Introducing LXI to a Network Administrator

by Conrad Proft – Proft InFocus, LLC

Introduction

This article is written to give network administrators a summary of key elements necessary to understand connecting LXI Devices to their corporate LAN.

When purchasing LAN equipment, you expect it to work reliably, consistently, and according to LAN standards. You will filter out those devices that do not work properly and settle on key components that meet your needs. Without adherence to standardized LAN protocols, an errant device can be a nightmare to configure, use, and support.

LXI Devices adhere to a number of LAN standards, but they go further. Every LXI Device must pass rigorous, third-party testing to be called LXI conformant. LXI means all conformant devices will connect to and communicate on a LAN in a known and predictable manner. It also means they have web pages for describing communication and configuration that are common between LXI Devices.

A majority of the measurement instrument manufacturers established the LXI Standard in 2005 to bring about this common behavior for LAN-based instruments. It was a huge step in compatibility such that a test engineer that builds a test system with LXI conformant devices can rely upon that LXI common behavior. As a network administrator, you can rely upon the LXI Devices to behave properly on the network in much the same way as a computer.

Even with this standardization, users still struggle with setting up and configuring a system properly using LXI Devices, because many users do not have a good understanding of LAN and proper configuration. Users also struggle working with corporate IT departments and network administrators to get LXI Devices used in the corporate environment and on the corporate network.

Corporate IT departments and network administrators have guidelines that must be followed to ensure the security and performance of the corporate network. Prior to the LXI Standard, LAN-based instruments varied widely in implementation of LAN protocols and services and often resulted in errant and unpredictable behavior when connected to the LAN.

The LXI Consortium recognized the need to better educate LXI Device users and network administrators, and created a special committee in December 2012 to develop tools and documents specifically to meet this need. The following will become available on the LXI website this spring:

- LXI Discovery Tool
- LXI Getting Started Guide
- Building LXI-based Test Systems
- Introducing LXI to your Network administrator

Key Elements in Understanding LXI Devices

There are a handful of topics that will help you to better understand the behavior of an LXI Device on the LAN. Once you see the typical use case configurations and behavior, you can then understand how best

to supply recommendations on LAN equipment to tie instruments together into a successful test system that meets the user's needs and maintains LAN integrity:

- Types of LXI Devices and their use model
- LXI required ports, protocols, and services
- Recommended LXI test system configurations
- Power-ON behavior
- Security protection

Let's take a summary look at each of these areas. When the LXI Consortium completes the aforementioned documents, you can obtain much more detailed information.

Types of LXI Devices and their Use Model

As of Jan 2013, there are approximately 1923 LXI conformant devices. Just about every measurement instrument type you can imagine has an LXI conformant offering: Power Supplies, Digital Multimeters, Digitizers, Capacitance Meters, Oscilloscopes, Spectrum Analyzers, Switches, Network Analyzers, Logic Analyzers, Signal Sources, LCR Meters, Counters, Power Meters, Sound and Vibration Analyzers, Solar Array Simulators, and many more, from over 35 vendors.

When integrated into a test system, there may be 5 to 8 such LXI Devices. Having so many devices mounted in a test rack and all interconnected with LAN cables to a single Switch or Router is simple to build and is a very reliable and economical solution.

Most test systems involve a sequence of programming steps for connecting test signals through an analog switch between a signal source, the Device Under Test (DUT), and the measurement instruments. It is typically a sequential programming model where the computer configures the instruments for each test using short bursts of commands and data. Do this…now do that…with hundreds of tests being performed that may last for hours.

Some LXI Devices require large amounts of data to be transferred from the computer to set up a signal which is applied to a DUT, and still other devices make 1000's of high speed measurements that must be transferred back to the computer as quickly as possible.

Most LXI devices have 100Mbit Full Duplex interfaces, but many have Gigabit interfaces. However, the majority of instruments interact in short bursts of ASCII or binary characters representing setup and data. Very few have a need for continuous transfer of large amounts of information. A Digitizer is an example of one that can transfer large amounts of data…possibly millions of readings per second, with each reading in a 2 to 8 byte format.

LXI Devices have varied operating systems just like printers, but some have Windows and Linux which require updates, virus, and worm protection. More will be said on that in the section on ***Security***.

Test Systems built with LXI Devices

Users of LXI Devices will typically operate in one of two configurations: Open System and Isolated System. The Open System is illustrated in Figure 1. For the Open System, developers of test programs desire access to the test system from their office computers. They want to be able to monitor what is happening and start or stop the test system at will. The Open System can be as simple as a User with a single instrument in his cubicle, with his computer and instrument connected to a Switch and the Switch connected to the LAN network. The computers and instruments obtain IP addresses from the company DHCP Server on the LAN network.

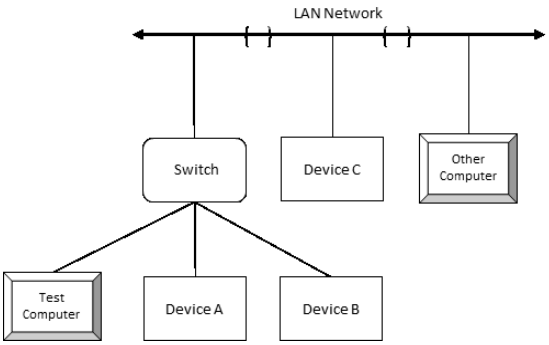

Figure 1. Open System

The Open System configuration works quite well for many companies, but instruments accessible to anyone on the network can be interrupted in the task they were asked to perform. And, Users can experience difficulty with their test programs not working properly when reconfiguration of the DHCP Server causes IP addresses to change.

To avoid interruptions in test system operation, the test computer and instruments can be isolated from the other Users on the network. Figures 2 and 3 illustrate two such configurations. Figure 2 places all devices, including the test computer, behind a Router, with the Router connected to the LAN network. The computer and the instruments obtain their IP addresses from the Router, and those IP addresses will not change. The test computer still has access to the LAN network through the Gateway of the Router.

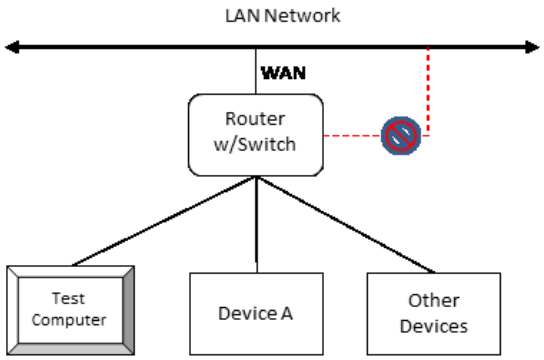

Figure 2. Isolated System with Router

This configuration has some potential issues for security that we will talk about shortly, since the test computer is now isolated from the network security software that wants to push OS updates, virus protection, backups, etc. Figure 3 offers a modification of this configuration by installing a second network interface in the test computer. Now, the test computer is fully visible to the network security software, and the instruments are all isolated on the second network interface. This configuration is a bit easier for test system developers, since they can remote login into the test computer.

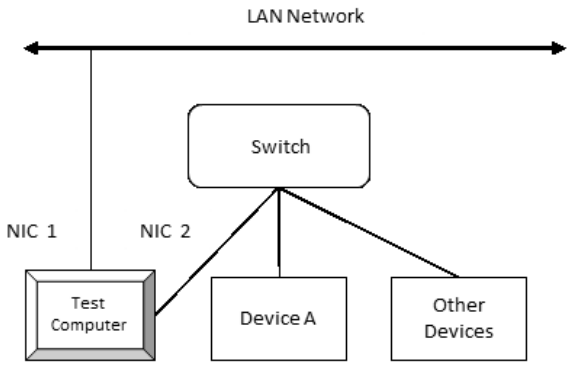

Figure 3. Isolated System with two NICs

As a network administrator, your job is to help the test system Users achieve their goals and still maintain the integrity of the network. Figures 2 and 3 have particular need for your recommendations on equipment and configuration of the test system computer. For example, you may have a Router that can be configured to permit you to "see" the test computer and other devices on the isolated subnet using port forwarding or a DMZ. And, you are likely the only one who could properly configure the test computer with a bridge between the two network interfaces in order to make the instruments still visible to the network security software.

Protocols, Ports, and Services

All LXI Devices must provide a base level of functionality to be LXI conformant, but some devices have Extended LXI features such as IPv6, IEEE-1588 time protocol, LAN messaging, and HiSLIP (High Speed LAN Instrument Protocol). An example of these protocols is illustrated in Figure 4.

Ports	Service	Description
21 tcp	FTP	Instrument web server - FTP port
80 tcp (HTTP)	Web server	Instrument web server (LXI)
111 tcp, 111 udp	Portmapper	Portmapper service for VXI-11 / LXI
161 udp 162 udp 705 tcp (AgentX)	SNMP	Standard ports for SNMP agent
319 tcp udp 320 tcp udp	1588 PTP	LXI Extended Feature – Precision Time Synchronization
2525 tcp	RSIB	R&S SCPI socket connection
4880 tcp	HiSLIP	High Speed LAN Interface Protocol
5025 (data) 5125 (abort)	TCP Socket	'Raw SCPI' socket connection
5044 tcp udp	LXI Message	LXI LAN messages and events Multicast address udp: 224.0.23.159
5800 tcp 5900 tcp	VNC	Instrument soft front panel via web server (Browser interface)
13217 tcp udp	RS Installer	R&S Software distributor service
14142 - 16383 tcp udp (dynamic assignment)	ONC-RPC	Sun ONC-RPC protocol – VXI-11

Figure 4. Example of Ports, Protocols, and Services of LXI Device

Power-ON Behavior

LXI Devices can be configured for Auto or Manual IP operation. The LXI standard requires that they are shipped with DHCP enabled, so that the User can quickly connect and use their instrument just as they would in connecting their laptop or computer. With the Auto mode, if a DHCP Serve is not found, the LXI Device does just what a laptop would do – it falls into Auto IP mode, where is assigns itself an IP address in the 169.254.*.* range and verifies that choice on the local subnet.

So how do you know what IP address the instrument has settled on? Instrument manufactures such as Agilent, National Instruments, Tektronix, and others have created VISA Libraries for communicating with instruments. These libraries typically include a discovery tool for finding LXI conformant devices. The LXI Consortium is also developing a simpler tool – the LXI Discovery Tool – which will become available this spring.

In addition to using the discovery tool, most LXI Devices have a front panel display which can *display* the LAN connection and IP address. Once you have the IP address or Hostname, you can access the home page of the instrument and determine its LAN full configuration.

Some LXI Devices don't have a front panel to view IP information. The discovery tools can still find the instrument, as long as it has a valid subnet mask and IP address. What if you are borrowing an LXI Device from someone, and it is configured for some obscure IP address and subnet mask? How will you discover its IP address? The LXI standard requires an LXI Reset softkey or hard key to be present on every LXI Device. Press that button, and the instrument reconfigures to the Auto mode and clears any password associated with configuring its LAN pages.

Security Issues

As mentioned earlier, LXI Devices are as varied in operating system implementation as printers. Most LXI Devices are not affected by virus issues due to their operating system and the fact that power-cycling the instrument will clean up any potential hazard issue they might have acquired. However, some use WinCE, Windows XP, Windows 7, Linux and other operating systems that are more readily susceptible to virus and worm attacks.

The instruments that are most vulnerable are typically very expensive Network Analyzers, Scopes, Spectrum Analyzers, and Signal Generator which literally use a full-blown computer under the hood for the best implementation solution. Makers of these instruments take great care in ensuring these instruments are not exposed to security risks during the manufacturing and test phases. When they are shipped to customers, firewalls are enabled and procedures are provided for users to install the virus protection of their choice on the instruments using detachable external storage devices, keyboards and mice. They also have recommendations for how and when such instruments should be updated with virus protection and operating system patches. It is clearly not a good idea for an instrument to auto-update or to have updates pushed to it during a test system procedure. These are typically scheduled once a week at a time when the test system is idle.

The good news is the computers within these instruments are not typically used to browse the internet nor are they used for email – two of the greatest security risks. However, they often have ports for USB sticks which are another prime method of propagating viruses. These instruments are configured to not auto-play any inserted USB stick. Rather, the virus protection software is permitted first access to the files on the USB stick.

Conclusion

All LXI Devices adhere to LAN standards and have predictable behavior. In fact, they are required to operate very much like a computer when connected to LAN. Like computers, some have security issues which much be addressed, but those risks need to be addressed carefully when the instrument is not in a test procedure. Test systems involving LXI Devices are typically configured using an Open system or Isolated system configuration, whichever best suits the needs of the test engineers. Your expertise is needed to make recommendations for the test system computer configurations, the Routers, and Switches used to tie the LXI Devices together.

Further reading can be found at the LXI Web site: www.lxistandard.org under Resources and the IT Topics tab:

Papers

Malware Protection White Paper
by Jochen Wolle, R&S (1.1 MB)

Guide to Configuring an LXI Instrument
by LXI Consortium (1.54 MB)

Introducing LXI to your IT Department
by Simon Appleby, Pickering Interfaces (1.9 MB)

Articles

Coordinate With IT for a Smooth LXI Rollout

LXI Can Ease Woes of Road-Weary Engineers

LXI helps engineers across the globe...literally!