# LXI Extended Function IPv6

Revision 2.1

January 18, 2024

 

 

## *Notices*

**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 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. 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 may 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:

Executive Director
LXI Consortium
www.lxistandard.org
ExecDir@lxistandard.org

**LXI is a registered trademark of the LXI Consortium**

**Revision history**

| ***Revision*** | ***Description*** |
|---|---|
| 2.1<br>Jan 18, 2024 | Fixed broken links in TOC |
| 2.1<br>Aug 17, 2023 | Rule 21.2.9 changed to allow Auto/Manual IP configuration.<br>Made 21.14 a Rule to reference the Identification section of the API Extended Function. Deleted rules 21.14.x as they are not necessary now. |
| 2.0.0<br>May 10, 2022 | Now referencing the NIST IPv6 profile and not the RFCs<br>Static and DHCPv6 addressing are now required instead of recommendations<br>Added rule to enable /disable ipv4<br>Added rule to enable/disable ipv6<br>Added rule to enable/disable mDNS<br>Added rule all extended functions supported on IPv4 shall be supported on IPv6 |
| 1.1.0<br>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 |
| 1.0<br>Feb 20, 2012 | Initial Release |

 

# 21 LXI IPv6 Extended Function

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

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.

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 ($\mathbf{2^{128}}$). Because of the limitations to IPv4, LXI supports use of instruments via the IPv6 protocol.

Google tracks the adoption rate of IPv6 worldwide. This shows much greater world-wide adoption of IPv6 since version 1.1 of this specification:

https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

The RFCs for IPv6 were changed from RFC category to the Standards Track (STD) in 2017. The U.S. Government is driving the adoption of IPv6 and has a goal of converting 80% of its IT equipment (backbone and clients) to IPv6 by 2025.

The Internet Engineering Task Force (IETF) created the original IPv6 RFC (RFC 4294) in 2006. It was subsequently replaced with RFC 6434 and then RFC 8504. Due to this constant churn in the standards NIST has created a NIST IPv6 Profile document that tracks all the relevant IPv6 specifications (RFCs). NIST will maintain this document and keep the RFC references up to date.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

## Purpose and Scope

This document is an extension of the LXI Device Specification 2022. Numbering for sections, **RULES,** and **RECOMMENDATIONS** is consistent with the hierarchy of the LXI Device Specification 2022.

### Purpose

The purpose of this Extended Function is to promote adoption of IPv6 and make sure an LXI IPv6 conformant device will work correctly on modern IT infrastructure. As IPv4 addresses have run out and the US Government (one example) is requiring that LAN equipment support IPv6, LXI Devices should support IPv6.

### Scope

This specification defines the **RULES** and **RECOMMENDATIONS** for constructing a LXI Device that conforms with the LXI IPv6 Extended Function. Whenever possible this specification uses existing standards.

Devices that implement this specification must also satisfy additional requirements in the LXI Device Specification and other supported LXI Extended Functions.

The standard specifies:

1. IPv6 Stack Compliant to NIST IPv6 Profile and the IPv6Ready Logo Program
2. LXI IPv6 Configuration requirements
3. IPv6 Address Selection requirements
4. Name Resolution requirements
5. LXI IPv6 DNS-SD service announcement requirements
6. IPv6 ICMPv6 requirements
7. IPv6 Duplicate Address Detection requirements
8. LXI LAN Status requirements
9. LXI LAN Configuration Initialization requirements
10. LXI IPv6 Web page requirements
11. LXI Clock Synchronization requirements for IPv6
12. LXI Event Messaging requirements for IPv6
13. LAN Discovery and Identification requirements for IPv6

## Definition of Terms

This document contains both normative and informative material. Unless otherwise stated the material in this document shall be considered normative.

Normative material shall be considered in determining whether an LXI Device is conformant to this standard. Any section or subsection designated as a RULE or PERMISSION is normative.

Informative material is explanatory and is not considered in determining the conformance of an LXI Device. Any section or subsection designated as RECOMMENDATION, SUGGESTION, or OBSERVATION is informative. Unless otherwise noted examples are informative.

**RULE**: Rules **SHALL** be followed to ensure compatibility for LAN-based devices. A rule is characterized by the use of the words **SHALL** and **SHALL NOT**

**RECOMMENDATION**: Recommendations consist of advice to implementers that may improve the final device. Discussions of particular hardware to enhance throughput would fall under a recommendation. These should be followed to avoid problems and to obtain optimum performance.

**PERMISSION**: Permissions are included to clarify the areas of the specification that are not specifically prohibited. Permissions reassure the reader that a certain approach is acceptable and will cause no problems. The word **MAY** is reserved for indicating permissions.

**OBSERVATION**: Observations spell out implications of rules and bring attention to things that might otherwise be overlooked. They also give the rationale behind certain rules, so that the reader understands why the rule must be followed.

# Applicable Standards and Documents

The following referenced documents are indispensable for the application of this document (that is, they must be understood and used). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

**NIST IPv6 Profile**

In the LXI IPv6 Extended Function version 1.1 the relevant IPv6 RFCs were called out in the document. As of version 2.0 the LXI IPv6 Extended Function regards the NIST IPv6 Profile as the definitive definition of IPv6.

The NIST IPv6 Profile is at revision 1 at the time of writing. See the latest NIST IPv6 Profile for a list of the relevant IPv6 RFCs.

For information regarding IPv6 implementation see:

- NIST IPv6 Profile
  - NIST IPv6 Profile Document: https://doi.org/10.6028/NIST.SP.500-267Ar1
  - NIST IPv6 Profile Summary Table: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-267Ar1s.pdf
- IPv6 Ready Logo Program: https://www.ipv6ready.org/

**IPv6 Compliance Testing**

Although the LXI Consortium does not perform IPv6 compliance testing, the IPv6 Forum provides an IPv6 testing service. The IPv6 Forum has a IPv6 Ready Logo Program which is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and is ready to be used.

www. https://www.ipv6ready.org/

The IPv6 Ready Logo Committee mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools and to deliver the IPv6 Ready Logo. The Key objectives and benefits of the IPv6 Ready Logo Program are to:

- Verify protocol implementation and validate interoperability of IPv6 products.
- Provide access to testing tools.
- Provide IPv6 Ready Logo testing laboratories across the globe dedicated to providing testing assistance or services.

### Trade Association Standards[1,2,3]

IVI-6.1, High-Speed LAN Instrument Protocol (HiSLIP) v2.0 April 23, 2020

## Relationship to other LXI Standards

Devices that comply with LXI IPv6 shall also conform to the LXI Device Specification.

Some LXI Extended Functions have additional IPv6 requirements on devices that also implement the IPv6 Extended Function.

## Terminology

This section contains background information on the terminology of this specification.

**Technical Terms**

The following terms are used in this specification:

| Terms | Definition |
|---|---|
| SLAAC | StateLess Address Auto-Configuration |
| DAD | Duplicate Address Detection – part of the SLAAC RFC for detecting if an IP address is already in use. |
| RA | In IPv6, a router is located through Router Advertisement (RA) messages sent from routers instead of by DHCPv6 |
| IID | The Interface Identifier (IID) is the last 64 bits of an IPv6 address. |
| Stable Addresses | The *stable address* does not vary over time, barring a manual change. |
| Temporary Addresses | A temporary address is an address that has a finite lifetime. |
| O/S | Operating System |

**IPv6 Address Lifetimes**

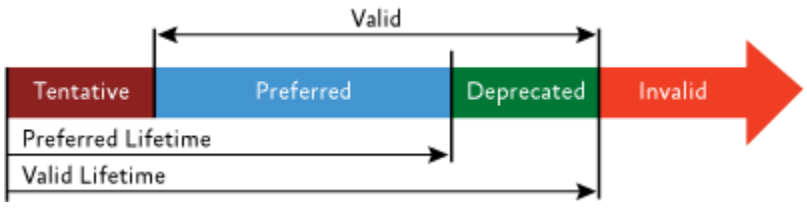


**Figure 21-1 IPv6 Address Lifetimes**

[1] IVI specifications are available from the IVI Foundation at http://www.ivifoundation.org
[2] LXI Standards are available from the LXI Consortium at http://www.lxistandard.org
[3] VXI-11 specifications are available from the VXI Bus Consortium at http://www.vxibus.org/

The figure above shows the states of an autoconfigured address and their relationship to the preferred and valid lifetimes.

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 is exceeded. No new connections are allowed if the interface has a deprecated address.

**Use of the Terms Default and Device**

When the term *default* is used in this document to refer to a setting, it refers to the value of the setting when the device is shipped by the vendor, or after the operator performs a reset on the device that entirely removes the previous configuration of the device.

The value of the setting after an LAN Configuration Initialize (LCI) is performed is referred to as the LCI value of the setting. See the LXI Device Specification, 8.13, for details on LCI.

Where the term *device* is used in this specification, it refers to a LXI device that implements this specification.

.

 

## 21.1 IPv6 Basic Requirements

The rules in this section specify general requirements for IPv6 conformance.

### 21.1.1 Rule – IPv6 Network Stack Compliance

Devices shall have a IPv6 compliant network stack.

See the website: www.ipv6ready.org for a list of IPv6 compliant operating systems and network stacks.

#### *Observation – Compliant IPv6 Network Stack*

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 device something could break the compliance. The LXI Consortium recommends that you run the compliance tests on the IPv6Ready website to verify that your device is fully IPv6 compliant, but this is not mandatory.

Device vendors should either:

1. Complete due diligence to make sure it conforms to all applicable RFCs for IPv6.
2. Verify with the vendor of the Operating System or network stack that their product passes the IPv6 tests at the IPv6Ready website or that the network stack was approved at another IPv6 Compliance Laboratory.
3. Run a set of IPv6 compliance tests to ensure conformance.

#### *Observation - Relevant IETF RFCs*

IPv6 compliant stacks comply with the numerous RFCs for IPv6. The NIST IPv6 Profile provides a list of all the relevant IPv6 RFCs.

At the time of writing this specification in the NIST profile table an LXI Device would fall under the “Host” functional role and not the “Router” or “Other” columns. If the NIST profile table has an “M” in the table then that RFC is mandatory. If it is blank, then that RFC is optional. If the cell is grey, then that RFC is not relevant for that functional role.

### 21.1.2 Deprecated Rule – Interoperate with IPv4 networks

Deprecated in LXI version 1.6.

### 21.1.3 Rule – IPv6 Instrument Control Connections

LXI IPv6 Devices shall support Command and Control connections using at least one 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 command set used 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 device command set.

### 21.1.6 Rule – IPv6 HTTP Web Access

LXI IPv6 Devices shall support web pages (LXI Device Specification, Sections 9 and 21.11) and the LXI XML Identification Document (LXI Specification, Section 10.2 and 21.14) via IPv6 connections. HTTP connections can be secure (over TLS) or insecure (over TCP).

If the LXI device implements the LXI API Extended Function, then the API shall operate on IPv6 as well as IPv4 connections.

### 21.1.7 Rule – Support IPv6 Operations with Extended Functions

LXI IPv6 conformant devices that implement LXI Extended Functions shall support IPv6 for all IP operations required by the extended function unless explicitly permitted to omit IPv6 support by this specification.

There are additional requirements in this specification for some extended functions.

### 21.1.8 Rule – Provide Way to Disable IPv6

Devices shall provide a way to enable and disable IPv6 traffic.

IT administrators may prefer only IPv4 traffic on their networks and prefer to disable IPv6 traffic.

This could be done by enabling/disabling the IPv6 stack, blocking all IPv6 traffic in and out using a firewall or any other suitable method.

### 21.1.9 Rule – IPv6 Enabled by Default or LCI

IPv6 traffic shall be enabled by default. LCI shall enable IPv6 if disabled.

### 21.1.10 Rule – Provide Way to Disable IPv4

Devices shall provide a way to enable and disable IPv4 traffic.

IPv6 is becoming more prevalent and users of LXI devices may want to eliminate IPv4 traffic on their network.

This could be by enabling/disabling the IPv4 stack, blocking all IPv4 traffic in and out using a firewall or any other suitable method.

### 21.1.11 Rule – IPv4 Enabled by Default or LXI

IPv4 traffic shall be enabled by default. LCI shall enable IPv4 if disabled.

## 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 compliant IPv6 protocol stacks.

IPv6 supports both "stateful" and "stateless" auto-configuration. 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 retain the device's previous address like DHCPv6 servers that are configured to be stateful.

 

## Types of IPv6 Autoconfiguration

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.

Creating a link-local address using the router assigned network prefix and a device derived unique 64-bit identifier 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. DHCPv6 servers can also be configured to do stateful address assignment or stateless assignment (SLAAC).

## 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.

## Static IP Addresses

Manual or static IP addresses can be assigned to IPv6 nodes, just like in IPv4. LXI devices need to support static addressing and provide a way to configure the different configuration settings: IPv6 IP Address, Network Prefix Length, Default gateway and optional DNS IP addresses.

## IPv6 Conformance Testing

Although devices are required to use an IPv6 compliant implementation, LXI conformance testing does not repeat a full IPv6 compliance verification.

LXI compliance testing does test certain features of IPv6 to ensure the device firmware (software) has been integrated correctly with the network stack. For example, LXI compliance testing verifies if in renewing an IP lease that all provided parameters are correctly used by the device. The LXI Conformance tests also contain tests to make sure leases do terminate and that the device shows the error via the LAN Status Indicator.

### 21.2.1 Rule – Create a Link-local address

All LXI IPv6 compliant devices shall create a unique link-local address (FE80/64).

IPv6 compliant stacks do this through IPv6 Stateless Address Autoconfiguration using the neighbor discovery messages, which are part of ICMPv6.

See the NIST IPv6 Profile, Section 4.2, *Basic Capabilities*.

### 21.2.2 Rule – Support Stateless Address Autoconfiguration (SLAAC)

LXI devices shall support IPv6 Stateless Address Autoconfiguration (SLAAC)

See the NIST IPv6 Profile, Section 4.2, *Basic Capabilities*.

### 21.2.3 Rule – Report an error if failure to renew a router advertised address

If an LXI Device is unable to renew a router advertised unicast address, then it shall report an error to the user via the LXI LAN Status Indicator.

#### *Observation – Failure to renew router assigned settings*

This rule only applies to the failure to renew router configuration information (unicast prefix and prefix length etc.). Failure to get router configuration information after a power on or a LCI (LAN reset) is not an error.

The IP address may become invalid or change due to the unicast prefix being changed. When this occurs, the following need to be updated:

- show only valid IP addresses on the LXI Web pages and front panel of the device
- stop advertising mDNS services with invalid IP addresses or update the service advertisements with the new IP addresses
- update the XML identification document with valid interfaces and IP addresses

### 21.2.4 Deprecated Recommendation – Support Router Advertisement Options for DNS Configuration

This recommendation has been deprecated in LXI Version 1.6 because it is included in compliant IPv6 LAN stacks.

### 21.2.5 Rule - Support Static IP Address Assignment

Devices shall support Static IP addressing.

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 these networks the network administrator provides the network configuration values to the device user.

LXI devices shall provide a way to enter the following parameters into the device:

- IPv6 IP Address
- Network Prefix Length
- Default gateway
- DNS IP addresses

Before using any static IP address, the device shall verify the address is not already in use.
See NIST IPv6 Profile, Section 4.2, Basic Capabilities, for IPv6 Stateless Address Autoconfiguration (SLAAC) and Duplicate Address Detection (DAD)

### 21.2.6 Rule – Support DHCPv6

Devices shall support both Stateless and Stateful DHCPv6 addressing.

#### *Observation – Stateless versus Stateful DHCPv6*

A **DHCPv6 server** configured in stateless mode does not provide IPv6 addresses at all. It only provides *other information* such as a DNS server list and a domain name. It works in conjunction with SLAAC that tells hosts how to generate global unicast addresses. In this context stateless means that **no server keeps track** of what addresses have been assigned by which hosts and what addresses are still available for an assignment.

A **DHCPv6 server** configured in stateful mode provides IPv6 addresses as well as the *other information* provided by stateless DHCP servers. The DHCP server also keeps track of the state of each assignment. It tracks the address pool availability. It also logs every assignment and keeps track of the expiration times.

The primary difference between DHCPv6 and DHCPv4 is that in IPv4 the DHCP server typically provides default gateway addresses to hosts. In IPv6, only routers sending Router Advertisement messages can provide a default gateway address dynamically.

***Observation – DHCPv6 Unique Local Addresses***

DHCPv6 servers can also assign Unique Local Addresses.

#### 21.2.6.1 Permission – DHCPv6 Waiver Requests

If the device O/S does not support DHCPv6, the vendor may request the LXI Conformance Committee to grant them a waiver.

### 21.2.7 Rule – Report an Error If Failure to Renew the DHCPv6 Lease

If an LXI Device is unable to renew its DHCPv6 lease it shall signal an error to the user via the LXI LAN Status Indicator.

***Observation – Failure to renew DHCPv6 lease***

This rule only applies to the failure to renew the DHCPv6 configuration information. Failing to get DHCPv6 server configuration information after a power on or a LCI (LAN reset) is not an error.

The IP address may become invalid or change due to the unicast prefix being changed. When this occurs, the following need to be updated:

- show only valid IP addresses on the LXI Web pages and front panel of the device
- stop advertising mDNS services with invalid IP addresses or update the service advertisements with the new IP addresses
- update the XML identification document with valid interfaces and IP addresses

### 21.2.8 Rule – Honor New DHCPv6 Options at Lease Renewal

LXI Devices shall honor new DHCPv6 options provided when renewing a lease.

***Observation – DHCPv6 Lease Renewal***

When a DHCPv6 client renews a lease or validates a current lease via a request transaction, it is possible for the DHCPv6 server to send a reply with different option values than when the prior lease information was sent.

For example, the DHCPv6 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 DHCPv6 protocol. The DHCPv6 client should honor new DHCPv6 options provided, when renewing a lease.

### 21.2.9 Rule – Selection of IP Address Configuration Modes

LXI Devices shall provide one of the following mechanisms to configure the different IP address configuration modes via the device front panel (if present) and the LXI required Web pages (see Section 21.11 for LXI Web page requirements):

- A single configuration setting that selects Automatic (implying DHCPv6 and Router Advertisement (RA)) or Manual (Static).
- Multiple configuration settings that independently enable or disable the following options:
  - Router Advertisement (RA)
  - DHCPv6
  - Static

### 21.2.10 Rule – Ability to Enable/Disable Privacy Setting

Devices shall support enabling and disabling privacy settings.

RFC 8981 describes an extension to IPv6 Stateless Address Autoconfiguration that causes hosts to generate temporary addresses with randomized interface identifiers (IID's) for each prefix advertised with autoconfiguration enabled. RFC 8981 obsoletes RFC 4941 which previously referred to this as privacy settings. LXI refers to this as privacy settings for backward compatibility reasons.

For further information please read the SLAAC RFCs for privacy extensions in the NIST IPv6 Profile.

### 21.2.11 Rule – Privacy Setting Enabled by Default or LCI

The privacy setting shall be enabled by LCI and be enabled by default.

## 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 reachability scopes (link-local, unique-local or global). IPv6 addresses may also be marked as "preferred" or "deprecated" - see the definition of "IPv6 Address Lifetimes" – in the section "Technical Terms" for more information on this.

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.

For further information see the NIST IPv6 Profile, Section 4.7.1 - Definition of Addressing Capability Requirements

The rules, recommendations and permissions in this section refer to displaying IPv6 addresses. Devices satisfy these requirements if the address is viewable on the LXI Welcome page and viewable from the front panel of the device if the device has a front panel. See section 21.11 for more information on the IPv6 requirements for the LXI web page(s).

***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.

### 21.3.1 Rule – Display Link-local Address

Devices shall display the preferred link-local address on the front panel display, if present, and the Welcome web page.

An IPv6 link-local address will have a network prefix of: FE80::/64 which corresponds to IPv4 169.254.0.0/16 addresses.

### 21.3.2 Rule – Display Stable Addresses

Devices shall display at least one stable global or unique-local address if it has one. For the definition of *stable address* see the Technical Terms section of this document.

### 21.3.3 Permission – To show all IPv6 assigned addresses

The vendor may choose to show all IPv6 assigned addresses.

This may confuse the user as to which IP address they should use.

Deprecated addresses should not be used for new connections. If a deprecated address is shown then the display shall indicate that it is deprecated.

## 21.4 Name Resolution

IPv6 IP addresses are rather unwieldy and difficult for humans to remember therefore LXI requires name resolution protocols such as DNS and multicast DNS (mDNS).

### 21.4.1 Rule - Support Multicast DNS

LXI IPv6 capable devices shall implement multicast DNS. All the rules and recommendations for mDNS and DNS-SD in the LXI Device specification, section 10 apply to IPv6 devices. See LXI Device Specification, sections 10.3-10.8 for more information.

***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

Devices shall support mDNS on IPv6-only networks.

Devices are only required, at a minimum, to use mDNS for link-local address scoping (FF02/16) on IPv6 networks.
Refer to RFC 6762 and RFC 6763 for more information

### 21.4.3 Recommendation – Send AAAA DNS Records over IPv4

If IPv6 and IPv4 are enabled on a given interface, then 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 as AAAA records over IPv4 if IPv4 is enabled 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 enabled 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 additional network infrastructure or protocols.
>
> Generally, a device doesn't have permission to update a DNS registry due to security reasons, so LXI doesn't specify that a device can update a DNS registry but only that it updates the DNS via a DHCPv6. 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 hostname used for dynamic naming services, such as mDNS. The single module hostname shall be a legal DNS name.

See LXI Device Specification, section 8.9 for more information.

### 21.4.5 Rule – Provide Manual DNS IP Address Entry

LXI Devices shall 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 DHCPv6 configuration information. This is useful in network environments with a DNS server per department and a DHCPv6 server per site.

### 21.4.6 Recommendation - Provide DNSv6 Client Capability

Devices should support DNSv6 client for resolving hostnames.

See the NIST IPv6 profile, Section 4.11, Network Support Capabilities for the RFCs about DNS-Client. Especially the RFC for DNS Extensions to Support IP Version 6.

 

***Observation – DNS Client Usage***

**Hostname Lookup Support**

The previous section discussed how to make a device reachable as a server via a hostname. This section discusses the ability of the device to become a client in the network running things like a Web browser. This capability may not be used on all devices because they have little need to act as a client on the network.

### 21.4.7 Rule - Provide way to Disable mDNS and DNS-SD for IPv6

Devices shall provide a way to enable and disable mDNS and DNS-SD for IPv6.

### 21.4.8 Permission – To provide a single mDNS and DNS-SD disable control

LXI Device Specification, Rule 10.5.2 requires a way to enable and disable mDNS and DNS-SD for IPv4. Devices may have a single setting to enable and disable mDNS and DNS-SD for IPv4 and IPv6

### 21.4.9 RULE – mDNS and DNS-SD Enabled by LAN Configuration Initialize (LCI)

When the LCI reset mechanism is activated, it shall enable mDNS and DNS-SD for IPv4 and IPv6.

***Observation – Disabling mDNS and DNS-SD***

mDNS is re-enabled when the LCI is activated because mDNS and DNS-SD are useful in locating devices on the LAN. The primary reason for disabling mDNS and DNS-SD is to suppress service announcement traffic which some IT organizations consider to be a security risk.

## 21.5 ICMPv6 Echo Reply (Ping)

### 21.5.1 Rule – ICMPv6 Echo Reply

LXI Devices shall support ICMPv6 (Internet Control Message Protocol) Echo Reply.

See the NIST IPv6 Profile, for the RFCs about ICMPv6.

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.

### 21.5.2 Recommendation – Support Echo 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).

The command: ping -6 FF02::FB%ScopeId provides a convenient way to find all the mDNS devices on the local link.

### 21.5.3 Rule– Provide Way to Disable ICMPv6 Echo Reply Message

LXI devices shall have a way to enable and disable the ICMP Echo Reply messages.

#### *Observation – Disabling ICMP Echo Reply in Windows*

Microsoft has several articles on using the Windows Firewall to enable/disable the echo reply message. By default, in Windows 7, 10 and 11 the reply to an echo request is disabled.

### 21.5.4 Rule – ICMPv6 Echo Reply Enabled by Default or LCI

The echo reply service shall be enabled by default. LCI will enable the echo reply service if it is disabled.

### 21.5.5 Recommendation – Support ICMPv6 Echo Request message (Ping Client)

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

#### *Observation – Ping Client Usage*

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

## 21.6 Rule – Static Duplicate IP Address Detection

If a duplicate address is detected, the Device shall 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 DHCPv6, Router Advertisement (RA) or 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 DHCPv6 configured systems are unlikely but they are possible. The DHCPv6 specification specifies how a duplicate IP address check should be done within the DHCP SOLICIT/ADVERTISE/REQUEST/CONFIRM protocol sequence. For the relevant RFCs on DHCPv6 see the NIST IPv6 Profile.

## 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:

- Detection of a duplicate IP address
- Failure to renew an already acquired auto-configured lease (Router Advertisement (RA) or DHCPv6) lease. Note that failure to obtain an "initial" RA or DHCPv6 lease is not a failure.
- LAN cable disconnected (as reported by Ethernet connection monitoring)

See LXI Device Specification, Section 2.5.2, 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 LXI Device Specification, section 2.5.2. This identifying indication is initiated by the user via the Web interface. See LXI Device Specification, section 9.3, and LXI Device Specification, 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 (Figure 21.2). Note that the state labeled "State Undefined" is transitory and the behavior of the indicator is not specified.

If the LXI Device has a valid stable address and the lease can't be renewed, then the LAN Status Indicator shall show a fault.

There are two scenarios that play out when dealing with the IPv6 address assignment process:

1) After power up or a LAN reset, if a device is configured for both DHCPv6 and Router Advertisement 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 IPv6 address, be it via DHCPv6 or SLAAC. However, at a later time if the device fails to renew that lease, then per rule 21.2.3 or 21.2.7 of this specification the device must stop using the IP Address it had obtained for any new connections, and the LAN Status Indicator must indicate a fault. This is to indicate to the user that an Autoconfiguration IPv6 address assignment renewal has failed, and that the device does not have the same IPv6 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 IPv6 address. (This can happen if it is configured to periodically attempt to obtain a new IPv6 address).

   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 DHCPv6 fails but a SLAAC address is obtained or vice versa, the LAN Status is no fault.

 

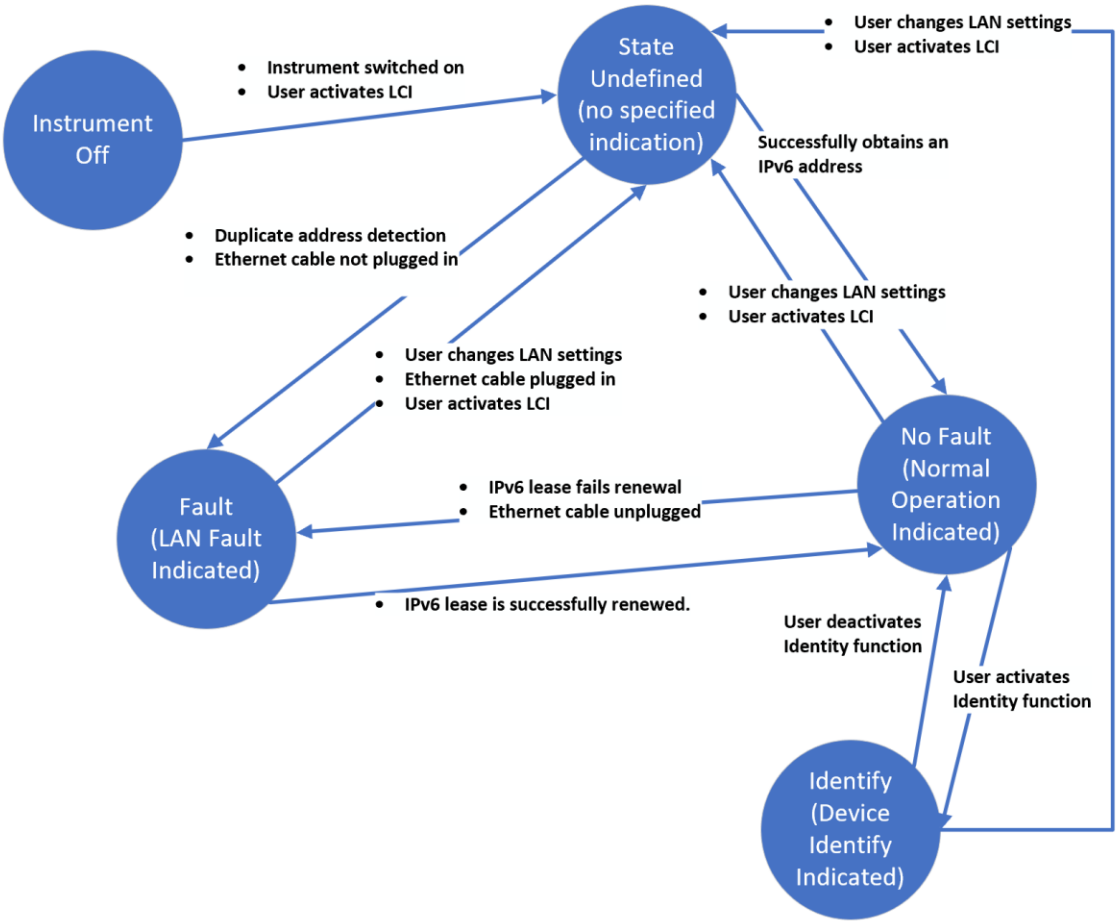


**Figure 21.2**

### 21.8.1 Rule – Combined IPv4 and IPv6 LAN Status Indicator

As per rule LXI Device Specification, section 2.5.2, there shall be at least one LAN Status Indicator, which conforms to the combined IPv4 state diagram in LXI Device Specification, section 8.10 and the IPv6 state diagram shown above.

There are three scenarios:

1. If only the IPv4 stack is enabled, then the status indicator shall conform to LXI Device Specification, section 8.10 only.

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

3. If both the IPv4 and IPv6 stacks are enabled, then the following apply:

 

a. If a LAN cable is not plugged in or the device is not connected to an Ethernet LAN, then this may be an error. See 21.8.6, *Permission – To show no fault if the LAN is inactive*.

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

c. If from power up or after an LCI 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 in which case the IPv6 stack would get an address and the IPv4 stack would not.

d. If from power up or after a LAN reset both stacks get IP addresses and then when either attempts to renew their leases and either 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 LCI or power-cycle the device for the error to be cleared as in 3c.

### 21.8.2 Rule – IPv6 Link-Local address only 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 it is to be expected that there may be no DHCPv6 server, nor router, configured to solicit the network prefix, so only a link-local address is expected behavior.

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

Devices may have separate LAN Status Indicators for IPv4 and IPv6 as long as the IPv4 indicator follows all rules in LXI Device Specification, section 8.10 and the IPv6 indicator follows the IPv6 rules in this section of the specification.

### 21.8.4 Recommendation – Ability to configure the LAN Status Indicator

Devices should have a way to configure the LAN Status Indicator to show faults from only the IPv4 or IPv6 stack. An alternative way to do this is to enable or disable the IP stacks – see Rules **21.1.7, 21.1.9 and 21.11.7**

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

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

### 21.8.6 Permission – To show no fault if the LAN is inactive

A LAN status indicator showing a fault when the LAN is inactive can be disconcerting to users when using the front panel display or using another Command-and-Control interface like USB.

LXI device manufacturers may show no fault on the Status Indicator when the LAN cable is not plugged. See LXI Device Specification, Permission 8.10.1.

## 21.9 Rule – LAN Configuration Initialize (LCI)

LXI Devices shall provide an LCI mechanism, as defined in the LXI Device Specification – section 2.4.5 that when activated places the LXI Device's network settings into a known 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 LCI reset mechanism may affect settings not called out by LXI that enable the customer to re-establish network communication with the device. The LXI Device LCI 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 | 21.1.9 & 21.11.7 |
| IPv6 stack | Enabled | 21.1.7 & 21.11.7 |
| IPv6 Address Configuration:<br>1. Router Advertisement<br>2. DHCPv6<br>3. Static | <br>1. Enabled<br>2. Enabled<br>3. Enabled | Section 21.2.9 |
| Privacy Setting | Enabled | 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 | Default<br><br>LXI Security Extended Function obviates this setting | LXI Device Specification, Section 9.8 |
| mDNS and DNS-SD | Enabled | Sections: LXI Device Specification, sections: 10.3, 10.4, 10.7.1 & Rule 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 device could simply be forgotten. Therefore, a simple mechanism, such as pressing the recessed rear panel LCI mechanism to force the LXI Device's network settings to a known state, is beneficial.

## 21.10 Optional Protocols and Features

This section of the specification lists IPv6 protocols or features that may be of interest to LXI devices.

### 21.10.1 Observation – IP Layer Security (IPSec)

IPSec may be part of a 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.

The RFCs for IPSec are in the NIST IPv6 Profile but are optional for a IPv6 compliant stack.

### 21.10.2 Observation - 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. Mobile IPv6 is not in the NIST Profile document so see RFC 6275 – Mobility Support in IPv6

## 21.11 IPv6 Web Page Requirements

This specification has some additional requirements on the LXI specified Web pages in section 9 of the LXI Device Specification.

### 21.11.1 Rule – Implement all Rules in the Web Interface Section

Implement all the LXI Device specification Rules in Section 9 – Web Interface of the Device Specification except:

- devices shall not include a subnet mask for IPv6 configuration
- devices should follow 21.2.9, *Rule – Selection of IP Address Configuration Modes*

### 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 Link-Local and Stable IPv6 Addresses on Welcome Web Page

Add the following information to the LXI Welcome Page:

- IPv6 Link-Local Address
- If available show at least one stable global or unique-local address. For the definition of *stable address* see the Technical Terms section of this document.

See LXI Device Specification, section 9.2, *LXI Welcome Page.*

### 21.11.4 Recommendation – Use one LAN Configuration Page

LXI Device Specification, Section 9.5, describes the information that needs to be present to configure an IPv4 device.
Devices should add the IPv6 LAN Configuration information required in this section to the LAN Configuration page.

This combined page must have everything stated in LXI Device Specification, section 9.5 for the IPv4 configuration and everything in section 21.11, *IPv6 Web Page Requirements.*

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

Devices are permitted to have separate IPv4 and IPv6 configuration pages.

If two pages are used, two links shall be present on the LXI Welcome Page (1) to an IPv4 configuration page and (2) to an IPv6 configuration page.

The links shall be clearly labeled IPv4 Configuration and IPv6 Configuration respectively.

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

LXI Device Specification, 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.

For Static IP Mode, on IPv6, then the following settings shall be on the IP Configuration Page and configurable by the user of the device:

- IPv6 Configuration Mode[4]
- IPv6 address [5]
- Prefix Length
- Default Gateway[6]
- DNS Server(s)[7]

The IPv6 Configuration Mode field controls how the IP address for the instrument is assigned. See Rule 21.2.9 for more information on this setting.

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 Rule – Add a Stack Disable Option to the Configuration Mode.

Devices shall have independent options to disable IPv4 and IPv6.

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

### 21.11.8 Rule – Display of Status for Disabled IP Protocols

The following rules shall be followed when displaying the status of disabled IP Protocols:

1) The configuration display of disabled IP protocols shall show the various configuration fields for IPv4 or IPv6.

2) The configuration display of disabled IP protocols shall show the IPv4 or IPv6 Configuration Mode, and show either the text “Disabled”, the text “-“, or a blank field in place of the IP address when the corresponding IP 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.

For example, some of the following extended functions could be supported on IPv4 only but if they are supported on IPv6 then list them as shown:

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

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

## 21.12 LXI Clock Synchronization Changes

This section has additional rules and recommendations for devices that implement LXI Clock Synchronization.

### 21.12.1 Rule – Devices with IPv6 Clock Synchronization Shall Conform with Section 21.12

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

All LXI IPv6 conformant devices that implement the LXI Clock Synchronization extended function shall conform with the rules in this section in addition to the requirements regarding LXI Clock Synchronization in the LXI Device specification and the LXI Clock Synchronization Extended Function.

### 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 be used.

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

This section contains rules and recommendations regarding support of LXI Event Messaging over IPv6.

### 21.13.1 Rule – Devices that Implement IPv6 LXI Events Shall Conform with Section 21.13

All LXI IPv6 compliant devices that implement the LXI Event Messaging extended function shall conform with the rules in this section in addition to the requirements regarding LXI Event Messaging in the LXI Device specification and the LXI Event Messaging Extended Function.

### 21.13.2 Rule – Use IPv6 Multicast Address and Port Number

Devices that implement IPv6 LXI Event Messaging 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 shall be 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 specification defines destination paths and filters that may contain IP addresses, called ‘host numbers’ in the IviLxiSync Specification.

Devices that support IPv6 LXI Events shall have IVI drivers that accept IPv6 addresses inside ***square brackets*** (“[“ and “]”) in the IviLxiSync interface 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 Rule - LAN Discovery and Identification Changes

IPv6 devices shall include a *NetworkInformation* element in their LXI Identification response that describes the IPv6 network configuration as specified in the *LXI API Extended Function.*

### *Observation – No VXI-11 for IPv6*

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.