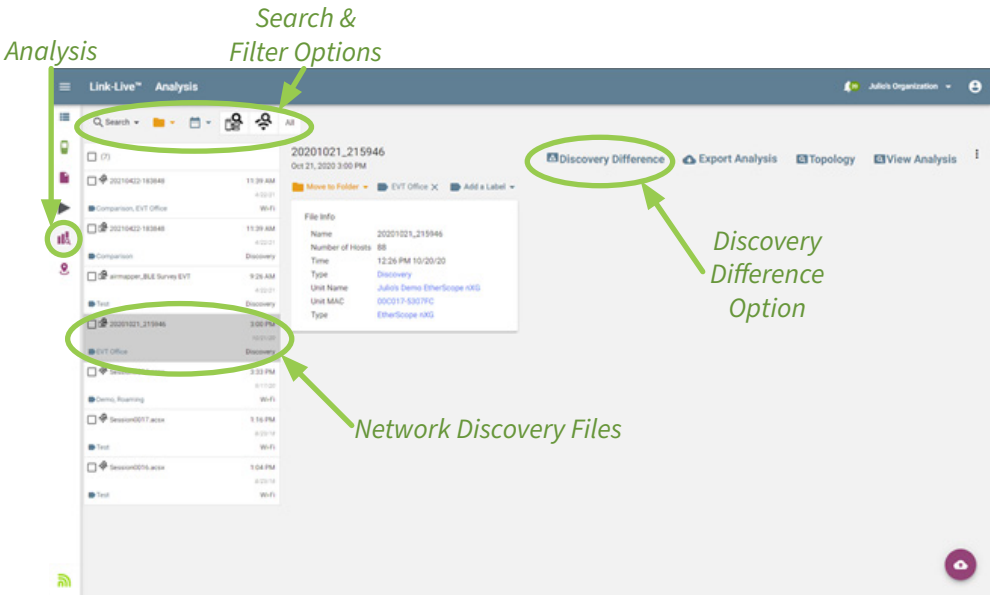
Combining Discovery Data

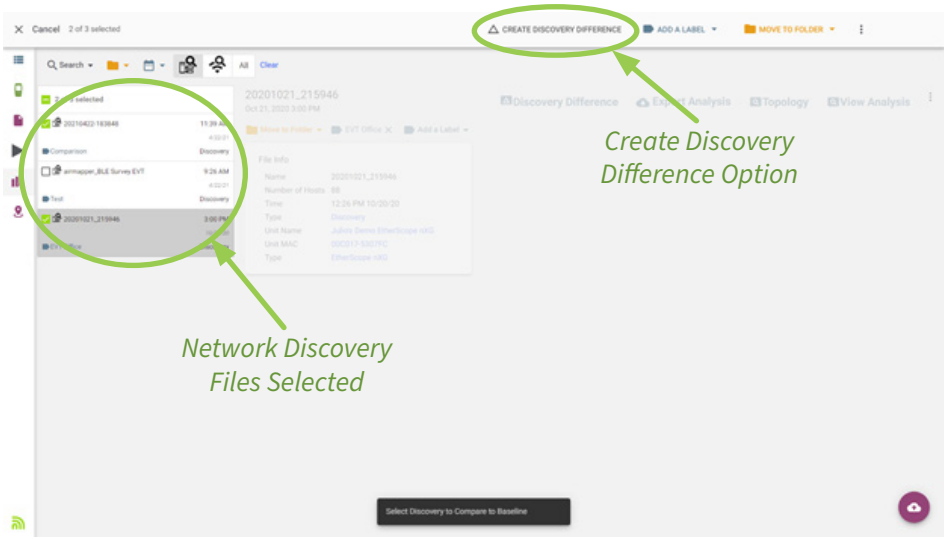
Before you can start your analysis, you will need to combine your two network discovery tests.

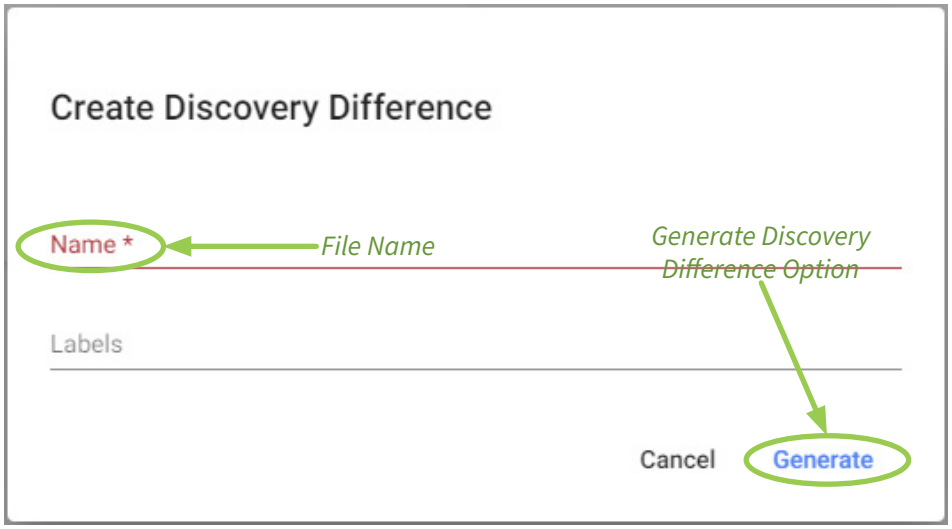
1) Start by going to link-live.com and login into your account
2) Select the “Analysis” option on the left side of the screen
3) On the left side of the Analysis screen, you will see a list of the analysis files that have been uploaded to Link-Live (this includes discovery, path analysis, and Wi-Fi analysis)
4) Use the “Search” and “Filter” tools on the upper left of the screen to find and select your baseline network discovery test (original state of your network)
5) The “Discovery Difference” option will now become available on the top of the screen. Select this option
6) Now select your second network discovery test (current state of your network)
7) The “Create Discovery Difference” option will now become available on the top of the screen. Select this option
8) When prompted, provide a name for the new “Discovery Difference” file. You can also provide labels at this time. When done, select the “Generate” option

The new discovery difference file will now show up on the list of “Network Discovery Tests”, and you will be able to use either the “Topology” or “View Analysis” options to review the data.

Note: The two network discovery test files that were used to generate the new discovery difference file will remain on the list and will continue to be available individually for further analysis







Using the Topology Map to Analyze Discovery Difference Data

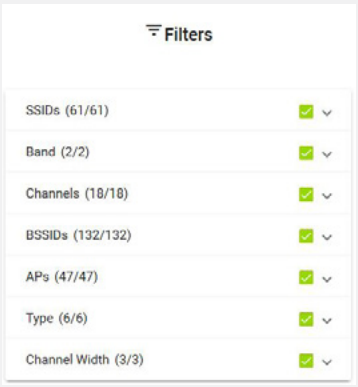
The topology map option provides a visual way to identify network changes, making it quick and simple to identify if new devices have been added to the network or if devices have been removed.

To start your analysis, select your network discovery difference file and then use the “Topology” option.

Note: To quickly find the discovery difference files, you can click on the icon to filter

A complete map of your network will be generated, and devices on your network will be color coded as follows:

- Black – No change, these devices were on your first network discovery test and were still present when the second network discovery test was performed
- Red – New devices, these devices were not part of your network when the first network discovery test was performed but were added to the network before the second discovery test was performed
- Orange – Missing devices, these devices were part of your network when the first network discovery test was performed but were removed before the second network discovery test was performed

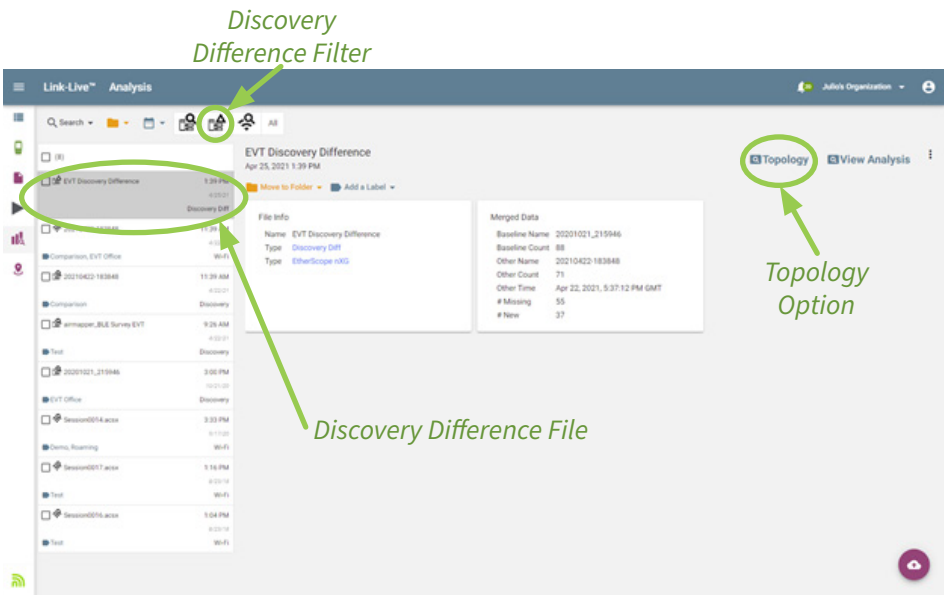


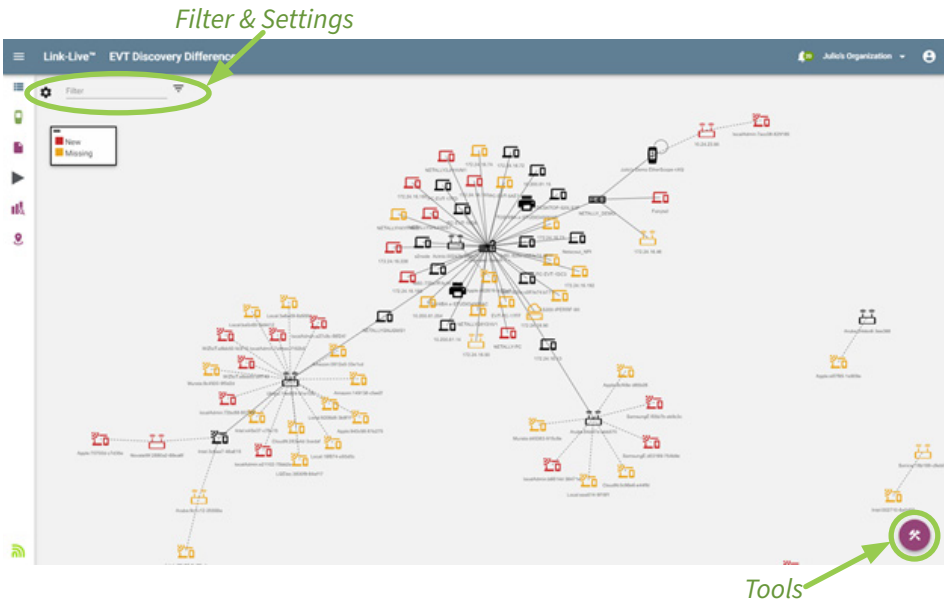
Multiple filters can be used to customize the visualization in Link-Live.

To find more information about new or missing devices on your network double click on the device.

Other analysis options available on the topology map include:

1) Filter - Allows you to focus on specific network devices or elements, including “Same”, “Missing”, and “New”
2) Settings – Used to change labels, data options, display options, and color options
3) Tools – Allows you to generate SVG files, report templates, and Visio reports





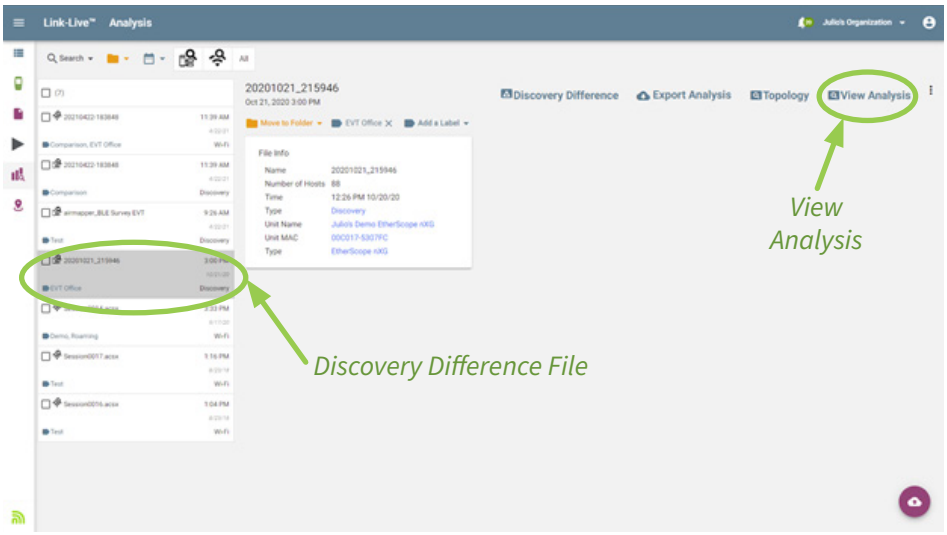
Using the View Analysis Tool to Analyze Discovery Difference Data

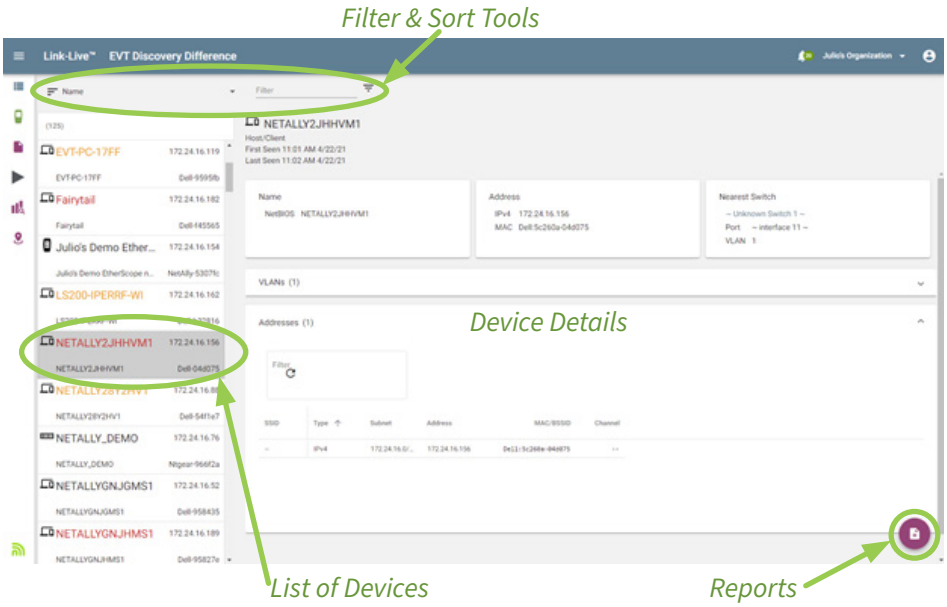
The “View Analysis” option provides a list of devices on your network and provides details about each device.

To start your analysis, select your network discovery difference file and then click the View Analysis option. A complete list of network devices will be generated, and devices on your network will be color coded.

To find more information about new or missing devices select the device of interest from the list on the left side of the screen. Details for the selected devices will show up on the right side of the screen. Other tools available on view analysis include:

1) Filter - Allows you to focus on specific network devices or elements
2) Sort – Used to sort the list of devices by name, type, IP address, MAC address, worst problem, or SSID
3) Reports – Allows you to generate CSV files, report templates, and PDF reports





CONCLUSION

In conclusion, it does not matter if you are trying to identify rogue devices, or to document network changes, or just feel confident that you know who and what is on your network (and where they are connected), NetAlly makes it fast and simple to find out what is connected to your network, and thus identify new or missing devices.

Just use your EtherScope nXG (or LinkRunner 10G with AllyCare support) to discover all the devices connected to your network and use Link-Live to automatically highlight network changes. No need to spend days manually documenting every device connected to your network. Network mapping, rogue detection, and change discovery has never been easier!