

Remote Network Management and Troubleshooting

Application Note

Table of Contents

Introduction	3
Interfaces	4
Test Ports	4
Management Ports	4
Interface AP Addresses.....	4
Management Ports	4
Remote Discovery	5
Remote Operation.....	6
Using a VNC Viewer on the Same Network	6
Remote Operation Using a VPN	6
Remote from Link-Live Cloud Service	8
Complete Flexibility for Any Environment	8
Remote Using Existing Conference Systems.....	9
Remote Analysis Using Link-Live	9
File Sharing.....	9
Wi-Fi and Discovery Snapshots	9
Packet Captures	9
Other Remote Use Models	10
Remotely Access On-Premise Devices.....	10
Monitor with Periodic AutoTest	10
Verify WAN and SD-WAN.....	11
Conclusion	11



Remote Network Management and Troubleshooting

Supporting remote sites has always been a challenge for network professionals. Lack of expertise at the remote offices frequently necessitates travel by senior IT personnel to troubleshoot problems. But in today's environment, that may not be an option.

With the inability to travel to your remote sites, or more recently even your local office, how do you get the visibility you need to solve tough problems? You can only get so far with infrastructure monitoring tools and VPN access. That's where NetAlly comes in. In this application note, we will cover how to gain "as if you were there" visibility, collaborate with on-site staff (whether they're technical or not), and solve problems fast using the EtherScope nXG Portable Network Expert and the Link-Live Cloud Service.

INTRODUCTION

The EtherScope™ nXG Portable Network Expert is a multi-technology, all-in-one, handheld network analyzer that enables engineers and technicians to deploy, troubleshoot, and document their Wi-Fi and Ethernet networks. Front-line personnel and network engineers use this portable tool, in hand, to test the local network where end users connect. EtherScope's intuitive user interface, light weight, and long battery life make it a potent on-location network analyzer. A robust set of NetAlly applications support measurement, discovery, analysis, and documentation of the network:

- AutoTest – Verify your network layers 1 through 7 in seconds.
- Ping/TCP – Validate and monitor responsiveness and connectivity.
- Capture – Record Wired or Wi-Fi frames with filters.
- Discovery – Identify and analyze all devices on your network.
- Wi-Fi – Identify APs, SSIDs, clients, and channels from your location.
- Path Analysis – Trace Layer 2 and 3 routes.
- Performance – Measure up to four packet streams at 10G line rate.
- iPerf – Test Wired or Wi-Fi connections to a NetAlly Test Accessory or server.
- Cable Test – Determine cable length and status with TDR, reveal wiremapping, and employ toning.
- Link-Live – Upload, manage, and analyze results and data in the Cloud.
- App Store – Download and install curated third-party Android applications.



In the April 2020 v1.2 update, EtherScope will add the new AirMapper™ app, which lets users perform Wi-Fi site surveys and generates heatmaps in Link-Live.

To extend the EtherScope's capabilities even further, it offers multiple methods for remote access and operation. However, to optimize the remote capabilities of the EtherScope, we need to understand its network interfaces and discovery process.

INTERFACES

Despite its small package, the EtherScope is equipped with four (4) primary network interfaces. These provide great flexibility for remote test deployment and operation:

Test Ports

There are two test ports on the EtherScope: Wired and Wi-Fi.

1. Wired Test Port

The Wired Test Port consists of both an RJ-45 and an SFP+ for connecting to the primary Network Under Test (NUT).

- The RJ-45 covers six NBASE-T speeds: 10M, 100M, 1G, 2.5G, 5G, and 10GBASE-T.
 - The SFP+ supports a variety of SFP modules, including 1G and 10GBASE-X for fiber and 10G DAC/AOC cable assemblies.
- Both RJ-45 and SFP+ are capable of capture and performance testing at line rates up to 10 Gbps. The RJ-45 port also contains proprietary Power-over-Ethernet circuitry to load PoE with TruPower™ up to 90 W.

2. Wi-Fi Test Radio

The Wi-Fi Test Radio is an instrument-grade radio that serves four functions:

- Promiscuous channel scanning for AP and Client traffic to map the relationship between SSIDs, APs, and their BSSIDs, Clients, and Channels
- Connectivity testing using AutoTest, including roaming analysis and key services verification
- Capture, including filters for frame types, BSSID/MAC, and channels
- External antenna connection for a directional antenna used for rogue hunting

Management Ports

In addition to the Wired and Wi-Fi Test interfaces, the EtherScope provides built-in management ports. The Management Ports allow you to remotely operate the unit without interfering with the Network-Under-Test (NUT) Ports, as the test interfaces may disconnect, reconnect, and resume scanning. When multiple connections exist, the EtherScope will always favor a management port over a test port for remote operation.



EtherScope™ nXG
EtherScope features four network interfaces.

Multiple connections provide test and unit management flexibility.

3. Wired Management Port

The RJ-45 10/100/1GBase-T port provides three major functions:

- Permanent, uninterrupted remote management using wired connectivity
- Discovery of an additional network, such as a production/test or student/teacher environment
- Cable tests, including TDR, for length/status, wiremap, and toning

4. Wi-Fi + Bluetooth Management Radio

This radio provides three functions:

- Permanent, uninterrupted remote management using Wi-Fi connectivity
- Discovery of the connected SSID to provide layer 3 identification of Wi-Fi devices seen in the air
- Bluetooth for paring to peripherals, such as a keyboard, headset, or even a label printer

The Wi-Fi Management Radio is controlled by the Android™ operating system and, therefore, can automatically connect to any saved networks.

The Management Ports allow the EtherScope to scan all the channels for over-the-air analysis using the Wi-Fi Test radio while simultaneously discovering the same devices from an IP layer perspective. Layer 3 identification includes IP addresses and device names from a variety of sources, such as NetBIOS, mDNS, and SNMP. With layer 3 access, EtherScope automatically associates IP addresses and device names with the MAC addresses seen in the air.

Interface IP Addresses




These four interfaces are the basis for a variety of flexible remote deployment scenarios. At the extreme, EtherScope can be connected to and troubleshooting four separate networks. The IP addresses of all the linked interfaces are available from the top pull-down notifications.

The most common deployment is to use the Management Port connections for remote operation, leaving the Test Ports for troubleshooting and characterization.

REMOTE DISCOVERY

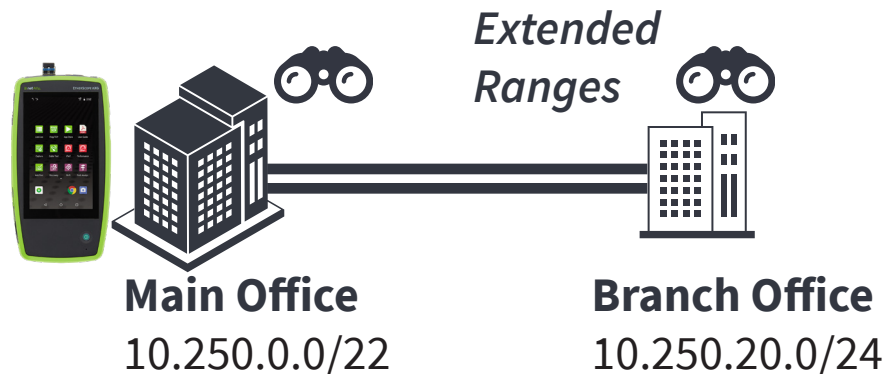
Discovery finds and classifies the networks on all connected network interfaces, including Ethernet, fiber, and Wi-Fi. Discovery provides three main functions:

- Device discovery to inventory, name, and identify all network elements, which you can then search, filter, and sort. Devices are named using SNMP, DNS, mDNS, and NetBIOS protocols.
- Infrastructure management by monitoring switches and router interfaces for utilization, errors, discards, and a variety of issues like recent reboots.

 EtherScope nXG ^
Wired Port
Speed: 1 G FDx
IP Address: 192.168.0.16
 EtherScope nXG ^
Wi-Fi linked on channel 36
SSID: CenturyLink5134_5G
IP Address: 192.168.0.10
 EtherScope ^
Multiple Management Port Connections
Wi-Fi Management Port
IP Address: 192.168.0.9
SSID: CenturyLink5134_5G
Channel: 36
Wired Management Port
IP Address: 192.168.0.28

- Topology Analysis by harvesting switch forwarding tables to augment layer 3 trace routes with layer 2 switch interconnectivity and determine where devices are connected to the network.

The EtherScope automatically performs active discovery on the IP subnets of any connected networks, be they wired or Wi-Fi. EtherScope also enables you to enter an unlimited number of Extended Ranges for off-net sites, meaning networks that are not in the subnets of any active EtherScope ports. These Extended Ranges add any routable remote/branch office to the layer 2 and 3 discovery process.



Extended ranges do not provide remote layer 1 diagnostics, such as PoE or Wi-Fi SNR. At some point, measurements must be taken at the remote site—from the point of view of the affected end user.

REMOTE OPERATION

Remote operation provides a way to control the EtherScope from any location. There are two primary use models:

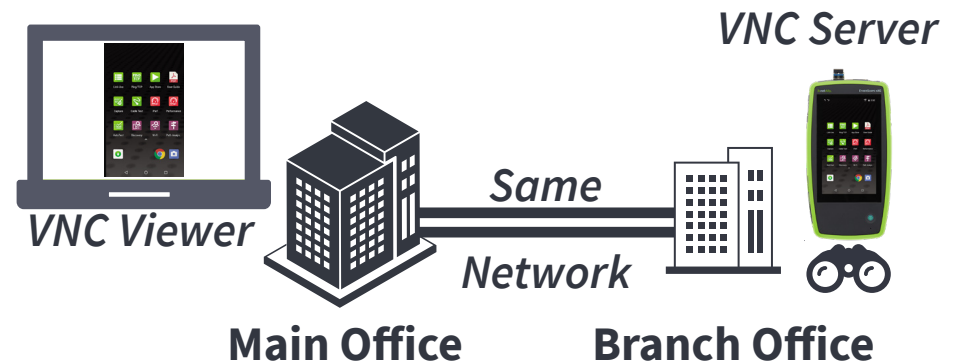
1. Unattended: The engineer operates an EtherScope entirely remotely. The unit could be in an equipment closet, data center, or in the proximity of a Wi-Fi problem.
2. Interactive: Since the local and remote interfaces can operate together, a variety of remote collaboration, teaching and learning opportunities are available: An on-premises technician can watch the remote engineer operate the unit, or the technician can show the engineer what they are doing.

Because the EtherScope is equipped with both a Wired and a Wi-Fi Management Port, users can remotely operate it without impacting the Network Under Test. Connecting the Wi-Fi Management Port allows the unit to be carried around, untethered by a person on site while also being operated remotely by an expert.

There are three ways to perform remote operation: using a VNC viewer, the Link-Live Cloud Service Remote function, and with a screen-sharing conference system utilizing a third-party app.

Using a VNC Viewer on the Same Network

VNC can be used when both the user and the EtherScope are connected to the same network. VNC is platform-independent and requires a server and a client. The VNC Server is on the EtherScope. The VNC Viewer can be a VNC Client, such as TightVNC or RealVNC, using port 5900 by default.



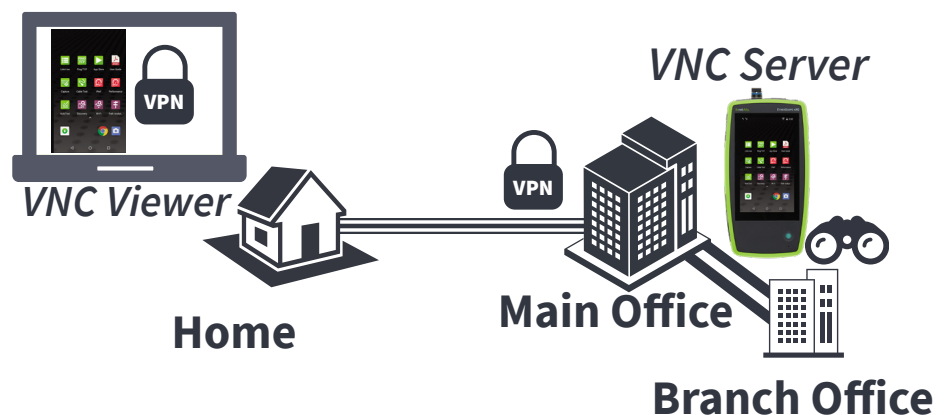
If a VNC client is not available, the EtherScope also supports VNC Web Browser remote operation. Simply point your browser at one of the EtherScope IP addresses and port 5800 to connect.

  192.168.0.9:5800

VNC operation is encrypted and, optionally, you can set a VNC password on the EtherScope.

Remote Operation Using a VPN

When you do not have a directly routable connection to the EtherScope, you can access VNC through a VPN. An external user can create a VPN tunnel, through which VPN traffic can flow, with the corporate VPN client on their PC, and then, access their unit with either a VNC client or a web browser. The EtherScope has complete Wired and Wi-Fi visibility in the connected location.



EtherScope Setting

Link-Live Remote
Enabled

Link-Live Button



Remote from Link-Live Cloud Service

The easiest method for controlling your unrouteable EtherScope is the Cloud Remote function available on Link-Live.com. From Link-Live, the user can control the EtherScope through up to two layers of Network Address Translation (NAT) and Firewalls. If the user's PC and the remote EtherScope both have internet connectivity, they can be connected and proxied through Link-Live using HTTPS and TLS1.2.

When the Link-Live Remote setting is enabled in the EtherScope's General Settings (within the testing apps), the user will see a corresponding REMOTE button on the Units page at Link-Live.com.

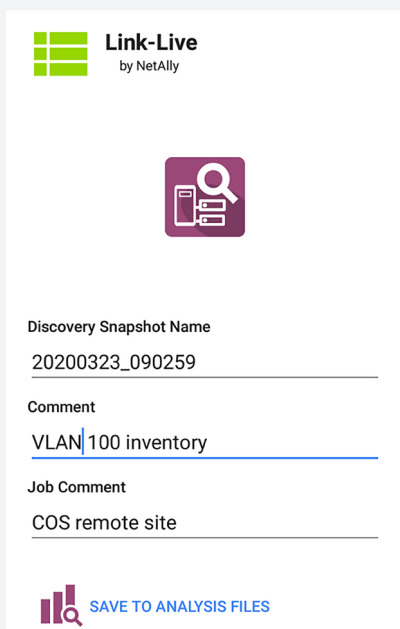
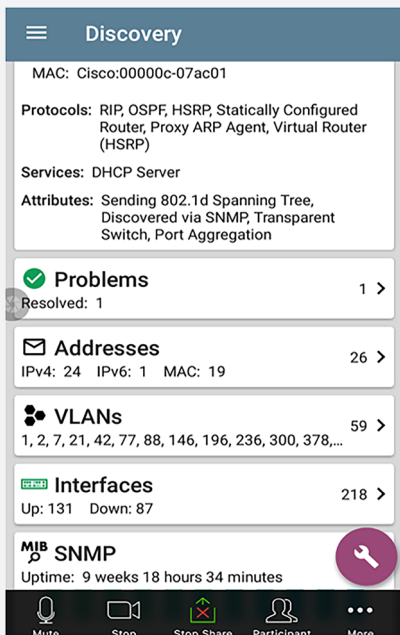
Unlike VNC, the user does not need to know the EtherScope's IP addresses and can simply select REMOTE in Link-Live. A pop-up window displays the EtherScope screen.



Complete Flexibility for any Environment

With four separate interfaces capable of supporting remote operation, and the choice of VNC or Link-Live connectivity, the EtherScope can be deployed in almost any remote environment. For example, users can remotely diagnose a problematic Work-from-Home network without impacting the home internet being tested. In this case, the Wi-Fi Management Port could be connected to a mobile hotspot, such as on a phone, essentially backhauling the remote user interface over the cellular network rather than the network under test.





Remote Using Existing Conferencing Systems

If a corporate conferencing system is in place, the associated Android app can run directly on the EtherScope. This method lets the EtherScope share its screen with a remote user. There is no front facing camera, but audio is supported with the EtherScope's speaker and microphone.

In addition to screen sharing, conferencing systems often include calling and chat as services.

REMOTE ANALYSIS USING LINK-LIVE

In the previous sections, we discussed the flexibility of the four primary interfaces, remote discovery, and operating the EtherScope user interface remotely using VNC or Link-Live.

Some test results, especially AutoTest's, are automatically uploaded to Link-Live to create a test history for troubleshooting, baselining, and reporting. Link-Live also provides a repository for other EtherScope files and results, including images, text files, and analyses, such as Discovery and Wi-Fi Analysis Files.

File Sharing

Any file on the EtherScope can be shared (uploaded) to the Link-Live Uploaded Files page, including screenshots and pictures from the embedded camera or connection logs.

Wi-Fi and Discovery Snapshots

Even if remote operation isn't possible, the EtherScope is so easy to use, it can be shipped to a location, plugged in, and operated. Snapshots of the autonomous Discovery and Wi-Fi Analysis can be sent to Link-Live in a few taps.

Packet Captures

Remotely debug especially difficult problems with the Capture app. In seconds, get a wired or Wi-Fi packet capture from the remote EtherScope into your protocol analyzer. Wi-Fi Capture includes the ability to filter on the channel, BSSID/MAC, and management/control/data frame types and includes the Radiotap header information. Wired capture runs at line rate, saving to a dedicated 1-GB capture memory, and includes the ability to filter by address, VLAN, port, and more.

Link-Live™ Wi-Fi 20200129_103726: APs (39)										
	Name	Mfg Prefix	Signal	Worst Problem	Type	Securities	SSIDs	BSSIDs	Channels	Client
	CiscoM:683a1e-2e80d0	CiscoM	-58 dBm		8x, ac, n, g, a	WPA2-P	2	4	2	6
	CiscoM:683a1e-2e80da	CiscoM	-63 dBm		8x, n, g	WPA2-P	2	4	2	0
	CiscoM:e0c8bc-33c2e8	CiscoM	-61 dBm		n, g, b	WPA2-P	1	1	1	0
	CiscoM:e0c8bc-33c291	CiscoM	-57 dBm		ac, n, g, b, a	WPA2-P	1	2	2	0
	CiscoM:e0c8bc-33de86	CiscoM	-59 dBm		ac, n, g, b, a	WPA2-P	1	2	2	0
	Fairis:0-7302c4a8808	Fairis			n, n, b	WPA2-P	1	1	1	0

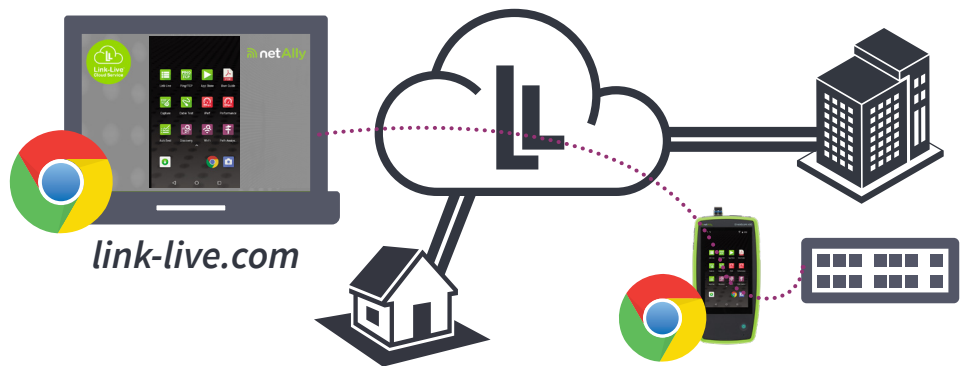
Off-line Wi-Fi Analysis in Link-Live

OTHER REMOTE USE MODELS

Here are a few more examples of the unlimited ways to use your EtherScope in remote environments:

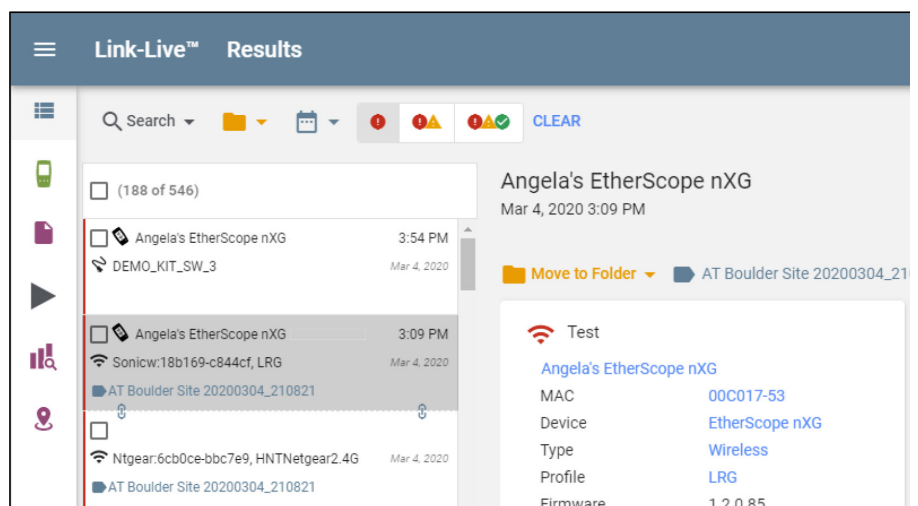
Remotely Access On-Premise Devices

When used remotely, the EtherScope can also operate as a proxy between the remote PC and Network under Test. For example, you can access a remote web portal, such as a switch management portal, using the on-EtherScope Web Browser. Likewise, Telnet, SSH, Mosh, and even USB-Serial Console operations are possible on the EtherScope.



Monitor with Periodic AutoTest

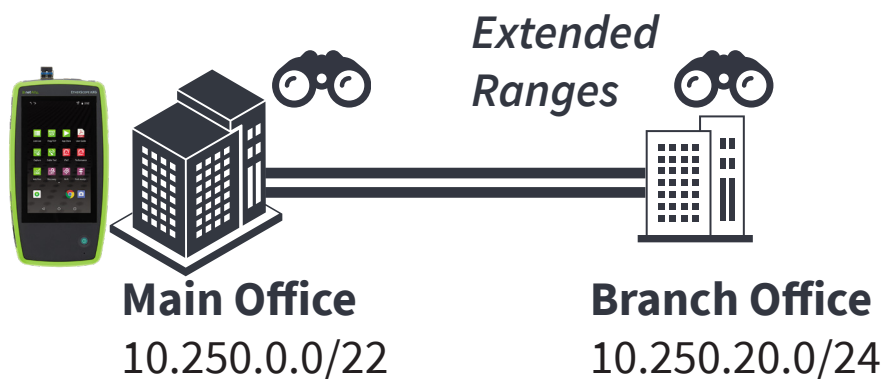
Often, remote network issues are intermittent. The EtherScope can actively monitor a network for up to twenty-four hours by running Periodic AutoTests as frequently as once a minute. An AutoTest can consist of a simple PoE or Wi-Fi connectivity test or go all the way to verifying connectivity and performance of all your business services, whether on-prem, hybrid, or in the cloud. On Link-Live.com, you can view and filter Periodic AutoTest results on the Results page in Link-Live and perform detailed Pass, Fail, and Warning triage and reporting.



Since the EtherScope measures every packet, it is also possible to characterize actual failover performance.

Verify WAN and SD-WAN

Remote sites are dependent on their WAN connections and Service Level Agreements. Whether deploying a single point-to-point connection or an SD-WAN with traffic shaping, the EtherScope's hardware accelerated Line Rate Performance Test allows you to verify and characterize your WAN(s) in terms of throughput, loss, latency, and jitter, at up to 10 Gbps. The Performance test exchanges a stream of traffic with other EtherScope Peers or various Reflectors. You can simulate real-world traffic by configuring up to four streams with traffic flow, frame size, VLAN, and layer 2 and 3 QoS options. The streams can target the same device for QoS traffic shaping validation of point-to-point connections or target multiple endpoints for point-to-multipoint testing. The tests can run at a full line rate for performance or SLA validation, run at lower speeds to minimize disruption when troubleshooting operational networks, or generate deterministic background traffic for scenario testing. Since the EtherScope measures every packet, it is also possible to characterize actual failover performance.



CONCLUSION

The EtherScope can be used in a variety of remote situations from branch office troubleshooting to analyzing the enterprise network from home. With its arsenal of test capabilities, four flexible interfaces, multiple screen sharing technologies, and Link-Live analyses, the EtherScope can save you time, travel, and expense when managing your networks.

RELEVANT PRODUCTS

EtherScope™ nXG

<https://www.netally.com/products/etherscopenxg/>