LXI Extended Function IPv6

Revision 1.1

8 November 2016

Notice of Rights. All rights reserved. This document is the property of the LXI Consortium. It may be reproduced, unaltered, in whole or in part, provided the LXI copyright notice is retained on every document page.

Notice of Liability. The information contained in this document is subject to change without notice. "Preliminary" releases are for specification development and proof-of-concept testing and may not reflect the final "Released" specification.

The LXI Consortium, Inc. makes no warranty of any kind with regard to this material, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The LXI Consortium, Inc. shall not be liable for errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

LXI Standards. Documents are developed within the LXI Consortium and LXI Technical Working Groups sponsored by the LXI Consortium Board of Directors. The LXI Consortium develops its standards through a consensus development process modeled after the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Consortium and serve without compensation. While the LXI Consortium administers the process and establishes rules to promote fairness in the consensus development process, the LXI Consortium does not exhaustively evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an LXI Consortium Standard is wholly voluntary. The LXI Consortium and its members disclaim liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other LXI Consortium Standard document.

The LXI Consortium does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. LXI Consortium Standards documents are supplied "as is". The existence of an LXI Consortium Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the LXI Consortium Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every LXI Consortium Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any LXI Consortium Standard.

In publishing and making this document available, the LXI Consortium is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the LXI Consortium undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other LXI Consortium Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

This specification is the property of the LXI Consortium, a Delaware 501c3 corporation, for the use of its members.

Interpretations. Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of LXI Consortium, the Consortium will initiate action to prepare appropriate responses. Since LXI Consortium Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, LXI Consortium and the members of its working groups are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. Requests for interpretations of this

standard must be sent to interpretations@lxistandard.org using the form "*Request for Interpretation of an LXI Standard Document*". This document plus a list of interpretations to this standard are found on the LXI Consortium's Web site: http://www.lxistandard.org

LXI is a registered trademark of the LXI Consortium

Legal Issues, Trademarks, Patents, and Licensing Policies. These items are addressed specifically in the document "LXI *Consortium Trademark, Patent, and Licensing Policies*" found on the LXI Consortium's Web site: http://www.lxistandard.org .

Conformance. The LXI Consortium draws attention to the document "*LXI Consortium Policy for Certifying Conformance to LXI Consortium Standards*" found on the LXI Consortium's Web site: http://www.lxistandard.org . That document specifies the procedures that must be followed to claim conformance with this standard.

Comments for Revision. Comments for revision of LXI Consortium Standards are welcome from any interested party, regardless of membership affiliation with LXI Consortium. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards should be addressed to:

Bob Helsel
Executive Director
LXI Consortium
PO Box 1016
Niwot, CO 80544-1016

303-652-2571 Office - LXI
303-579-2636 Mobile
303-652-1444 Fax
ExecDir@lxistandard.org
LXI.WGs@gmail.com

LXI is a registered trademark of the LXI Consortium

Revision history

Revision	***Description***
Nov 8, 2016	Release specification.
Sept 12, 2016	Updated Overview to reflect advances in the deployment of IPv6. Repositioned text to align properly with page boundaries. Insertion of clarification to 21.31.and 21.3.2 as an observation. Removed appendices to example documentation and changed pointers to refer to LXI Example and Reference Material.
Mar 14, 2012	Minor edit corrections. Overview, 21.3.3, and 21.12.4
Feb 20, 2012	Initial Release of version 1.0

(This page left intentionally blank)

21 IPv6 LAN Configuration Overview

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4).

The world officially ran out of the 4.3 billion available IPv4 addresses in February 2011. IPv6 was created to provide a virtually inexhaustible supply of addresses for every device (2^{128}). Because of the limitations to IPv4, LXI supports use of instruments via the IPv6 protocol.

Although IPv6 has been available since 1999, real-world deployment has been slower than anticipated. As of January, 2016, the world reached 10% deployment, which was up from 6% a year earlier. It appears deployment of IPv6 is on an exponential curve moving forward.

Even though IPv4 addresses are exhausted at this point, the need for migration to IPv6 support can be more gradual. Most LAN-based instruments are used only on a local subnet, which can continue to use and re-use the local DHCP-supplied IPv4 addresses for instruments. It is only when subnets become IPv6-only or when instrument connections must be made over the WAN that IPv6 becomes more important.

Like IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable, and thus IPv6 is not backwards compatible. However, in most respects, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6.

IPv6 allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering and router announcements when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer media addressing information (MAC address). Network security is also integrated into the design of the IPv6 architecture, and the IPv6 specification mandates support for IPsec as a fundamental interoperability requirement.

The Internet Engineering Task Force (IETF) created RFC 6434 – IPv6 Node Requirements, in December 2011, which obsoletes the original RFC 4294. That document controls the standards that describe all the different RFC's pertaining to IPv6, but to implement the IPv6 protocol requires considerably more insight and assistance from other sources of information. There is a plethora of pointers to information available on IPv6 from The Internet Society (www.internetsociety.org), documents, case studies, training videos, etc. Here are a few key information sources for IPv6 deployment:

- RFC 6180 - Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment. This is not a "standard" but a document intended to be helpful
- IPv6 for IPv4 Experts – an eBook available to assist those already familiar with IPv4 to deploy IPv6.

- DoD/DREN IPv6 Knowledge Base – the United States Department of Defense (DoD) maintains a comprehensive site devoted to sharing information about IPv6. The actual link to the knowledge base is http://www.hpc.mil/dren/v6, but you must have a private internet connection to access this site.

- National Institute of Standards and Technology (NIST) – providing technical infrastructure to assist in IPv6 adoption: http://www-x.antd.nist.gov/usgv6/index.html

The intention of these information sources is to differentiate which RFC's are relevant to very different types of devices, which are called profiles.

The LXI Consortium has borrowed heavily on the research of the DoD and NIST information sources. NIST and the DoD have provided their information sources to help other government agencies in purchasing networking devices. They are also tightly coupled to the numerous institutions that provide IPv6 compliance testing or test suites. U.S. Government agencies are insisting that every piece of networking equipment purchased be compliant for IPv6. This testing and conformance initiative is to provide some confidence that all the IPv6 devices can interoperate and be "Good network citizens".

Following along the same lines as the U.S. Government, the LXI consortium is requiring that any LXI compliant IPv6 device have a compliant IPv6 network stack. If your instrument has an O/S system like Windows 10, 8, 7, Vista, Windows CE, VxWorks, or Linux, then the vendor (e.g. Microsoft) has already done this testing and the conformance declaration. If you have an operating system in an existing device, check with the manufacturer if they have an IPv6 stack and whether or not it is compliant. If compliant, did they use a testing house or did they run freely available test suites? You should also determine which test suites were used.

The web site: www.IPv6Ready.org seems to be the authority on the listing of "all things IPv6 compliant". Test suites can be downloaded from here, and you can see which vendors have completed the IPv6 testing and have been accepted for the IPv6 Ready logo.

LXI Reference Design Assistance

Given the discussion thus far, the LXI Consortium recognized the complexities associated with implementing an LXI conformant device. The LXI Consortium commissioned the LXI Reference Design, which includes an implementation of the IPv6 protocol in addition to other foundational building blocks in creating an LXI conformant device. Refer to the provided link for more information.

21.1 IPv6 Basic Requirements

If an LXI Device wants to claim conformance with the LXI IPv6 Extended Function, then all the rules in this document must be implemented. The recommendations in this document are technologies that if implemented would provide a "fully rounded" IPv6 device but are not necessary to pass the LXI Conformance Tests.

At this time, the LXI Consortium is recommending that a subset of IPv6 be implemented in LXI IPv6 compliant devices, which we are calling a **Minimal Viable Product** (MVP). There are several reasons for this:

- In our experimentation with IPv6, it seems that several vendors of IPv6 hardware and software stacks either have left DHCPv6 out or have implemented it improperly.

  That is, the DHCP server is not the first choice method to automatically assign IP addresses.

- Numerous T&M devices are using Windows XP, and it does not support DHCPv6.

Because of these, the following Rules and Recommendations may seem a little weak or lacking from a full IPv6 implementation.

Our philosophy with this MVP approach is to make sure we have an LXI specification for IPv6 for member companies to implement as soon as they see the need. And, this provides a minimalistic approach and should not be a huge burden to implement.

As a consortium we will continue to watch the IPv6 market place, and when we see a trend that deviates from what we have specified here, we may make things that are currently recommendations into rules.

MVP summary:

- Rule - create a link-local address
- Rule - implement SLAAC (get an address from the router if present)
- Rule - Web server must support IPv6
- Rule - IPv6 control connection (e.g. HiSLIP)
- Rule – mDNS must work on IPv6 only networks
- Recommendation – implement DHCPv6
- Recommendation – implement Static (fixed) IP addressing
- Recommendation – implement an IPv6 version of IEEE-1588 (ptp)
- Recommendation – implement an IPv6 version of the LAN triggers (events)

IPv6 is far more involved than IPv4, and government organizations like the U.S. Department of Defense (DOD) require that any IPv6 network equipment meet certain high standards of interoperability. Because of this, various testing houses have been setup, which will test IPv6 network appliances (hardware) or IPv6 network stacks (software) for conformance to the IPv6 standards.

The Web site: www.IPv6Ready.org is a good place to find a list of IPv6 approved O/S's, Network stacks and Testing Houses. This Web site is part of the IPv6 Forum, which is a group of companies that have a stake in the success of IPv6.

21.1.1 Rule – IPv6 Network Stack Compliance

All LXI IPv6 capable devices shall have IPv6 compliant network stacks. The vendor of the device must disclose to the LXI Conformance tester why they think their IPv6 stack is IPv6 compliant. This information will be kept confidential and need only be communicated to the LXI Conformance Committee Chairman.

By specifying that the device's IPv6 stack is IPv6 compliant, we are assuming you have done due diligence to make sure it conforms to all the RFC's for IPv6. One way to accomplish this is to run the IPv6 compliance tests that are located on the University of New Hampshire (UNH) Interoperability Labs (IOL) web site: http://www.iol.unh.edu/services/testing/ipv6/testsuites.

Using an operating system that has a fully compliant IPv6 stack is probably the quickest way to get IPv6 functionality in the device, but there is always some doubt that when the compliant stack is integrated with the hardware in the LXI device something could break the compliance. The LXI Consortium recommends that you run the compliance tests on the UNH web site as a sanity check that your device is fully IPv6 compliant, but this is not mandatory.

What follows are some of the key RFC's that need to be in the IPv6 stack of the device:

TCP/IP, UDP, IPv6 Network Protocols
LXI Devices shall support TCP/IP networking, as outlined in a number of RFC's, including 2460 (IPv6), 793 (TCP), and 768 (UDP).

LXI Devices can be controlled and communicated with using any higher-level protocol (such as HiSLIP or HTTP), as long as it is built on top of the TCP or UDP transport layers.

Low-level protocols other than TCP/IP may be used for non-control applications.

IPv6 over Ethernet
LXI IPv6 capable devices shall conform to RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks.

ICMPv6
LXI IPv6 capable devices shall implement and conform to RFC 4861 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.

Neighbor Discovery (ND)
LXI IPv6 capable devices shall implement and conform to RFC 4443 - Neighbor Discovery for IP version 6 (IPv6) Specification.

21.1.2 Rule – Interoperate with IPv4 networks

LXI compliant IPv6 devices shall be able to interoperate with other IPv6 capable devices on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6.

A compliant dual stack (IPv4 & IPv6) approach will accomplish this.

21.1.3 Rule – IPv6 Instrument Control Connections

LXI IPv6 Devices shall support instrument control connections using at least one TCP/IP IPv6-based protocol.

21.1.4 Recommendation – IPv6 HiSLIP Connections

LXI IPv6 Devices should support IPv6 device connections using IVI 6.1 HiSLIP. (See LXI HiSLIP Extended Function document) .

21.1.5 Recommendation – IPv6 SCPI Raw Connections

LXI IPv6 Devices should support IPv6 device connections using raw TCP/IP sockets. The syntax of the commands over this link is generally SCPI (See www.IVIFoundation.org for the SCPI Standard), but it doesn't have to be. It can be a propriety/vendor specific syntax.

21.1.6 Rule – IPv6 HTTP Web Access

LXI IPv6 Devices shall support IPv6 HTTP connections to the instrument web pages (Sections 9 and 21.11) and the LXI XML Identification Document (Section 10.2 and 21.14).

Observation - Relevant IETF RFC's

IPv6 compliant stacks comply with the following RFC's. This is not a comprehensive list but lists the major RFC's that need to be part of a compliant LXI IPv6 stack.

RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
RFC 5095 - Deprecation of Type 0 Routing Headers in IPv6
RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.
RFC 4861 - Neighbor Discovery for IP version 6 (IPv6) – supersedes RFC 2461
RFC 4291 - Internet Protocol Version 6 (IPv6) Addressing Architecture – supersedes RFC 3513.
RFC 4007 - IPv6 Scoped Address Architecture
RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
RFC 3484 - Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 5220 - Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules
RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3736 - Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 4862 - IPv6 Stateless Address Autoconfiguration – supersedes RFC 2462
RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 2401 - Security Architecture for the Internet Protocol
RFC 3646 – DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 2874 - DNS Extensions to Support IPv6 Address Aggregation and Renumbering
RFC 3364 - Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 IPv6)
RFC 3596 - DNS Extensions to Support IP Version 6
RFC 2136 - Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC-6106 - IPv6 Router Advertisement Options for DNS Configuration

21.2 IPv6 Address Configuration Techniques

IPv6 address configuration refers to the mechanism that the device uses to obtain an IPv6 address, Network Prefix, Default Gateway IP Address, and DNS IP Address. Much of this is handled automatically by the available Core IPv6 Protocol Stacks.

IPv6 supports both "stateful" and "stateless" auto-configuration. Being configured via a DHCP server is known as "stateful" whereas when a device configures itself (Link-Local address generation or via Router solicitation), it is known as "stateless". This method is called "stateless" because, in the case of the router, it is just configuring the network prefix and leaves the interface

identifier up to the device to configure. The router doesn't remember the device's previous address like DHCP servers can (stateful).

Types of IPv6 Autoconfiguration

Based on RFC 4862, all IPv6 nodes automatically configure a link-local address for each interface. An IPv6 host also uses router discovery—an exchange of *Router Solicitation* and *Router Advertisement* messages. These messages can include one or more Network Prefix Information options, which the receiving host can use to derive stateless addresses.

Acquiring a link-local address and any network prefix information from the router is known as Stateless Address Autoconfiguration (**SLAAC**).

Finally, a host can also use both stateless and stateful Autoconfiguration, which is a combination of addresses included in the router advertisement and obtained from a DHCPv6 server.

Auto configured Address States

When an auto configured address is in the tentative state, it is in the process of being verified as unique through duplicate address detection (DAD). An address in the valid state has been verified as unique and can be used for sending and receiving unicast traffic. The valid state includes both preferred and deprecated states. In the preferred state, the address can be used for unlimited communication. In the deprecated state, the address should not be used for new communication; however, existing communications using the address can continue.

IPv6 Autoconfiguration Process

The following steps describe the Autoconfiguration process for an IPv6 host as defined in RFC 2462:

- Derive a tentative link-local address with an Extended Unique Identifier (EUI)-64 interface identifier (ID). Refer to ***EUI-64 Identifiers*** in the ***LXI Example and Reference Material*** document for more information on how to create an EUI-64 identifier.
- Perform DAD on the tentative link-local address by sending a Neighbor Solicitation message with the Target Address in the message is set to the tentative link-local address.
- If a Neighbor Advertisement message sent in response to the Neighbor Solicitation message is received, the tentative link-local address is a duplicate address. Stop the address Autoconfiguration. At this point, manual configuration must be performed on the host.
- If no Neighbor Advertisement message (sent in response to the Neighbor Solicitation message) is received, the tentative link-local address is unique. Change the state of the address on the interface to Preferred.
- Send a Router Solicitation message.
- If no Router Advertisement messages are received and DHCPv6 is enabled, use DHCPv6 to obtain addresses and other configuration parameters.
- If a Router Advertisement message is received, configure tentative addresses for the included prefixes and perform duplicate address detection for each tentative address. If the addresses are unique, change the state of the addresses on the interface to Preferred.
- If the Managed Address Configuration flag (M flag) in the Router Advertisement message is set to 1, use DHCPv6 to obtain additional stateful addresses.
- If the M flag in the Router Advertisement message is set to 0 and the Other Stateful Configuration flag (O flag) is set to 1, use DHCPv6 to obtain additional configuration parameters.

Manual or static IP addresses can still be assigned to IPv6 nodes, just like in IPv4. If your device supports static addressing then it MUST provide a way to configure the different configuration modes (options): SLAAC, DHCP or Static.

IPv6 Address Scope

Scope	Prefix	Description
Unspecified	::	Equivalent to 0.0.0.0 in IPv4.
Loopback	::1	Equivalent to 127.0.0.1 in IPv4.
Link-Local	FE80::/64	Like IPv4 Auto-IP addresses - 169.254.0.0/16. Link-local addresses are used on the same subnet.
Site - local	FEC0::/10 Site-local addresses always begin with: "fec", "fed", "fee", or "fef"	Equivalent to IPv4 192.168.0.0 /16 – private IPv4 addresses. Site-local addresses are used within an organization's intranet and can be reused for different sites of an organization**. Site-local addresses have been deprecated in RFC 3879**, but can be used in current IPv6 implementations.
Unique - Local	FC00::/7	RFC 4193. They are supposed to be used for networks that are not connected to the Internet
Global	The first 3 bits in a global IPv6 addresses are 001.	Like public IPv4 addresses, IPv6 global addresses are globally reachable on the IPv6 portion of the Internet.
6to4 addresses	2002::/16	IPv6 uses 6to4 addresses to communicate between two IPv6/IPv4 nodes over the IPv4 Internet. A 6to4 address combines the prefix 2002::/16 with the 32 bits of the public IPv4 address of the node to create a 48-bit prefix — 2002:*WWXX*:*YYZZ*::/48, where *WWXX*:*YYZZ* is the colon-hexadecimal representation of *w.x.y.z*, a public IPv4 address. Therefore, the IPv4 address 157.60.91.123 translates into a 6to4 address prefix of 2002:9D3C:5B7B::/48.
Teredo Tunneling	2001::/32	
Multicast	FF00::/8	

Address Lifetimes (Leases)

An advertising router or DHCPv6 server specifies the valid and preferred lifetimes for an address prefix. An address enters the deprecated state after the preferred lifetime of the address has been exceeded. The preferred lifetime of an autoconfigured address is refreshed by receiving router advertisements or by renewing the DHCPv6 address configuration. When an address is in the deprecated state any existing connections can still proceed up until the valid lifetime lease is exceeded. No new connections are allowed if the interface has a deprecated address.

Figure 21.1 shows the states of an autoconfigured address and their relationship to the preferred and valid lifetimes.

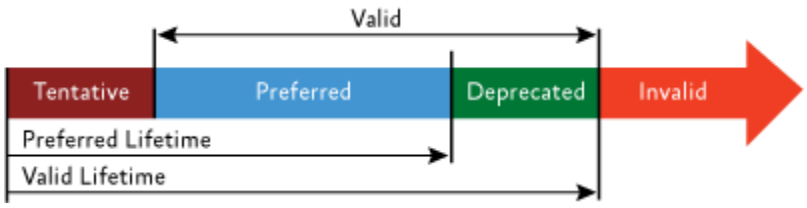

Figure 21.1

21.2.1 Rule – Create a Link-local address

All LXI IPv6 compliant devices shall create a unique Link-local address (FE80/64) first as described in RFC 4862 - IPv6 Stateless Address Autoconfiguration using the Neighbor discovery messages, which are part of ICMPv6.

21.2.2 Rule – Support Stateless Address Autoconfiguration (SLAAC)

LXI devices shall support RFC 4862 - IPv6 Stateless Address Autoconfiguration that supersedes RFC 2462.

21.2.3 Rule – Stop using the router assigned IP Address if the valid lifetime lease not renewed

If an LXI Device is unable to renew its router assigned valid lifetime lease, it shall stop using the supplied IP configuration that failed to be renewed, and signal an error to the user via the LXI LAN Status Indicator. Refer to Figure 21.1 for the definition of the valid lifetime lease.

21.2.4 Recommendation – Support Router Advertisement Options for DNS Configuration

For LXI IPv6 devices to be useful on intranets and extranets they need to be configured with the address for DNS servers. As the LXI MVP for IPv6 only requires SLAAC and not DHCP, if a device is automatically configured with the address for a DNS server, you should implement RFC-6106 - IPv6 Router Advertisement Options for DNS Configuration.

Observation – Router Advertisement Message Option Flags

The SLAAC specification – RFC 2462 described a method to get DNS addresses and other network configuration information from a DHCP server by looking at the Router Advertisement message option flags:

- If the Managed Address Configuration flag (M flag) in the Router Advertisement message is set to 1, use DHCPv6 to obtain additional stateful addresses.
- If the M flag in the Router Advertisement message is set to 0 and the Other Stateful Configuration flag (O flag) is set to 1, use DHCPv6 to obtain additional configuration parameters.

RFC 4862, which obsoletes RFC 2462, has removed the description about the M and O flags. Therefore, it is the LXI consortium's opinion that this option will be phased out in the future or that routers are not implementing this feature. It is likely they see the Router Advertisement Option for DNS Configuration, RFC 6106, more useful.

21.2.5 Recommendation - Support Static IP Address Assignment

Some TCP/IP networks require each device to be manually configured with an IP address, network prefix length, default gateway, and optionally DNS IP addresses. On manually configured networks, the network administrator will provide the network configuration values to the device user.

LXI IPv6 compliant devices should support Static IP addressing.

If you implement this recommendation, then devices shall provide some way to enter the following parameters into the device. Make sure you also follow the rules in section 21.11 about the LXI Web page requirements:

- IPv6 IP Address
- Network Prefix Length
- Default gateway
- DNS IP addresses – if you support a DNS client (21.4.6)

21.2.6 Recommendation – Support DHCPv6

LXI IPv6 compliant devices should support DHCPv6 which is the "stateful address Autoconfiguration protocol". See RFC 3315.

Observation – DHCPv6 Support

Some O/S LAN Stacks do not support DHCPv6…Windows XP SP3, in particular. The real requirement is that there is some way to automatically configure a global IPv6 address. Stateless router-advertisement-based addresses fit this bill, too.

21.2.7 Rule – Stop using the DHCP assigned IP Address if the valid lifetime lease not renewed

If an LXI device implements DHCPv6 then it must abide by this rule.

If an LXI Device is unable to renew its DHCPv6 valid lifetime lease, it shall stop using the supplied IP configuration that failed to be renewed, and signal an error to the user via the LXI LAN Status Indicator. Refer to Figure 21.1 for the definition of the valid lifetime lease.

21.2.8 Rule – Honor New DHCP Options at Lease Renewal

If an LXI device implements DHCPv6, then it must abide by this rule.

LXI Devices shall honor new DHCP options provided when renewing a lease.

Observation – DHCP Lifetime Renewal

When a DHCP client renews a lifetime or validates a current lifetime via a request transaction, it is possible for the DHCP server to send a reply with different option values than it sent when first sending the lifetime. For example, the DHCP server may specify a new DNS server to use. The implication is that the server wants the client to use the new values; however, this is not explicitly stated in the DHCP protocol. The DHCP client should honor new DHCP options provided, when renewing a lifetime.

21.2.9 Rule – Selection of IP Configuration Modes

If an LXI device supports DHCPv6 and/or Static IP, then there need to be options to configure the different modes via the LXI required Web pages (see Section 21.11 for LXI Web page requirements). Either of the following configurations is valid:

- A single configuration setting which allows a selection of one of the following options:
  - Automatic (implying SLAAC, DHCP)
  - Manual (Static IP address only).

- Individual configuration settings to enable or disable the following options :
  - SLAAC
  - DHCP
  - Static

If you only support one of these additional modes, then leave the one you did not implement out of the possible configuration settings, shown above.

Observation –LXI Options for IPv6 LAN Configuration

The MVP for LXI IPv6 Extended Function is to support only SLAAC, so there are no IPv6 LAN configuration settings required to select the mode.

All LXI IPv6 compliant devices create a link-local address, so this does not need to be configured.

21.2.10 Recommendation – Ability to Enable/Disable Privacy Setting

RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6 describes an extension to IPv6 stateless address Autoconfiguration for interfaces whose interface identifier is derived from an IEEE identifier (such as the MAC address). Use of the extension causes nodes to generate global scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node. These addresses are also known as temporary addresses.

For further information please read the privacy extensions in RFC 4941.

Various Operating Systems have this feature enabled by default and others have it disabled by default.

LXI IPv6 compliant devices should support enabling/disabling the privacy setting.

Observation – Enabling and Disabling Privacy setting on certain Operating Systems

When you enable IPv6 on your Windows based device, the kernel will change the interface portion of the IPv6 address to keep the device anonymous. If you want to use a static address or a non-changing EUI64 address, you will have to disable this privacy feature.

To disable it on Windows XP and Vista
Netsh int ipv6 set privacy disabled

On Windows 7:
Netsh interface ipv6 set global randomizeidentifiers=disabled
Netsh interface ipv6 set global randomizeidentifiers=enabled

On Linux based operating systems, this privacy feature is disabled by default. To enable it do the following in sysctl:
echo 2 >/proc/sys/net/ipv6/conf/all/use_tempaddr
or add "net.ipv6.conf.all.use_tempaddr=2" to /etc/sysctl.conf
To disable it again set the use_tempaddr to 0.

21.2.11 Rule – Privacy Setting Disabled by Default

Rule 21.2.10 explains what the privacy setting is. If an LXI implements enabling and disabling the privacy setting for the IP address, then by default this setting shall be disabled. This means when a LAN reset (LCI) is initiated the privacy setting shall be disabled.

21.3 Default Address Selection for IPv6

The IPv6 addressing architecture allows multiple unicast addresses to be assigned to interfaces. These addresses may have different reach-ability scopes (link-local, site-local, unique-local or global). These addresses may also be "preferred" or "deprecated".

The end result is that IPv6 implementations will very often be faced with multiple possible source and destination addresses when initiating communication. It is desirable to have default

algorithms, common across all implementations, for selecting source and destination addresses so that developers and administrators can reason about and predict the behavior of their systems.

(Relevant IEFT RFCs: 3484 and 5220)

The following rules, recommendations and permissions refer to displaying IPv6 addresses on LXI IPv6 compliant devices. This means they must be viewable from the front panel of the device, if the device has a front panel and it needs to be on the IPv6 Configuration Web page. See section 21.11 for more information on the IPv6 LXI web page(s).

21.3.1 Rule – Display Link-local Address

All IPv6 devices will display the preferred link-local address on the front panel displays, if present, and the Welcome web page. An IPv6 link-local address will have a network prefix of: FE80::/64 equivalent to IPv4: 169.254.0.0/16 addresses.

21.3.2 Rule – Display a minimum of one other Preferred Address

If an LXI IPv6 compliant device creates a globally scoped, preferred address, then this should be displayed via the front panel of the device, if it has one, and on the LXI defined Welcome page (see section 21.11 for IPv6 Web pages requirements).

Observation –Display of Addresses

It is in the best interest of users to display the addresses under Rule 21.3.1 and Rule 21.3.2 wherever it is reasonable to do so but the rule is not intended to be excessively onerous. A Test House will make a judgment in association with the vendor whether it is reasonable for the display to show the required information, and if unreasonable to deem the device does not have a suitable display. The intent is not to force vendors of devices with limited display functionality to display the address if the outcome is not useful to users.

.

21.3.3 Permission – To show all IPv6 assigned addresses

The vendor may choose to show all IPv6 assigned preferred addresses. This does make it confusing to the user as to which IP address they should use.

21.4 Name Resolution

IPv6 IP addresses are rather unwieldy and difficult for humans to remember therefore it is deemed that name resolution protocols such as DNS and multicast DNS (mDNS) are essential for LXI test systems.

21.4.1 Rule - Support Multicast DNS

LXI IPv6 capable devices must implement multicast DNS. All the rules and recommendations in section 10, for mDNS and DNS-SD, apply to IPv6 devices. See sections 10.3-10.8 of the Core LXI specification for more on this.

Observation

Some mDNS implementations prefer to send all mDNS traffic over IPv4, including AAAA records if the device running the mDNS implementation supports IPv4 as well as IPv6. Since mDNS is a local-subnet protocol, this should work if local mDNS receivers accept IPv4 traffic, as Windows PCs and other test controllers should.

21.4.2 Rule – Support mDNS on IPv6 only networks

mDNS must work on IPv6 only networks. LXI only requires at a minimum that mDNS use link-local address scoping (FF02/16) on IPv6 networks.

Refer to the following links for more information:

http://datatracker.ietf.org/doc/draft-cheshire-dnsext-multicastdns/

http://datatracker.ietf.org/doc/draft-cheshire-dnsext-dns-sd/

21.4.3 Recommendation – Send AAAA DNS Records over IPv4

LXI devices should include IPv6 addresses in their IPv4 mDNS messages in the form of AAAA DNS records.

Observation –Apple mDNS implementation concerning IPv6

The current Apple mDNS implementation, called Bonjour, sends IPv6 address AAAA records over IPv4 if it is available on an interface and does not send any IPv6 mDNS messages. The browsing part of that code also only listens to IPv4 mDNS traffic if IPv4 is available on an interface. As a result, Apple-Bonjour-based LXI mDNS discovery may not see IPv6 addresses unless they are included in the IPv4 mDNS messages from an LXI device.

.

Observation –Dynamic DNS is not supported on DHCPv6

For IPv4, Dynamic DNS (Domain Name System) Servers allow a network device (LXI Device) to set up a hostname without a network administrator doing anything.

Generally, a device doesn't have permission to update a DNS due to security reasons, so LXI doesn't specify that a device can update a DNS but only that it updates the DNS via a DHCP. However, DHCP server (option 12) doesn't exist on IPv6.

21.4.4 Recommendation – Single Hostname for All Naming Services

LXI Devices should have a single default hostname used for dynamic naming services, such as mDNS. The single module hostname shall be a legal DNS name.
Default Hostname recommendations:

- Syntax requirements:
- Maximum length of 15 characters.
- First character must be a letter (RFC 1035).
- Last character must be either a letter or a digit (RFC 1035).
- Intervening characters must be either a letter or a digit or a hyphen (RFC 1035).

Within a subnet or system or DNS domain, this name needs to be unique. Therefore, a pattern constructed from the model name and last part of the serial number should normally meet this requirement, as in the following example from Agilent Technologies: A-E4440A-12345.

21.4.5 Recommendation – Provide Manual DNS IP Address Entry

LXI Devices should allow the user to enter DNS server(s) IP addresses. The automatic IP configuration with manual DNS configuration enables the user to select a specific DNS configuration in addition to the DHCP configuration information. This is useful in network environments with a DNS server per department and a DHCP server per site.

21.4.6 Recommendation - Provide DNSv6 Client

LXI Devices should support a DNSv6 client for resolving hostnames. See RFC 3596 - DNS Extensions to Support IP Version 6

Observation – DNS Client Usage

Hostname Lookup Support

The previous section discussed how to make a module reachable as a server via a hostname. This section discusses the ability of the module to become a client in the network running things like a Web browser. This capability may not be used on all modules because they have little need to become a client on the network. In order to be a client on the network the module needs to be able to do hostname look-ups just like any other computer in the network.

Observation – DNS Client Advantages

DNS client capability allows an LXI Device to translate a hostname into an IP address. This capability may be used for the following applications:

- Running client applications (like a web browser) on the LXI Device to connect to other resources and/or servers on the network. This would be used, for example, to do firmware updates from a supplier's website.
- Doing reverse look-ups of IP addresses that have a connection to the LXI Device to get the hostname of the user connected, which is more recognizable than an IP address.
- Enabling a connection by hostname to nodes on the organization's LAN, such as servers or printers.
- Validating the DNS hostname that the LXI Device has by doing a reverse IP-to-hostname look-up on the LXI Device's IP address and then doing a forward hostname-to-IP address look-up to verify that it returns back the LXI Device's IP address.

21.5 ICMPv6 Echo Reply (Ping)

21.5.1 Rule – ICMPv6 Ping Reply

LXI Devices shall support ICMPv6 (Internet Control Message Protocol), used for a Ping Responder for diagnostics. (Relevant IETF RFC: 4443)

The TCP/IP stack in the LXI device shall be able to reply to the ICMPv6 echo request message used by the ping command. The 'ping -6 <hostname>' or 'ping -6 <IP address>' command is the standard way to understand whether a user's connection to an Ethernet device is working.

Note that both ping and ARP equivalents in IPv4 are done via ICMPv6, with ARP (IPv4) being replaced with neighbor discovery (IPv6). Echo request and Echo reply implement the 'ping' functionality.

Observation – How to use Ping in Windows

To ping the link-local address of another node on your link (also known as a subnet)

Type ping -6 Address%ScopeID

Where Address is the link-local address of the other node and ScopeID is the interface index for the interface from which you want to send ping packets.

You can obtain the interface index by typing "ipconfig /all" or "ipv6" and then pressing ENTER. ScopeId is also known as ZoneId.

To ping the global address of another node

Type ping -6 Address, where Address is the global address of the other node.

21.5.2 Recommendation – Support Ping Reply of the Multicast DNS Address

All LXI IPv6 compliant devices should reply to any Echo Request (pings) on the link-local scoped, multicast address for mDNS (FF02::FB). Using the command: ***ping -6 FF02::FB%ScopeId*** provides a convenient way to find all the mDNS devices on the link-local.

21.5.3 Recommendation – Provide Way to Disable ICMPv6 Ping Reply Message

It is recommended that the user should have a way to disable the ICMP Ping Reply in an LXI IPv6 device.

Observation – Disabling ICMP Ping Reply in Windows

Microsoft has several articles on using the Windows Firewall to enable/disable the echo reply message. By default in Windows XP, Vista and Windows 7 the reply to an echo request is disabled.

21.5.4 Rule – ICMPv6 Echo Reply Enabled by Default

If a way is provided to disable the ICMPv6 echo reply service then the echo reply service shall be enabled by default.

21.5.5 Recommendation – Support ICMPv6 Echo Responder message (Ping Client)

LXI Devices should support ICMPv6 echo responder messages (Ping Client) capability so that the user can ping other Ethernet devices from the LXI device.

Observation – Ping Client Usage

An ICMPv6 Ping Client available in a module may be useful in debugging communication problems with a TCP/IP configuration on a module.

21.6 Rule – Duplicate IP Address Detection

Duplicate IP Address Detection (DAD) is an essential part of the Neighbor Discovery protocol in IPv6. See RFC 4861 - Neighbor Discovery for IP version 6 (IPv6).

To do DAD the LXI device sends ICMPv6 packets on the link where this detection has to occur. Those packets contain *Neighbor Solicitation* messages. Their source address is the undefined IPv6 address "::" and the target address is the tentative address. A node already using this tentative address replies with a *Neighbor Advertisement* message. In that case, the address cannot be assigned to the interface. If there is no response, it is assumed that the address is unique and can be assigned to the interface.

LXI Devices shall disconnect from the network when a duplicate IP address is detected. IPv6 allows for automatic resolution of Autoconfiguration IP addresses, but manually set IPv6 addresses may still require disconnect behavior.

If a DAD is detected the device can fall back to the previous address it had as long as DAD on this address passes or it can just disconnect from the network and show its IP address as "::" and use the LXI LAN Status Indicator to signal a fault condition.

Observation – Duplicate IP Addresses in Manually Configured Networks

Manually configured IP addresses may result in duplicating an address already in use; this generally does not occur when using DHCP/Dynamic Link-Local Addressing. Avoiding the use of an IP address already in use ensures the LXI Device will not create a problem on the network. Duplicate IP Address detection gives the user the basic diagnostic information to know there is a problem on the network.

Duplicate IP addresses on DHCP configured systems are unlikely but they are possible. The DHCPv6 specification (RFC 3315 section 18.1.8) specifies how a duplicate IP address check should be done within the DHCP SOLICIT/ADVERTISE/REQUEST/CONFIRM protocol sequence.

Observation – How to Clear a Duplicate IP Address

A duplicate IP address indicates network problems. To clear a duplicate IP address, check the following :
(1) If using manual configuration (static IP) check the address is correct via the front panel.
(2) Use the LAN Configuration Initialization (LCI) reset mechanism to get the device back into a known state. See section 21.9 for the default state.

21.7 Recommendation – Check Network Configuration Values for Validity

The values entered by the device user should be checked to ensure they are in the valid range.

21.8 Rule – Provide an Error Indicator for LAN Configuration Faults

LXI Devices shall make use of the LXI LAN Status Indicator to inform the user of a LAN fault or error caused by:

- Failure to acquire a valid IP address
- Detection of a duplicate IP address
- Failure to renew an already acquired auto-configured address (SLAAC or DHCP) valid lifetime (lease). Failure to obtain an initial SLAAC or DHCP lifetime is not a failure.
- LAN cable disconnected (as reported by Ethernet connection monitoring)

Observation – DHCP is only a recommendation

To be clear - implementing DHCPv6 is optional.

See Section 2.5.5 of the Core Specification LAN Status Indicator for details about the annunciator.

The LXI LAN Status indicator indicates both the LAN error conditions above and provides an *identify* indication as described in the core specification, section 2.5.2. This identifying indication is initiated by the user via the Web interface, section 9.3, or by the API, section 6.8.

The LXI LAN Status indicator shall provide *LAN Fault*, *Normal Operation*, and *Device Identify* indications as shown in the state diagram below. Note that the state labeled "State Undefined" is transitory and the behavior of the indicator is not specified.

IPv6 Autoconfiguration addresses have two lifetimes associated with them – refer to Figure 21.1. The first one is the preferred lifetime, which is how long the address remains a preferred address. After this time period the address becomes a deprecated address, which means it can still be used for existing communication sessions but should not be used for new communication sessions. After the valid lifetime has expired, then the address should not be used at all unless it is renewed and checked that it is not a duplicate using DAD.

Sometime before the preferred lifetime is up, the device should try to renew the lifetime. In normal circumstances, this request should be granted and the devices address remains the same. If something changes on the network then this request may fail. If a new address is given when the request to use the old one is done then the device must use the new address. If the request fails because there was no response then this is an error that should set the LAN Status Indicator.

There are two scenarios that play out when dealing with the address lifetime process.

1) After power up or a LAN reset, if a device is configured for both DHCP and SLAAC and one of these configuration methods fails but the other one successfully gets a validated address, then there is no fault and the LAN Status Indicator should indicate no fault.

2) In the second case, where a device is connected to the network, it does successfully obtain a validated IP address, be it via DHCP or SLAAC. However, at a later time the device fails to renew that lease. Then per rule 21.2.3 or 21.2.7 the device must stop using the IP Address it had obtained at this point and the LAN Status Indicator must indicate a fault. This is to indicate to the user that an Autoconfiguration address lifetime renewal has failed and that the device does not have the same IP Address that it did before.

At this point, the LAN Status Indicator must remain in the fault state until one of the following happens:

a) The device successfully acquires a new lifetime. (This can happen if it is configured to periodically attempt to obtain a lifetime.).

b) The device is restarted.

c) The LAN Configuration is reinitialized for the device by the user. (This could be done through the LCI, unplugging and re-plugging the LAN cable, or another mechanism if the device is so equipped.)

In scenarios b and c, the behavior when the device again attempts to obtain an address is the same as in the case 1, if DHCP fails but a SLAAC address is obtained or vice versa, the LAN Status is no fault.

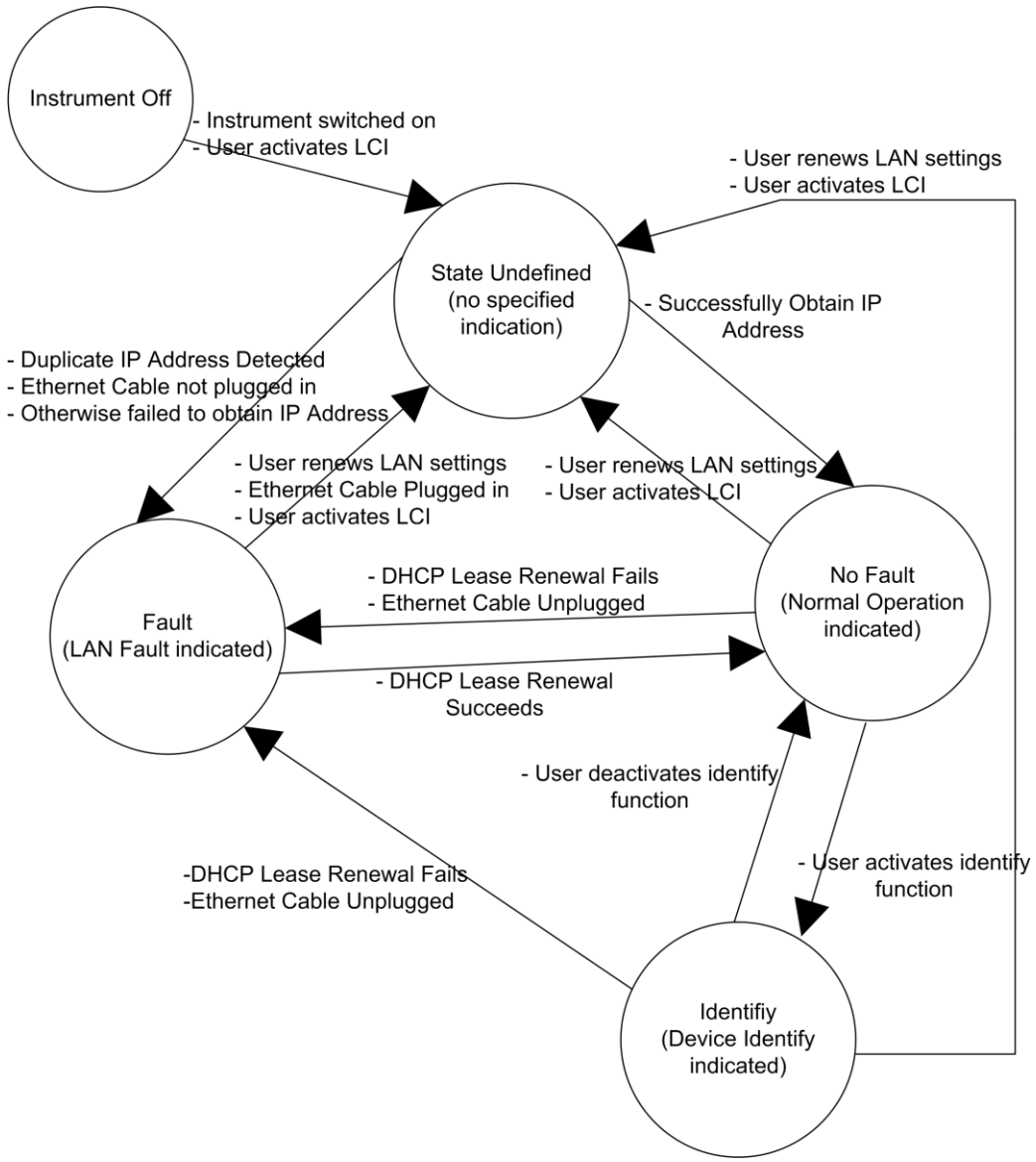

Figure 21.2

21.8.1 Rule – Combined IPv4 and IPv6 LAN Status Indicator

As per rule 2.5.5 of the Core Specification, there must be at least one LAN Status Indicator, which conforms to the combined IPv4 state diagram in section 8.10 and the IPv6 state diagram shown above.

Four possible scenarios need to be considered:

1. If the IPv4 stack only is enabled, then the status indicator needs to conform to section 8.10 only.

2. If the IPv6 stack only is enabled, then the status indicator needs to conform to section 21.8 only.

3. If both the IPv4 and IPv6 stacks are enabled, then a definite error condition is a little more complex. In the following text, a failure to get an IP address could be for one of the following reasons: no DHCP server (v4 or v6) present, duplicate address detected or no address created through router solicitation (SLAAC).

    a. If a LAN cable is not plugged in or the device is not connected to an Ethernet LAN, then this is an error.

    b. If both the IPv4 and IPv6 stacks get addresses, then there is no error condition.

    c. If from power up or after a LAN reset one of the stacks gets an IP address and the other stack doesn't, then there is no error condition. This could happen if you connect the device to an IPv6 only network then we would expect the IPv6 stack to get an address while the IPv4 will fail.

    d. If from power up or after a LAN reset both of the stacks get IP addresses and then when they try to renew their leases one of them fails, then this is an error condition. Something has changed on the network from the first time the device gained its addresses and so the user should be notified through the status indicator. If the network change was planned, for example, a DHCPv4 server was shutdown, then the user just has to initiate a LAN reset or power the device back on for the error to go a way – same as 3c.

4. If the IP privacy mode is enabled (see 21.2.10) then the network stack will create random IPv6 addresses (obscuring the MAC address) every so often but it will also do DAD on each new address. When this happens it is not a LAN Status error condition as it is similar to a router or DHCP server giving out new parameters when a device tries to renew a lease.

21.8.2 Rule – IPv6 Link-Local address is not an error condition

If the IPv6 stack obtains a Link-Local address only, then this is not an error condition. On most private IPv6 local networks then it is to be expected that there may be no DHCPv6 server or a router configured to solicit the network prefix, so a link-local only address is expected behavior.

21.8.3 Permission – Allow separate LAN Status Indicators for IPv4 and IPv6

It is allowed to have separate LAN Status Indicators for IPv4 and IPv6 as long as the IPv4 indicator follows all rules in section 8.10 and the IPv6 indicator follows all rules in this section of the specification.

21.8.4 Recommendation – Ability to configure the LAN Status Indicator

Having the ability to configure the LAN Status Indicator to show faults from only the IPv4 or IPv6 stack is useful. An alternative way to do this is to provide a way to enable or disable the IP stacks – see **Recommendation 21.11.7**

21.8.5 Rule – LAN Status Indicator enabled by default for both IPv4 and IPv6

If the LAN Status Indicator can be configured, the LAN Status indicator by default shall show both IPv4 and IPv6 errors.

21.9 Rule – LAN Configuration Initialize (LCI)

LXI Devices shall provide an LCI reset mechanism, as defined in the core specification – section 2.4.5 that when activated places the LXI Device's network settings into a default state. These settings shall take effect when the LCI mechanism is activated, without requiring any further operator actions (e.g., if the LXI Device requires a reboot for the changes to take effect, the LXI Device shall reboot automatically). The LXI Device default state shall be fully documented and available in the manufacturer's supplied documentation.

Table of items affected by LAN Configuration Initialize Mechanism

Item	Value	Section
IPv4 stack	Enabled	21.11.7
IPv6 stack	Enabled	21.11.7
IPv6 Address Configuration: 1. SLAAC 2. DHCPv6 3. Static	1. Enabled 2. Enabled if implemented 3. Disabled if implemented	Section 21.2.9
Privacy Setting	Disabled	Section 21.2.11
LAN Status Indicator	Enabled for both IPv4 and IPv6	Section 21.8.5
ICMPv6 Echo Reply Message	Enabled	Section 21.5.4
Web Password for configuration	Factory Default	Section 9.8
mDNS and DNS-SD	Enabled	Sections: 10.3, 10.4 &, 10.7.1 & 21.4.1

If an LXI Device has a manual user interface (physical front panel) that allows the configuration of these items plus the network configuration, then that shall be sufficient to meet the needs addressed by this button – as long as there is a single LAN Configuration Initialize key in the manual interface that sets the items in the above table as indicated.

Observation – It Is Possible To Misconfigure Network Settings

It is possible to misconfigure the network settings of an LXI Device, potentially rendering it unable to communicate with any hosts. Additionally, the settings on a box could simply be forgotten. Due to the limited user interface of a typical LXI Device, there is no simple way to view or modify the network settings (e.g., via a web browser) without a working network connection. Therefore, a simple mechanism, such as pressing the recessed rear panel LCI mechanism to force the LXI Device's network settings to a known default state, is a very desirable feature.

21.10 Optional Protocols and Features

Listed above are the core rules and recommendations that are required for LXI IPv6 compliance. Listed in this section of the specification are other IPv6 protocols or features that may be of interest to LXI devices.

21.10.1 Recommendation – IP Layer Security (IPSec)

IPSec is an essential part of any compliant IPv6 network stack and may be of use to some LXI devices to encrypt data or commands between the host and the LXI device.
See RFC 2401 - Security Architecture for the Internet Protocol.

21.10.2 Mobile IPv6

Mobile IPv6 allows an IPv6 node to be mobile – to arbitrarily change its location on an IPv6 network – and still maintain existing connections. This is neither a rule nor a recommendation but an observation that this might be useful.
See RFC 3775 – Mobility Support in IPv6

21.11 IPv6 Web Page Requirements

IPv6 requires that some additional information and configuration settings be on the LXI specified Web pages.

Observation – IPv6 Compatible browsers

Note: The LXI devices Web server needs to be accessible via IPv6 see rule 21.1.6.

To access an IPv6 device from an IPv6 compatible browser you would usually surrounded the IPv6 address in the URL with square parenthesis. In the Web browser, a user would type something like this for a URL:

http://[fe80::216:cbff:fe97:4a4e]

To access the instruments identification schema you would type in:
http://[fe80::216:cbff:fe97:4a4e]/lxi/identification

21.11.1 Rule – Implement all Rules in the Web Interface Section

Implement all the Rules in Section 9 – Web Interface.

21.11.2 Rule – Include 'LXI IPv6' in Welcome Web Page "LXI Extended Functions"

Devices implementing the LXI IPv6 function shall include 'LXI IPv6' in the 'LXI Extended Functions' display item of the welcome web page.

21.11.3 Rule – Show LinkLocal and Preferred IPv6 Addresses on Welcome Web Page

Add the following information to the LXI Welcome Page - Rule 9.2:

- IPv6 Link-Local Address
- Show at least one preferred Global addresses obtained through SLAAC, DHCPv6 or Static addressing. If none are available then just show the link-local address.
- Optionally show any other scoped and preferred addresses obtained through SLAAC, DHCPv6 or Static addressing such as Unique-Local addresses.

21.11.4 Recommendation – Use one LAN Configuration Page

Section 9.5 describes the information that needs to be present to configure an IPv4 device.
You should add the IPv6 LAN Configuration information required in this section to the same web page.

This combined page must have everything stated in Rule 9.5 for the IPv4 configuration and everything in Rule 21.11 for IPv6 configuration.

See ***Example Web Pages*** in the *LXI Example and Reference Material* for example LAN Configuration pages.

21.11.5 Permission –Separate IPv4 and IPv6 LAN Configuration pages are allowed

Rather than have one combined IPv4 and IPv6 Configuration Page you can have separate ones if you require. Two links need to be present on the LXI Welcome Page (1) to an IPv4 configuration page and (2) to an IPv6 configuration page. The links need to be clearly labeled IPv4 Configuration and IPv6 Configuration respectively.

21.11.6 Rule – Show Static IPv6 Settings on LAN Configuration Web Page

Section 9.5 describes the information that needs to be present to configure an IPv4 device. The hostname and description are common for both IPv4 and IPv6 so this only needs to be present once.

If the device supports Static IP mode, on IPv6, then the following settings need to be on the IP Configuration Page and configurable by the user of the device:

- IPv6 Configuration Mode[1]
- IPv6 address [2]
- Prefix Length
- Default Gateway[3]
- DNS Server(s)[4]

The IPv6 Configuration Mode field controls how the IP address for the instrument is assigned. For the manual configuration mode, the static IP address, prefix length, and default gateway are used to configure the LAN. The automatic configuration mode uses Autoconfiguration addressing (SLAAC and DHCPv6 – if implemented), as described in section 21.2 to obtain the instrument IP address(es).

21.11.7 Recommendation – Add a stack disable option to the Configuration Mode.

Add an option to the IPv4 and IPv6 Configuration Mode selection to disable IPv4 and IPv6 respectively but not both at the same time. See ***Example Web Pages*** in the ***LXI Example and Reference Material*** for example LAN Configuration pages.

21.11.8 Rule – Show Mode as 'Disabled' and Blank or '-' fields for disabled IP Protocol

If recommendation 21.11.7 is implemented, which is the capability to disable either of the IP stacks then the required information, to be shown on the web page, for the disabled stack needs to do the following:

1) Show only the relevant field descriptions for IPv4 or IPv6. If one protocol is disabled, the web page should show blank or dashed ("-") entries for that protocol.

2) For the IPv4 or IPv6 Configuration Mode, show the text "Disabled" when that protocol is disabled.

See ***Example Web Pages*** in the ***LXI Example and Reference Material*** for example LAN Configuration pages.

21.11.9 Recommendation – Identify IPv6 Enabled Features on Welcome Page

All optional IPv6 capabilities should be identified on the instrument's Welcome Page for the benefit of the End User.

Example for IPv6 identification:

[1] Refer to section 21.2.9
[2] Static IP address. Refer to section 21.2.5
[3] IPv6 Gateway to use in manual (static) addressing mode.
[4] IPv6 DNS address(s)

IPv6-Enabled: LXI Event Messaging, LXI Clock Synchronization, LXI HiSLIP, Sockets

21.12 LXI Clock Synchronization Changes

All LXI IPv6 compliant devices that are implementing the LXI Clock Synchronization using IEEE 1588 extended function need to implement this section in addition to sections 3, 4 and 6.

21.12.1 Recommendation – Implement an IPv6 version of IEEE-1588

As the IEEE-1588 protocol usually runs over the local-link scope it is only a recommendation to implement an IPv6 version of IEEE-1588.

If you implement an IPv6 version of LXI Clock Synchronization, then you need to abide by the following rules in this section.

21.12.2 Rule – Support IEEE-1588 via UDP over IPv6 for the Link-Local Scope

The LXI IEEE-1588 Profile 1.0 recommends that UDP over IPv6 transport should be possible (Recommendation 2.6.2 – UDP over IPv6). If the device implements recommendation 21.12.1 then the device shall support IEEE-1588 via UDP over IPv6 for the link-local scope (FF02/16).

21.12.3 Rule- Support selecting IPv4 or IPv6 for IEEE-1588

If you implement recommendation 21.12.1 then you shall abide by this rule.

IEEE-1588 running on IPv6 is not compatible with IEEE-1588 running on IPv4 because you can't have 2 master clocks.

LXI IPv6 compliant devices shall have the ability to select which IP protocol to run over: IPv4 or IPv6 and they shall never allow both to be enabled. This configuration option should be located on the LXI Sync Web page.

21.12.4 Rule – Changes to LXI Sync Web Page

If you implement recommendation 21.12.1, then you shall abide by this rule.

There are no changes needed to the LXI Sync Web page if the IEEE-1588 stack only supports IPv4. If it supports either then the device shall add the ability to select which protocol the IEEE-1588 stack is supposed to use.

If the Current Grandmaster clock and Parent clock are identified by IP address then they shall show the IPv6 addresses if the IEEE-1588 stack was using IPv6. The normal nomenclature for these 2 parameters is to show the EUI-64 identifier.

21.13 LXI Event Messaging Changes

All LXI IPv6 compliant devices that are implementing the LXI Event Messaging extended function need to implement this section in addition to section 3, 4 and 6.

21.13.1 Recommendation – Implement an IPv6 version of LXI Events

As LXI Events are usually run over the local-link, it is only a recommendation to implement an IPv6 version of LAN Events.

If you implement an IPv6 version of LXI Events then you must abide by the following rules in this section.

21.13.2 Rule – Use IPv6 Multicast Address and Port Number

If you implement recommendation 21.13.1, then you shall abide by this rule.

LXI Devices shall use the IANA registered IPv6 multicast address of FF02::138 for LXI Event Message transmission using UDP multicast.

The default IANA registered port number is 5044 for LXI Event Messages—user configuration may override this default.

21.13.3 Rule – Support IPv6 Address in Square Brackets in IviLxiSync Interface

The IviLxiSync IVI document defines destination paths and filters that may contain IP addresses, called ‘host numbers’ in the IviLxiSync Specification. If devices support IPv6 LXI Events, then their IVI driver IviLxiSync interface shall accept IPv6 addresses inside ***square brackets*** anywhere host numbers can appear in the IviLxiSync interface. The device shall use these IPv6 addresses to implement destination paths and filters.

Example for Event Destination Path (IviLxiSync 5.2.2):

[2000:1::1]/MyEventName, mySource.local/MyEventName

21.14 LAN Discovery and Identification Changes

All LXI IPv6 compliant devices need to implement all the rules in section 10 of the core specification except section 10.1 – Support VXI-11.

Observation – No VXI-11 for IPv6

> Rule 10.1 says all devices have to support VXI-11. The VXI-11 protocol uses a LAN broadcast packet in the discovery phase of the device. Broadcast packets are not supported in IPv6 and so a new LAN protocol for instrumentation was devised that works on both IPv4 and IPv6 networks and is much faster than VXI-11. This protocol is called High-Speed LAN Instrument Protocol (HiSLIP). See the IVI (www.ivi.foundation.org) specification 6.1 for further information on this.
>
> Also see Rule 21.1.3, 21.1.4 and 21.1.5 about control connections to the device.

21.14.1 Rule - Support IPv6 access to Identification XML Document

The LXI XML Identification document shall be accessible via IPv6.

21.14.2 Rule - Include LXI IPv6 Address in <Interface>

If an IPv6 global address is available devices shall include it in an <Interface> XML element. If no IPv6 global address is available, devices shall include the link-local IPv6 address in an <Interface> XML element.

21.14.3 Rule – IP Type is "IPv6"

Devices shall use "IPv6" as the IP type for the IPv6 address <Interface> element.

21.14.4 Recommendation - Include LXI link-local IPv6 Address in <Interface>

Devices should include the IPv6 link-local address in an <Interface> element.

21.14.5 Rule - Include LXI IPv6 Address in <Gateway>

If an IPv6 address for the gateway is available, devices shall include it in the <Gateway> element of the IPv6 <Interface> element.

21.14.6 Rule - Show LXI Prefix length in <SubnetMask>

Devices shall show the prefix length in the <SubnetMask> element of the IPv6 <Interface> element.

21.14.7 Rule – Include the LXI IPv6 Function in the <LxiExtendedFunctions> element

LXI devices implementing IPv6 shall include a <Function> element in the <LxiExtendedFunctions> XML element with the FunctionName attribute of "LXI IPv6" and a Version attribute containing the version number of this document.

Example:
<Function FunctionName="LXI IPv6" Version="1.0"/>