LXI Consortium

LXI Test Procedure Definition

1.6

2024/01/12

1.0 Overview

Categories: General Device

1.4.1.2.5 LXI Clock Synchronization Conformance Requirements

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: LXI Clock Synchronization Conformance Requirements

Explanation: The rules in this document define the conformance requirements for this Extended Function. In addition to the requirements for all LXI Devices found in the LXI Device Specification, there may be cases where an Extended Function requires conformance to another Extended Function. All requirements follow below:

LXI Device Specification Document:

- All LXI Devices shall conform to the rules found in Section 1.4 and all subsections
- All LXI Devices shall conform to the rules found in Section 1.4 and all subsections
- Section 6.1.1 and 6.5 including all subsections
- Section 9.6 including all subsections
- Function element with the FunctionName attributes of “LXI Clock Synchronization” and version “1.0” in the LXIExtended Function element of the LXI identification document as described in section 10.2.5.

LXI Clock Synchronization (this document):

- Include all rules

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

1.4.6	LXI Clock Synchronization

1.4.4.2.3 LXI Wired Trigger Bus Conformance Requirements

Category: LXI Wired Trigger Bus

Test Type: Kerberos Test, automated

Rule: LXI Wired Trigger Bus Conformance Requirements

Explanation: All LXI Devices shall conform to the rules found in Section 1.4 and all subsections, Sections 3.5 and 3.7, including all subsections, Section 6.1.1, sections 6.3 , through 6.4.2 including all subsections, and 6.4.4 through 6.4.6, including all subsections, Section 9.6 including all subsections. A Function element with the FunctionName attributes of LXI Wired Trigger Bus and version 1.0 in the LXIExtendedFunction element of the LXI identification document as described by section 10.2.5, LXI Wired Trigger Bus Extended Function Include all rules

Test Procedure: NOT SUPPORTED

This test is currently not implemented. If the configuration would expect this test to run, then it will fail. Otherwise it will pass with message 'not supported'.

1.4.4.2.6 LXI Timestamped Data Conformance Requirements

Category: LXI Timestamped Data

Test Type: Kerberos Test, automated

Rule: LXI Timestamped Data Conformance Requirements

Explanation

The rules in this document define the conformance requirements for this Extended Function. In addition to the requirements for all LXI Devices found in the LXI Device Specification, there may be cases where an Extended Function requires conformance to another Extended Function. All requirements follow below:

LXI Device Specification Document:

- All LXI Devices shall conform to the rules found in Section 1.4 and all subsections
- A Function element with the FunctionName attributes of “LXI Timestamped Data” and version “1.0” in the LXIExtendedFunction element of the LXI identification document as described by section 10.2.5.

LXI Clock Synchronization Document:

- Include all rules

LXI Timestamped Data (this document):

- Include all rules

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies

1.4.6	LXI Clock Synchronization	LXI Timestamped Data

1.4.4.2.7 LXI Event Log Conformance Requirements

Category

LXI Event Log

Test Type

Kerberos Test, automated

Rule

LXI Event Log Conformance Requirements

Explanation

All LXI Devices shall conform to the rules found in Section 1.4 and all subsections, Section 3.7 including all subsections. A Function element with the FunctionName attributes of “LXI Event Log” and version “1.0” in the LXIExtendedFunction element of the LXI identification document as described by section 10.2.5. LXI Clock Synchronization Document If using non-zero time-stamped events, then include all rules. LXI Event Includes all rules

Test Procedure

NOT SUPPORTED

This test is currently not implemented. If the configuration would expect this test to run, then it will fail. Otherwise it will pass with message 'not supported'.

1.4.6 Web Indication of Functional Declaration

Category

Web Interface, Device Specification

Test Type

Kerberos Test, manual

Rule

Web Indication of Functional Declaration

Explanation	The Functional Declaration shall be declared on the web interface and is the definitive source for Functional Declaration information for an LXI Device. See section 9.2, RULE – Welcome Web Page Display Items for additional requirements regarding this page. It shall include: **LXI Version:** 1.6 LXI Device Specification 2022 **LXI Extended Functions:** List of supported LXI Extended Functions using the extended function names as defined in each LXI Extended Function specification (example: LXI HiSLIP). The web page shall list all the LXI Extended Functions supported.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Query Functional Declarations Query tester for the functional declarations given on the Welcome Page. Validate Functional Declaration Match the Functional Declaration and Extended Function tags given by user against the test configuration.

1.4.7 Terms Using the LXI Trademark

Category	Device Specification
Test Type	Vendor Declaration
Rule	Terms Using the LXI Trademark
Explanation	The LXI Trademark or registered name, LXI, shall be used to describe the LXI Device and any LXI Extended Function

2.0 LXI Physical Specification

Categories: General Device

2.4.5.1 LCI Mechanism

Category: General Device, Device Specification

Test Type: Kerberos Test, manual

Rule: LCI Mechanism

Explanation: LXI Devices shall provide an LCI Mechanism that, when activated, places its network settings in a default state. The functions performed by this mechanism are defined in Section 8.13.

Test Procedure: Query LCI Mechanism

Query tester if an LCI mechanism is found on the device.
This may be either a physical button or switch or a soft implementation in the the device's user interface.

2.4.5.2 LXI Devices Without a Front-Panel Manual Data-Entry Method

Category: General Device, Device Specification

Test Type: Kerberos Test, manual

Rule: LXI Devices Without a Front-Panel Manual Data-Entry Method

Explanation: LXI Devices shall provide an LCI mechanism by either:

a) A separate recessed mechanical LCI mechanism on the rear or front of the device (rear is preferred).

b) A soft LCI mechanism through a permanently attached user interface (e.g., a front panel, monitor, mouse, keyboard, et cetera) that does not use the LAN as the interface.

Test Procedure: Query LCI Mechanism Without Front-Panel

Query tester if the LCI Mechanism is available for devices without a front panel manual data entry method.

2.4.5.3 LCI Mechanism Protection

Category: General Device, Device Specification

Test Type: Kerberos Test, manual

Rule: LCI Mechanism Protection

Explanation: The LCI Mechanism shall be protected by a time-delay, user query, or mechanical protection feature designed to prevent inadvertent operation.

Test Procedure: Query LCI Mechanism Protection

Query tester if the LCI Mechanism is protected by a time-delay, user query or mechanical protection feature designed to prevent applying the LCI unintentionally.

2.4.9.1 IEEE 802.3

Category: General Device, Device Specification

Test Type: Kerberos Test, manual

Rule: IEEE 802.3

Explanation: Physical Ethernet connections shall be IEEE 802.3 compliant.

Test Procedure	Query Physical Ethernet connection Query tester if the device has a RJ45 connector which accepts a standard LAN cable.

2.5.1.1 Power Indicator

Category	General Device, Device Specification
Test Type	Kerberos Test, manual
Rule	Power Indicator
Explanation	A Power Indicator shall be provided on the front panel of the device.
Test Procedure	Query Power Indicator Query tester if the device has a power indicator on its front panel.

2.5.2.1 LAN Status Indicator

Category	General Device, Device Specification
Test Type	Kerberos Test, manual
Rule	LAN Status Indicator
Explanation	A LAN Status Indicator shall be provided on the device front panel.
Test Procedure	Query LAN Status Indicator Query tester if the device has a LAN status indicator on the front panel. It may be on the user interface. A permission also allows it to be on the rear panel.

2.6.1.1 Front Panel Labeling Requirements

Category	General Device, Device Specification
Test Type	Kerberos Test, manual
Rule	Front Panel Labeling Requirements
Explanation	There shall be an LXI Logo on the front of the device. The logo shall conform to the specifications in the document 'LXI Consortium Trademark, Patent and Licensing Policies.'
Test Procedure	Query LXI logo Query tester if the LXI logo is on the front panel. It may also be displayed as part of the power up display.

3.0 LXI Device Synchronization and Events

Categories: LXI Clock Synchronization LXI Event Messaging LXI Wired Trigger Bus

3.2.1 Implementation of IEEE 1588 Precision Time Protocol

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Implementation of IEEE 1588 Precision Time Protocol

Explanation: Each LXI Device that implements IEEE 1588 shall provide functionality fully conformant to the standard IEEE 1588 and the LXI 1588 Profile.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

3.2.1.0	3.2.1.1	3.2.1.2
3.2.1.3	3.2.1.4	3.2.1.5
3.2.1.6	3.2.1.7	3.2.1.8
3.2.1.9	3.2.1.10	3.2.1.11
3.2.1.12	3.2.1.13	3.2.1.15
3.2.1.16	3.2.1.17	

3.2.1.0 Target Address

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Target Address

Explanation: IEEE 1588 clocks in an LXI Device shall implement the IEEE 1588 management messages specified in clause 15.2 of IEEE 1588-2008. This test checks various target address settings.

Pre Condition: Connect DUT

Connect the DUT to the test network

Start management node

Start up the PTP management node

Test Procedure: Test management address settings

Test various management message address settings, where the DUT should or should not answer.

Target Clock Identity	Target Clock Port	Expect Response
DUT Identity	DUT Port	Yes
DUT Identity	0xFFFF	Yes
ff:ff:ff:ff:ff:ff:ff:ff	DUT Port	Yes
ff:ff:ff:ff:ff:ff:ff:ff	0xFFFF	Yes
DUT Identity	Random	No
ff:ff:ff:ff:ff:ff:ff:ff	Random	No
00:00:00:00:00:00:00:00	0xFFFF	No
Random	0xFFFF	No

Post Condition: Shutdown management node

Shutdown the PTP management node

3.2.1.1 Management Messages

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Management Messages
Explanation	IEEE 1588 clocks in an LXI Device shall implement the IEEE 1588 management messages specified in clause 15.2 of IEEE 1588-2008. This test checks the GET/SET/CMD action for all neccessary management messages. Management messages associated with IEEE 1588-2008 optional clauses that are NOT required are NOT tested.
Pre Condition	Connect DUT Connect the DUT to the test network Start management node Start up the PTP management node
Test Procedure	Test management messages Test the correct functionality of the management messages for their GET/SET/CMD action.
Post Condition	Shutdown management node Shutdown the PTP management node

3.2.1.2 Default best master clock algorithm

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Default best master clock algorithm
Explanation	LXI Devices shall determine the master-slave hierarchy using the IEEE 1588 specified default best master clock algorithm, clauses 9.3.2, 9.3.3, and 9.3.4, of IEEE 1588-2008.
Pre Condition	Connect DUT Connect the DUT to the test network Start management node Start up the PTP management node Start ordinary clock Start up the PTP clock Initialize all clocks Send a management message INITIALIZE to all clocks. Get Clock Quality from DUT Get the Default Data Set by sending a DEFAULT_DATA_SET management message to the DUT. Extract the Clock Quality from response. Get Announce Interval from DUT Get the Log Announce Interval by sending a LOG_ANNOUNCE_INTERVAL management message to the DUT. Extract the Log Announce Interval and calculate the announce interval.

Test Procedure	Test BMC algorithm	
		Test the best master clock algorithm (BMC) by changing the clock quality and the priority of the dut, to introduce the different BMC states • priority1 • clock class • clock accuracy • offset scaled log variance • priority2
Post Condition	Shutdown management node	
		Shutdown the PTP management node
	Shutdown ordinary clock	
		Shutdown the PTP clock

3.2.1.3 Test BMC related timeout ANNOUNCE_RECEIPT_TIMEOUT event

Category	LXI Clock Synchronization	
Test Type	Kerberos Test, automated	
Rule	Test BMC related timeout ANNOUNCE_RECEIPT_TIMEOUT event	
Explanation	The test first examines the DUT in the slave state by causing the PC Clock to cease sending Announce messages to the DUT (by moving the PC Clock to a different domain) and observing how long it takes for the DUT to start sending Announce messages. The test then examines the DUT in the listening state by first initializing it and then observing how long it takes to start Announce messages given that there are no other clocks in the domain.	
Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Start ordinary clock	
		Start up the PTP clock
	Start management node	
		Start up the PTP management node
	Initialize all clocks	
		Send a management message INITIALIZE to all clocks.
Test Procedure	Get Announce Interval from DUT	
		Get the Log Announce Interval by sending a LOG_ANNOUNCE_INTERVAL management message to the DUT. Extract the Log Announce Interval and calculate the announce interval.
	Get Announce receipt timeout from DUT	
		Get the Announce receipt timeout by sending a ANNOUNCE_RECEIPT_TIMEOUT management message to the DUT. Extract the Announce receipt timeout value.
	Set DUT to Slave	
		Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Test master stops	
		Disable the local clock, calculate the announce receipt timeout from the timestamps of the last announce message send from the local clock and the first announce message sent from the DUT. Match this against the DUT's configured announce receipt timeout.

Test after initializing

Local clock is disabled. Send an INITITALIZE management message to the DUT, calculate the announce receipt timeout from the timestamps of the Initialize response message and the first announce message sent from the DUT. Match this against the DUT's configured announce receipt timeout

Test when master does not keep to threshold

Enable local clock with an announce interval larger than the announce receipt timeout of the DUT. Wait several announce intervals and expect the DUT to act as master, because the announce intervals of the local clock are to long.

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.4 Ignore irrelevant messages

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Ignore irrelevant messages

Explanation: There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the following of these:

- versionPTP: Discard versions >2 18.1, translate version 1 optional 18.2(not required by LXI).
- domainNumber: Discard messages from a different domain, 9.5.1
- alternateMasterFlag: Discard messages with this flag TRUE, 9.1 and LXI Profile 2.10.1, 9.3.2.2 for Announce,
- Delay_Resp message not from current master or not associated with a Delay_Req from the slave clock: Discard, 9.5.7

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies

3.2.1.4.1	3.2.1.4.2	3.2.1.4.3
3.2.1.4.4	3.2.1.4.5	3.2.1.4.6
3.2.1.4.7		

3.2.1.4.1 Ignore irrelevant version messages

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Ignore irrelevant version messages

Explanation: There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the versionPTP: Discard versions

Pre Condition

Connect DUT

Connect the DUT to the test network

Start management node

Start up the PTP management node

Start ordinary clock

Start up the PTP clock

Start device 2 ordinary clock

Start up the PTP clock of device 2.

Initialize all clocks

Send a management message INITIALIZE to all clocks.

Set DUT to Slave

Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)

Set Device2 to 2nd in line

Set the device2 priority so that it is second in line to become master. For example local clock priority 0, DUT priority 128, then set Device2 to 45.

Test Procedure

Set local PTP version

Change the local PTP version away from Version 2

Change local clock time

Set the local clock time to a different value then the current time, to see if the DUT keeps to the local clock time or not.

Ensure DUT is Slave

Wait for the DUT to be slave and the local clock master.

Is Device 2 master of DUT

Check if the DUT has accepted Device 2 as master.

Is Device 2 time the time of DUT

Check if the DUT's time is close to the Device 2 time.

Discard Management messages

Check if the DUT is discarding management messages. Send a management message to the DUT with wrong PTP version which should not get a response as wrong PTP versions shall be discarded.

Repeat Version test steps

Repeat the test steps for following PTP versions:

- PTP Version 1
- PTP Version 3

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown device 2 ordinary clock

Shutdown the PTP clock of device 2.

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.4.2 Ignore irrelevant messages from alternate master

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule	Ignore irrelevant messages from alternate master
Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the alternateMasterFlag: Discard messages with this flag TRUE, 9.1 and LXI Profile 2.10.1, 9.3.2.2 for Announce
Pre Condition	Connect DUT Connect the DUT to the test network Start management node Start up the PTP management node Start ordinary clock Start up the PTP clock Start device 2 ordinary clock Start up the PTP clock of device 2. Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128) Set Device2 to 2nd in line Set the device2 priority so that it is second in line to become master. For example local clock priority 0, DUT priority 128, then set Device2 to 45.
Test Procedure	Enable alternate master flag Enable the alternate master flag on the local clock. Other clocks should now stop using the local clock as master. Change local clock time Set the local clock time to a different value then the current time, to see if the DUT keeps to the local clock time or not. Ensure DUT is Slave Wait for the DUT to be slave and the local clock master. Is Device 2 master of DUT Check if the DUT has accepted Device 2 as master. Is Device 2 time the time of DUT Check if the DUT's time is close to the Device 2 time.
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown device 2 ordinary clock Shutdown the PTP clock of device 2. Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.4.3 Ignore irrelevant Delay Resp messages

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Ignore irrelevant Delay Resp messages

Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the Delay_Resp message not from current master or not associated with a Delay_Req from the slave clock: Discard, 9.5.7
Pre Condition	Connect DUT Connect the DUT to the test network Start management node Start up the PTP management node Start ordinary clock Start up the PTP clock Start device 2 ordinary clock Start up the PTP clock of device 2. Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128) Set Device2 to DUT priority Set the device2 priority to the same priority as the DUT.
Test Procedure	Check device 2 correction field influence on message: DELAY RESP Set the correction field value for DELAY_RESP messages to device 2. The meanPathDelay of the DUT should not be influenced by this. Set Device2 to local clock priority Set the device2 priority to the same priority as the local clock. Set local clock to receive only DELAY_REQ Modify the local clocks behaviour to only receive DELYA_REQ messages. Simulate device 2 DELAY RESP Modify the local clock to simulate device 2 DELAY_RESP messages and set the correction field. The DUT should not accept these messages, therefore the meanPathDelay should stay stable. Send DELAY RESP as master Send only delay resp messages to the DUT acting as regular master and set the correction field. The DUT should not accept these messages as local clock is not master, therefore the meanPathDelay should stay stable.
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown device 2 ordinary clock Shutdown the PTP clock of device 2. Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.4.4 Ignore irrelevant Follow Up messages

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated

Rule	Ignore irrelevant Follow Up messages
Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the Follow Up message not from current master
Pre Condition	Connect DUT Connect the DUT to the test network Start management node Start up the PTP management node Start ordinary clock Start up the PTP clock Start device 2 ordinary clock Start up the PTP clock of device 2. Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128) Set Device2 to local clock priority Set the device2 priority to the same priority as the local clock.
Test Procedure	Set local clock to send only FOLLOW_UP Modify the local clocks behaviour to only send FOLLOW_UP messages. Send FOLLOW_UP as master Send only follow_up messages to the DUT acting as regular master and set the correction field. The DUT should not accept these messages as local clock is not master, therefore the meanPathDelay should stay stable. Simulate device 2 FOLLOW_UP Modify the local clock to simulate device 2 FOLLOW_UP messages and set the correction field. The DUT should not accept these messages, therefore the meanPathDelay should stay stable.
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown device 2 ordinary clock Shutdown the PTP clock of device 2. Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.4.5 Ignore irrelevant Delay Req messages

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Ignore irrelevant Delay Req messages
Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the Delay req messages received when not being master.

Pre Condition	Connect DUT
	Connect the DUT to the test network
	Start management node
	Start up the PTP management node
	Start ordinary clock
	Start up the PTP clock
	Start device 2 ordinary clock
	Start up the PTP clock of device 2.
	Initialize all clocks
	Send a management message INITIALIZE to all clocks.
	Set DUT to Slave
	Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Set Device2 to DUT priority
	Set the device2 priority to the same priority as the DUT.
Test Procedure	Check for DUT DELAY_RESP messages
	Check if the DUT is sending any DELAY_RESP messages. DUT should not be sending any DELAY_RESP messages as it is in state Slave.
Post Condition	Reset local clock
	Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown device 2 ordinary clock
	Shutdown the PTP clock of device 2.
	Shutdown ordinary clock
	Shutdown the PTP clock
	Shutdown management node
	Shutdown the PTP management node

3.2.1.4.6 Ignore irrelevant messages in Disable state

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Ignore irrelevant messages in Disable state
Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the messages to be discarded when device is in DISABLE state.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Start management node
	Start up the PTP management node
	Start ordinary clock
	Start up the PTP clock
	Start device 2 ordinary clock
	Start up the PTP clock of device 2.
	Initialize all clocks
	Send a management message INITIALIZE to all clocks.

	Set DUT to Slave	
		Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Set Device2 to DUT priority	
		Set the device2 priority to the same priority as the DUT.
Test Procedure	Disable DUT	
		Send a DISABLE_PORT management message to the DUT to disable the clock.
	Check for DUT messages	
		Check if the DUT is sending any messages. THe DUT is disabled therefore we expect no messages to be found.
Post Condition	Reset local clock	
		Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown device 2 ordinary clock	
		Shutdown the PTP clock of device 2.
	Shutdown ordinary clock	
		Shutdown the PTP clock
	Shutdown management node	
		Shutdown the PTP management node

3.2.1.4.7 Ignore irrelevant messages with undefined TLV

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Ignore irrelevant messages with undefined TLV
Explanation	There are several sections of IEEE 1588 that specify conditions under which a clock disregards all or part of a received PTP message. This test covers the messages with undefined TLV.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Start management node
	Start up the PTP management node
	Start ordinary clock
	Start up the PTP clock
	Start device 2 ordinary clock
	Start up the PTP clock of device 2.
	Initialize all clocks
	Send a management message INITIALIZE to all clocks.
	Set DUT to Slave
	Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Set Device2 to Slave
	Set the device2 priority to a very low priority value (e.g. 255).
Test Procedure	Append Invalid TLV
	Append invalid TLV to all messages of the local clock.

Check Slave offset is reasonable

Get the offset of the slave by sending a CURRENT_DATA_SET management message to the slave. Check if the offset is reasonable.

Set DUT to Master

Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.

Check Slave offset is reasonable

Get the offset of the slave by sending a CURRENT_DATA_SET management message to the slave. Check if the offset is reasonable.

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown device 2 ordinary clock

Shutdown the PTP clock of device 2.

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.5 Honor Delay_Req inter-message interval

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Honor Delay_Req inter-message interval

Explanation: In its Delay_Resp messages, the master tells slaves how frequently slaves are allowed to send Delay_Req messages. The master sends the minimum average inter-message time (strictly, the log2 of this time) in the Delay_Resp messages. Slaves may send slower than that, but not faster. Slaves are required to make a fresh random choice of time for each message, while honoring this minimum. If they choose to set their average to the minimum allowed, the interval over which they choose random inter-message times is [0, 2t] seconds, where t is the time published by the master. 9.5.11.2

This test is conducted for two values of the expected intervals to verify that the slave correctly responds to different values.

Pre Condition

Connect DUT

Connect the DUT to the test network

Start ordinary clock

Start up the PTP clock

Start management node

Start up the PTP management node

Initialize all clocks

Send a management message INITIALIZE to all clocks.

Test Procedure

Get Min Delay Request Interval from DUT

Get the Port Set by sending a PORT_DATA_SET management message to the DUT.
Extract the Log Min Delay Req Internal from response and calculate the Min Delay Request Interval.

Set DUT to Slave

Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)

Test Min Delay Request Interval

Evaluate the intervals between the captured Min Delay Request messages and ensure the interval is larger than the minimum delay request interval.

Post Condition

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.6 Meet timing constraints

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Meet timing constraints

Explanation: This test checks timing requirements on Announce and Sync messages from a clock in the master state outlined in section 7.7 and 9.5 of IEEE 1588.

The tests will be conducted in the following order:

1. Test Announce intervals. 9.5.8 A node shall, with 90% confidence, issue messages with intervals within +/- 30% of the value of the interval computed from portDS.logAnnounceInterval.
2. Test Sync intervals. 9.5.9.2 A node shall, with 90% confidence, issue messages with intervals within +/- 30% of the value of the interval computed from portDS.logSyncInterval.
3. Test accuracy of originTimestamp in Sync messages. 9.5.9.4 0 or no worse than 1 second from actual time of master.

Pre Condition

Connect DUT

Connect the DUT to the test network

Start ordinary clock

Start up the PTP clock

Start management node

Start up the PTP management node

Initialize all clocks

Send a management message INITIALIZE to all clocks.

Set DUT to Master

Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.

Test Procedure

Check log interval values from DUT

Get the Port Set by sending a PORT_DATA_SET management message to the DUT.
Extract the Log Announce and Log Sync Interval from response and make sure they are within the expected boundaries.

	Min Value	Max Value
Log Announce Interval	0	4
Log Sync Interval	-4	-1

Ensure DUT is Slave

Wait for the DUT to be slave and the local clock master.

Check interval confidence

Wait for a certain amount of messages. Calculate the interval between these messages and make sure 90% of the messages keep to the expected interval. Test this for SYNC and ANNOUNCE messages.

Check Sync timestamp quality

Wait for a certain amount of SYNC messages or FOLLOW_UP messages if two step is active. Extract the timestamps and make sure the timestamp differences between two messages match the SYNC interval length.

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.7 Correction Field

Category

LXI Clock Synchronization

Test Type

Kerberos Test, automated

Rule

Correction Field

Explanation

The timing messages in IEEE 1588 version 2 contain a field named correctionField. These fields contain modifications of the timestamp fields and must be correctly used by a slave clock in order to properly synchronize to its parent clock. Likewise a master clock must ensure that the combination of master transmitted timestamps and correctionFields correctly indicates the time intended.

Pre Condition

Connect DUT

Connect the DUT to the test network

Start ordinary clock

Start up the PTP clock

Start management node

Start up the PTP management node

Initialize all clocks

Send a management message INITIALIZE to all clocks.

	Set DUT to Slave	
		Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
Test Procedure	Ensure DUT is Slave	
		Wait for the DUT to be slave and the local clock master.
	Wait for stable meanPathDelay of Slave	
		Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.
	Check correction field influence on messages: SYNC, FOLLOW UP, DELAY RESP	
		Set the correction field value for one of the following messages: SYNC, FOLLOW UP, DELAY RESP. Expect the meanPathDelay perturbation to rise by half the value set in correction field.
	Set DUT to Master	
		Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.
	Ensure DUT is Master	
		Wait for the DUT to be master and the local clock slave.
	Wait for stable meanPathDelay of Slave	
		Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.
	Check correction field influence on messages: DELAY REQ	
		Set the correction field value for one of the following messages: DELAY REQ. Expect the meanPathDelay perturbation to rise by half the value set in correction field.
Post Condition	Reset local clock	
		Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown ordinary clock	
		Shutdown the PTP clock
	Shutdown management node	
		Shutdown the PTP management node

3.2.1.8 Synchronize to one-step and two-step masters

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Synchronize to one-step and two-step masters

Explanation

One-step clocks do not send Follow_Up messages but any clock, one- or two-step, must be able to synchronize to it. Two-step clocks do send Follow_Up messages and any clock, one- or two-step, must correctly use the Follow_Up message as part of synchronization, see 11.2.

The test is to verify that the DUT correctly synchronizes to both types of clocks. Specifically this requires:

- A DUT in the slave state correctly synchronize to a one-step master clock, and
- A DUT in the slave state correctly synchronize to a two-step master clock.

The first test has effectively been accomplished by the execution of test 7 in which a two-step clock is used and the measure of synchronization is the meanPathDelay having a reasonable value.

Pre Condition

Connect DUT

Connect the DUT to the test network

Start ordinary clock

Start up the PTP clock

Start management node

Start up the PTP management node

Initialize all clocks

Send a management message INITIALIZE to all clocks.

Set DUT to Slave

Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)

Test Procedure

Set local clock to One-Step

Set the lock clock to act as a One-Step master. This means the local clock will be delivering the timestamps directly in the SYNC message instead of sending a Follow_Up message with the timestamp.

Wait for stable meanPathDelay of Slave

Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.

Set local clock to Two-Step

Set the lock clock to act as a Two-Step master. This means the local clock will be delivering the timestamps in a Follow_Up message.

Wait for stable meanPathDelay of Slave

Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.9 Honor V1 HW compatibility bit

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Honor V1 HW compatibility bit
Explanation	Some devices designed under IEEE 1588-2002 but still usable with IEEE 1588-2008 use the packet length in deciding whether to timestamp packets. Annex D of IEEE 1588-2008 requires that clocks interacting with such a device respond correctly to the hardwareCompatibility bit in the transport specific fields of Announce, Sync, and Delay_Req messages. The test first checks that a slave clock correctly responds to Announce and Sync messages with this bit set. The second part of the test checks that a master correctly responds to a Delay_Req with this bit set.
Pre Condition	Connect DUT Connect the DUT to the test network Start ordinary clock Start up the PTP clock Start management node Start up the PTP management node Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
Test Procedure	Check V1 hardware compatibility for DELAY_REQ Check the Delay_Req messages are extended when V1 hardware compatibility is set and that the flag is set, otherwise flag must not be set and messages are V2 size. Set DUT to Master Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay. Check V1 hardware compatibility for SYNC and ANNOUNCE Check the Sync messages are extended when V1 hardware compatibility is set and that the flag is set, otherwise flag must not be set and messages are V2 size. Check the Announce messages have the flag set when V1 hardware compatibility is set, otherwise flag must not be set.
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.10 Reject Rogue Frames

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Reject Rogue Frames
Explanation	Subsection 9.3.2.5 of IEEE 1588-2008 says to ignore Announce messages which have traversed more than 255 boundary clocks - a preposterous depth for a tree. That requirement is intended to break loops.
Pre Condition	Connect DUT Connect the DUT to the test network Start ordinary clock Start up the PTP clock Start management node Start up the PTP management node Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
Test Procedure	Ensure DUT is Slave Wait for the DUT to be slave and the local clock master. Set steps removed Increase the steps removed of the local clock to 255, so that the DUT does not accept the local clock as master. Wait for announce intervals Wait for a certain amount of announce intervals Ensure DUT is Master Wait for the DUT to be master and the local clock slave.
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.11 Protocol not affected by sequence number rollover

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Protocol not affected by sequence number rollover
Explanation	Mandatory: testing the response of the DUT to sequence rollover in messages from the PC Clock, i.e. Announce, Sync, Follow_Up. Subsection 7.3.7 of IEEE 1588-2008 requires separate sequenceId values for certain messages with rollover properties defined by the datatype UInteger16.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Start ordinary clock	
		Start up the PTP clock
	Start management node	
		Start up the PTP management node
	Initialize all clocks	
		Send a management message INITIALIZE to all clocks.
	Set DUT to Slave	
		Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Ensure DUT is Slave	
		Wait for the DUT to be slave and the local clock master.
	Wait for stable meanPathDelay of Slave	
		Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.
Test Procedure	Check sequence ID's for rollover: ANNOUNCE and SYNC	
		Make sure a sequence ID rollover does not disturb the clock. Increase the sequence ID on local clock close to rollover. Wait for the rollover to happen and ensure the DUT is still stable. Do this check for Announce and Sync messages.
Post Condition	Reset local clock	
		Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown ordinary clock	
		Shutdown the PTP clock
	Shutdown management node	
		Shutdown the PTP management node

3.2.1.12 Seperate sequence number spaces maintained

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Seperate sequence number spaces maintained
Explanation	Subsection 7.3.7 of IEEE 1588-2008 requires separate sequenceId number spaces for Sync, Delay_Req, Announce, Signaling and Management messages.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Start ordinary clock	
		Start up the PTP clock
	Start management node	
		Start up the PTP management node
	Initialize all clocks	
		Send a management message INITIALIZE to all clocks.

Test Procedure	Set DUT to Master	
		Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.
	Test sequence ID's of DUT in state Master	
		Get messages of the type sync, delay req, announce and delay resp. Sync message ID's shall match Follow_Up message ID's Delay_Req message ID's shall match Delay_Resp message ID's Announce message ID's shall not match Sync or Delay_Resp message ID's Delay_Resp message ID's shall not match Sync message ID's
	Set DUT to Slave	
		Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)
	Test sequence ID's of DUT in state Slave	
		Get messages of the type delay req, delay_resp as well as the last DUT messages as master from type sync, delay_resp announce. Delay_Resp message ID's shall match Delay_Res message ID's last Delay_Resp message ID as master shall not match last Sync message ID as master last Delay Resp message ID as master shall not match last Delay_Resp as slave
Post Condition	Reset local clock	
		Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown ordinary clock	
		Shutdown the PTP clock
	Shutdown management node	
		Shutdown the PTP management node

3.2.1.13 Max and min Sync message rate

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Max and min Sync message rate
Explanation	This test verifies that the DUT as a slave can synchronize to a master over the range of Sync intervals required by the LXI 1588 Profile and that as a master it can service slaves over the required range of Sync intervals. The test exercises the required minimum and maximum Sync intervals and the recommended minimum interval supported by the DUT.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Start ordinary clock	
		Start up the PTP clock
	Start management node	
		Start up the PTP management node
	Initialize all clocks	
		Send a management message INITIALIZE to all clocks.
Test Procedure	Set Sync Interval	
		Set the sync interval to the local clock and send a LOG_SYNC_INTERVAL management message to the DUT to set its sync interval as well.

Set DUT to Slave

Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)

Check Slave offset is reasonable

Get the offset of the slave by sending a CURRENT_DATA_SET management message to the slave. Check if the offset is reasonable.

Set DUT to Master

Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.

Check Slave offset is reasonable

Get the offset of the slave by sending a CURRENT_DATA_SET management message to the slave. Check if the offset is reasonable.

Check interval confidence

Wait for a certain amount of messages. Calculate the interval between these messages and make sure 90% of the messages keep to the expected interval. Test this for SYNC and ANNOUNCE messages.

Repeat Sync test steps

Repeat the test steps for following sync values:

- Max Sync value: 1
- Default Min Sync value: -1
- Recommended Min Sync value: -1 to -4

The recommended Min Sync value must first be determined. Lowest recommended value is -4.

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.15 Clock Description

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Clock Description

Explanation

This test verifies that the DUT as a master correctly describes itself in the Announce and Sync messages.

The attributes related to the timescale have been tested in test 14. The contents of the datasets have been examined in test 1 as part of the testing of management messages. This test checks that the contents of the datasets for the fields listed appear correctly in the Announce and Sync messages.

Tested fields:

- versionPTP
- twoStepFlag
- grandmasterPriority1
- grandmasterClockQuality
- grandmasterPriority2
- grandmasterIdentity

Pre Condition

Connect DUT

Connect the DUT to the test network

Start ordinary clock

Start up the PTP clock

Start management node

Start up the PTP management node

Initialize all clocks

Send a management message INITIALIZE to all clocks.

Set DUT to Master

Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.

Test Procedure

Get default data set from DUT

Send a DEFAULT_DATA_SET management message to the DUT to get the default data set.

Get port data set from DUT

Send a PORT_DATA_SET management message to the DUT to get the port data set.

Test sync message details

Test sync message details against port and default data sets.

- Version Number
- Source Port Identity
- Two Step flag

Test announce message details

Test announce message details against port and default data sets.

- Version Number
- Source Port Identity
- Grandmaster Priority1
- Grandmaster Priority2
- Grandmaster Identity

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.1.16 Time span

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Time span
Explanation	This test verifies that the clock in the DUT can advance from 232-1 seconds to 232 seconds, both as master and as slave. This is best done by looking at the timestamps on the wire, since operating systems may not format the date correctly. The date is approximately 6:28:16 am Feb 7, 2106, TAI. (It's impossible to know what the UTC time is because the leap second offset for that date is unknown). Correct operation when the DUT is master is observed using Wireshark.
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies	
3.2.1.5	3.2.1.6

3.2.1.17 Leap second info passed from master to slave

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Leap second info passed from master to slave
Explanation	This test verifies that the DUT correctly updates the time properties data set from the Announce message from the grandmaster.
Pre Condition	Connect DUT Connect the DUT to the test network Start ordinary clock Start up the PTP clock Start management node Start up the PTP management node Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128) Ensure DUT is Slave Wait for the DUT to be slave and the local clock master.

Test Procedure	Compare time properties between local clock and DUT Compare the time properties between the local clock and the DUT. • Current UTC offset • Current UTC offset valid flag • Frequency Traceable flag • Leap59 flag • Leap61 flag • Timescale flag • Time source • Time traceable flag Modify local clock time properties Change the local clock properties of the local clock, as it is master the DUT shall accept these new clock properties. Compare time properties between local clock and DUT Compare the time properties between the local clock and the DUT. • Current UTC offset • Current UTC offset valid flag • Frequency Traceable flag • Leap59 flag • Leap61 flag • Timescale flag • Time source • Time traceable flag
Post Condition	Reset local clock Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.) Shutdown ordinary clock Shutdown the PTP clock Shutdown management node Shutdown the PTP management node

3.2.1.19 Correct nominal clock speed

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	Correct nominal clock speed
Explanation	Clause J.3.4.1 requires that the frequency of a master clock be within 0.01% of the SI second. This is part of the IEEE1588 standard.

3.2.1.20 Clock subsystem survives time jump

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	Clock subsystem survives time jump
Explanation	IEEE 1588 specifies certain changes of state and issuing of messages based on timeouts such as the ANNOUNCE_RECEIPT_TIMEOUT and the Sync and Delay_Req intervals. This declaration ensures a jump in the local clock does not disturb the accuracy of these timeouts and intervals for some common cases. This is part of the IEEE1588 standard.

3.2.1.22 Application of asymmetry correction

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	Application of asymmetry correction
Explanation	The protocol assumes the packet travel time between master and slave is equal in both directions. If it is not, an uncorrected system will exhibit a systematic offset between slave and master equal to half the asymmetry. PTP can't measure this asymmetry, but if it is measured the implementation can be told its magnitude and sign, and PTP will correct for it. This test is only useful if the implementation has a mechanism for entering the value of the asymmetry of the link to its master. The appropriate corrections for this asymmetry are specified in clause 11 of IEEE 1588. This is part of the IEEE1588 standard.

3.2.1.23 Proper simultaneous startup of many clocks

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	Proper simultaneous startup of many clocks
Explanation	The protocol is supposed to converge to 1 master and n-1 slaves under almost any conditions. This checks one of the challenging conditions: many clocks waking up at the same time. The protocol should settle, and all clocks should agree on who the master is. This is part of the IEEE1588 standard.

3.2.1.24 DUT uses grandmaster not parent data in BMC

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	DUT uses grandmaster not parent data in BMC
Explanation	This declaration verifies that the DUT uses the grandmaster fields in Announce messages rather than parent fields as inputs to the best master clock algorithm. This is part of the IEEE1588 standard.

3.2.5 Must Be Able to Set UTC Time

Category	LXI Clock Synchronization
Test Type	Kerberos Test, automated
Rule	Must Be Able to Set UTC Time
Explanation	Any LXI device implementing IEEE 1588 functionality shall be capable of being made traceable to UTC in the event that it is selected as the grandmaster clock by the IEEE 1588 protocol.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	3.2.6

3.2.6 Must Be Able to Set UTC Time Manually

Category	LXI Clock Synchronization
Test Type	Kerberos Test, manual

Rule	Must Be Able to Set UTC Time Manually
Explanation	Traceability to UTC shall be, at a minimum, available by the use of IEEE 1588 management messages with managementId values of: TIME, CLOCK_ACCURACY, UTC_PROPERTIES, TRACEABILITY_PROPERTIES, and TIMESCALE_PROPERTIES.If the test for 3.2.1.14--setting time manually via management messages was successful, then click yes. Otherwise, using the web pages set the time to January 1, 1970, 00:00:00 UTC (this is the date/ time corresponding to a timestamp of zero). The formatted time should go to that value and the value seen in its timestamps should go to 0.0, and then both should advance at 1 sec/sec. The timestamps can be seen via Wireshark in its Sync packets, and the time can be seen on the device's Sync Configuration Web Page. Set the master to the correct time before proceeding to other tests.If the time was set to the correct value, and advances at 1 sec/sec then click Yes.Otherwise, note what failed the the Test Result window and click No. This test verifies that the DUT as a master can have its time adjusted to be traceable to UTC. UTC as required by 3.2.5 and 3.2.6 of the LXI Standard. LXI Devices can use either the web page or IEEE 1588 management messages to set the time and the related time properties.
Pre Condition	Connect DUT Connect the DUT to the test network Start ordinary clock Start up the PTP clock Start management node Start up the PTP management node Initialize all clocks Send a management message INITIALIZE to all clocks. Set DUT to Master Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.
Test Procedure	Check UTC properties against announce message Set the UTC properties of the DUT and check the announce messages for these UTC properties. UTC properties: • Current UTC offset • Current UTC offset valid flag • Leap59 flag • Leap61 flag

Check properties against sync and announce message

Set the Utc-, traceability-, timescale properties and time of to DUT. Check the sync message timestamp and announce messages, if properties and time have been accepted.
UTC properties:

- Current UTC offset
- Current UTC offset valid flag
- Leap59 flag
- Leap61 flag

Traceability properties:

- Frequency Traceable flag
- Time traceable flag

Timescale properties:

- Timescale flag
- Time source

Check sync timespan

Evaluate the timespan between two received messages, the timespan should match the Sync Interval.

Check manual via web page

If time could not be set via management messages, we need to test if time can be set via the web page.

1. Go to the web page
2. Is time settable via web page?
3. Set clock time to 'January 1, 1970, 00:00:00 UTC' (equivalent of timestamp 0)
4. Check time has been accepted by evaluating the Sync message properties

Post Condition

Reset local clock

Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)

Shutdown ordinary clock

Shutdown the PTP clock

Shutdown management node

Shutdown the PTP management node

3.2.8 Communication of Time Must Use IEEE 1588 Time Base

Category: LXI Clock Synchronization

Test Type: Kerberos Test, manual

Rule: Communication of Time Must Use IEEE 1588 Time Base

Explanation: All time references communicated to or from LXI Devices in an LXI system shall be based on the system-wide IEEE 1588 timescale established by the IEEE 1588 clocks in each device. Translation between the IEEE 1588 time base and UTC in an LXI Device shall only occur at the interface to another subsystem external to the portion of the system operating based wholly or in part on time (e.g. a user interface or a database). All LXI Devices required to make this translation shall use the currentUtcOffset information distributed by the IEEE 1588 protocol.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Test inter-module messages use IEEE 1588 as time base

- Set the PTP time to January 1st, 1970, 00:00:00 UTC (corresponding timestamp of zero)
- Send a message to any destination via a time based trigger (alarm)
- Use a packet detector to check the timestamp to be within a few milliseconds of zero

If all timestamps were close to zero timestamp, click Yes otherwise No.

3.2.10 Inclusion of IEEE 1588 Time-Based Triggers

Category: LXI Clock Synchronization

Test Type: Kerberos Test, automated

Rule: Inclusion of IEEE 1588 Time-Based Triggers

Explanation: LXI Devices containing triggerable functions or events and which implement IEEE 1588 shall include one or more time-based triggers. This is necessary for implementation of autonomous time-based event coordination in the LXI Device.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: 3.2.8

3.2.11 Generation of Timestamps

Category: LXI Timestamped Data

Test Type: Vendor Declaration

Rule: Generation of Timestamps

Explanation: LXI Device generating timestamps based upon an IEEE 1588 clock shall provide information as to the accuracy of the timestamps that they supply. As a minimum, this information shall be available as part of the documentation that accompanies each LXI Device (whether printed or electronic).

3.2.12 Pulse-per-Second Output

Category: LXI Clock Synchronization

Test Type: Vendor Declaration

Rule: Pulse-per-Second Output

Explanation: A pulse-per-second output shall be available on all LXI Devices implementing IEEE 1588. The mechanical and electrical specifications of this output shall be vendor-defined, but the output shall generate a rising edge synchronous with the second's transitions of the IEEE 1588 clock.

This pulse-per-second output is intended to be compared with corresponding outputs of the other clocks in the system to verify synchronization performance. The test point does not need to be available externally, although it can be brought to an external point if desired (for instance, by configuring the LXI Wired Trigger Bus to carry the signal).

3.6 Data Timestamps

Category: LXI Timestamped Data

Test Type: Vendor Declaration

Rule	Data Timestamps
Explanation	LXI Devices shall assign a timestamp to all measurement data. See Section 6.5 of the LXI Device Specification concerning driver requirements associated with LXI Timestamped Data. For all LXI Devices implementing IEEE 1588, all such timestamps shall be derived from the local IEEE 1588 synchronized real-time clock. LXI Devices implementing any part of the standard LXI API (see Section 6 of the LXI Device Specification document) shall return a valid data timestamp value.

4.0 Module-To-Module Data Communication of LXI Event Messages

Categories LXI Event Messaging

5.0 LXI Device Wired Trigger Bus

Categories LXI Wired Trigger Bus

6.0 LXI Programmatic Interface (Drivers)

Categories: General Device

6.1 IVI Driver Requirement

Category: General Device

Test Type: Vendor Declaration

Rule: IVI Driver Requirement

Explanation: All LXI Devices shall provide an IVI Specific Driver. The details of this requirement are called out in Section 5 of IVI-3.1. If an LXI Device is a reasonable match to an existing IVI Class specification, its driver shall be compliant to that IVI Class10.

6.1.1 Trigger and Event Required API

Category: LXI Clock Synchronization

Test Type: Vendor Declaration

Rule: Trigger and Event Required API

Explanation: IVI drivers for LXI Devices shall conform to the IVI-3.15 IviLxiSync specification when required by an LXI Extended Function.

6.2 Syntax of the Device Address

Category: General Device

Test Type: Vendor Declaration

Rule: Syntax of the Device Address

Explanation: LXI IVI Drivers shall accept VISA resource names.
The IVI driver provided with an LXI Device may use whatever underlying protocol is permitted by sections 8.1. However, the driver shall accept any valid VISA resource name as the network resource location as described in this section.
Specifically, valid VISA resource names for LXI Devices are:
TCPIP[board]::host address[::LAN device name][::INSTR]
TCPIP[board]::host address::port::SOCKET11
TCPIP[board]::host address[::HiSLIP device name[,HiSLIP port]][::INSTR]

6.5 API Shall Represent Time as Two 64-bit Floats

Category: LXI Clock Synchronization

Test Type: Vendor Declaration

Rule: API Shall Represent Time as Two 64-bit Floats

Explanation: All IVI interfaces shall represent IEEE 1588 time, time-stamps, or alarms as two 64-bit floating point numbers. One containing the seconds portion and one containing the fractional seconds.

6.5.1 Property Names for Real-Time Representation

Category: LXI Clock Synchronization

Test Type: Vendor Declaration

Rule: Property Names for Real-Time Representation

Explanation: All interfaces for setting or retrieving IEEE 1588 time or alarms derived from IEEE 1588 time shall have two properties of type DOUBLE named TimeSeconds and TimeFraction.

6.5.2 Property Names for Real-Time Timestamp

Category	LXI Clock Synchronization
Test Type	Vendor Declaration
Rule	Property Names for Real-Time Timestamp
Explanation	LXI Devices generating timestamps shall provide two properties of type DOUBLE named TimeStampSeconds and TimeStampFraction in all interfaces that are capable of querying measured data from the device for retrieving the timestamp associated with said data. These properties shall be read only.

7.0 LAN Specification

Categories: General Device

7.1 Ethernet Required

Category: LAN, Device Specification

Test Type: Kerberos Test, automated

Rule: Ethernet Required

Explanation: LXI Devices shall implement Ethernet For a physical connection, this shall be a minimum of 100 Mbits/second, IEEE 802.3 Type 100 BASE-TX.

Pre Condition: Connect DUT

Connect the DUT to the test network

Test Procedure: Detect Network speed

Detect the current network speed. The device and the hardware are connected directly therefore the network speed of the hardware is the speed negotiated by the DUT.

Evaluate Network speed

Evaluate the network speed for 1000BaseT, 100BaseTx and 10BaseT. 10BaseT is optional and need not pass.

7.1.2 Proper Operation in Slower Networks

Category: LAN, Device Specification

Test Type: Kerberos Test, automated

Rule: Proper Operation in Slower Networks

Explanation: LXI Devices shall operate properly in Ethernet networks of equal or slower speed than themselves, at least down to 100 Mbits/sec Ethernet. If LXI Devices could operate at 10 Mbits/second, they shall be IEEE 802.3 Type 10 BASE-T.

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: Detect Network speed

Detect the current network speed. The device and the hardware are connected directly therefore the network speed of the hardware is the speed negotiated by the DUT.

Change Network speed 1000

Change the network speed to 1000BaseT

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

Change Network speed 100

Change the network speed to 100BaseTX

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

Change Network speed 10

Change the network speed to 10BaseT

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

7.2 MAC Address Display

Category	LAN, Device Specification
Test Type	Kerberos Test, manual
Rule	MAC Address Display
Explanation	LXI Devices shall display the MAC address of the LXI Device via a user-accessible display or label affixed to the LXI Device. The MAC address is not changeable.
Test Procedure	Query MAC address display Query the Tester for the MAC address displayed via the user interface or on a label fixed to the device.

7.3 Ethernet Connection Monitoring

Category	LAN, Device Specification
Test Type	Kerberos Test, manual
Rule	Ethernet Connection Monitoring
Explanation	LXI Devices shall incorporate Ethernet connection monitoring (one possible implementation of which is commonly known as Media Sense in Microsoft operating systems). Upon detecting a connection event, the current IP configuration shall be validated (including duplicate IP address detection) and, if necessary, updated.
Test Procedure	Disconnect DUT Disconnect the DUT from the test network Is LAN Status Indicator showing FAULT Prompt the Tester to check the LAN Status indicator for FAULT. Connect DUT Connect the DUT to the test network Is LAN Status Indicator showing OK Prompt the Tester to check the LAN Status indicator for OK.

7.5 Label Required on LXI Devices Without Auto-MDIX

Category	LAN, Device Specification
Test Type	Kerberos Test, manual
Rule	Label Required on LXI Devices Without Auto-MDIX
Explanation	If Auto-MDIX is not supported the LXI Device shall be clearly labeled with a physical, human-readable label. A “soft” label, on an instrument display, for instance is insufficient.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Change to MDIX off Change the LAN settings to MDIX off Ping the DUT for success Ping the DUT via IPv4 which is expected to succeed Change to MDIX on Change the LAN settings to MDIX on Ping the DUT for success Ping the DUT via IPv4 which is expected to succeed

	Query Auto-MDIX label	
		Query tester if a label clearly notifies this device is not Auto-MDIX capable.
Post Condition	Change to MDIX auto	
		Change the LAN settings to MDIX auto. This is the default setting.

7.6 Enable Auto-Negotiation by Default

Category	LAN, Device Specification
Test Type	Kerberos Test, automated
Rule	Enable Auto-Negotiation by Default
Explanation	LXI Devices should support auto-negotiation by default to select the highest operating mode. In most cases, Auto-Negotiation eliminates the need for the user to explicitly set the operating modes at both ends of the cable. Most Ethernet products enable Auto-Negotiation by default.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Detect Advertised Auto-Negotiation flag
	Detect whether DUT is advertising Auto-Negotiate

7.7 Multiple LAN Interfaces

Category	LAN, Device Specification
Test Type	Kerberos Test, manual
Rule	Multiple LAN Interfaces
Explanation	If multiple LAN interfaces (NIC's) are present in an LXI Device, at least one of them shall be fully conformant with the LXI Device Specification (Rule 1.4.4.2.1). The other NIC's don't have to provide any LXI capabilities. If a vendor decides that all the NIC's are LXI capable, then they shall be fully conformant with the LXI Device Specification (web server, mDNS, XML identification schema etc.) as a minimum. All NIC's claiming to be LXI conformant will be tested when submitted for LXI Compliance Testing.
Test Procedure	Evaluate Multiple Interfaces
	Test if only one interface shall be LXI compliant, otherwise query Tester if all interfaces have been tested and are LXI compliant.

8.0 IPv4 LAN Configuration

Categories: IPv4 DDNS

8.1 TCP/IP, UDP, IPv4 Network Protocols

Category: IPv4, Device Specification

Test Type: Kerberos Test, automated

Rule: TCP/IP, UDP, IPv4 Network Protocols

Explanation: LXI Devices shall support TCP/IP networking, as outlined in a number of RFCs, including 791 (IP), 793 (TCP), and 768 (UDP). IPv4 shall be supported at a minimum.
LXI Devices can be controlled and communicated with using any higher-level protocol (such as RPC), as long as it is built on top of the TCP or UDP transport layers.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

Test Procedure: Start wireshark capture: Filter "bootp"

Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured

Connect DUT

Connect the DUT to the test network

Stop wireshark capture

Stop the wireshark from further package capturing

Analyse wireshark capture for DHCP packets

Analyse the wireshark capture for the presence of DHCP packets

Post Condition: Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

8.2 ICMP Ping Responder

Category: IPv4, Device Specification

Test Type: Kerberos Test, automated

Rule: ICMP Ping Responder

Explanation: LXI Devices shall support ICMP (Internet Control Message Protocol, used for a Ping Responder) for diagnostics.
The TCP/IP stack shall be able to respond to the ICMP echo message used by the ping command. The ‘ping ’ or ‘ping ’ command is the standard way to understand whether a user’s connection to an Ethernet device is working.

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

8.3 ICMP Ping Responder Enabled by Default

Category: IPv4, Device Specification

Test Type: Kerberos Test, manual

Rule	ICMP Ping Responder Enabled by Default
Explanation	ICMP Ping service (“Ping Responder”) shall be enabled by default.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Disable Ping Responder Prompt the Tester to disable the ICMP Ping Responder
Test Procedure	Ping the DUT for failure Ping the DUT via IPv4 which is expected to fail. Do LCI The tester is prompted to do a manual LAN reset on the DUT. Ping the DUT for success Ping the DUT via IPv4 which is expected to succeed

8.4 Provide Way to Disable ICMP Ping Responder

Category	IPv4, Device Specification
Test Type	Kerberos Test, automated
Rule	Provide Way to Disable ICMP Ping Responder
Explanation	LXI Devices shall provide a way to disable the IPv4 ICMP ping responder.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	8.3

8.6 IP Address Configuration Techniques

Category	IPv4, Device Specification
Test Type	Kerberos Test, automated
Rule	IP Address Configuration Techniques
Explanation	LXI Devices shall support three LAN configuration techniques: DHCP, Dynamically Configured Link Local Addressing (Auto-IP), and manual. LAN configuration refers to the mechanism that the device uses to obtain IP Address, Subnet Mask, Default Gateway IP Address, and DNS Server IP Address(es). Collectively, DHCP and Dynamically Configured Link Local Addressing are considered automatic configuration methods. These automatic methods may provide additional or supplemental user entries for DNS servers as appropriate. The DHCP and Manual configuration methods provide configuration for: 1) module IP address, 2) Subnet Mask, 3) Default Gateway IP Address, 4) DNS server IP addresses.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	8.6.1, 9.5

8.6.1 Options for LAN configuration

Category	IPv4, Device Specification
Test Type	Kerberos Test, manual
Rule	Options for LAN configuration
Explanation	LXI Devices shall support one of the following options for LAN configuration: A single configuration setting of Automatic (implying DHCP and Dynamically Configured Link Local Addressing) or Manual. Individual configuration settings for: DHCP, Dynamically Configured Link Local Addressing, and Manual. If more than one is enabled, the LXI Device's LAN configuration shall proceed in the following order: 1) DHCP, 2) Dynamically Configured Link Local Addressing, 3) manual.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Check IPv4 configuration options Prompt the Tester to check configuration options. Either a "Auto/Manual" selection method must be found or a way to individually set DHCP/Dynamically Configured Link-Local/Manual must be available.

8.6.3 Explicitly Request All Desired DHCP Parameters

Category	IPv4, Device Specification
Test Type	Kerberos Test, automated
Rule	Explicitly Request All Desired DHCP Parameters
Explanation	LXI Devices shall explicitly request all desired DHCP parameters from the DHCP server. A DHCP client uses the "parameter request list" option to request specific parameter values from a server. The LXI Device DHCP implementation should ensure that parameters like default gateway and subnet mask are in the "parameter request list".
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Disconnect DUT Disconnect the DUT from the test network
Test Procedure	Start wireshark capture: Filter "bootp" Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured Connect DUT Connect the DUT to the test network Stop wireshark capture Stop the wireshark from further package capturing

Analyse DHCP request packets of wireshark capture

Analyse DHCP request packets of the wireshark capture for the parameters
- Subnet Mask,
- Router
- Domain Name Server

Post Condition: Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

8.6.5 Do Not Require Additional DHCP Options for Normal Operations

Category: IPv4, Device Specification

Test Type: Kerberos Test, automated

Rule: Do Not Require Additional DHCP Options for Normal Operations

Explanation: LXI Devices shall not require any additional DHCP options for normal operations beyond what is needed for IP and DNS configuration. Other options may be requested, but the operation of the LXI Device shall not depend on receiving these parameters.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

Test Procedure: Start wireshark capture: Filter "bootp"

Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured

Connect DUT

Connect the DUT to the test network

Stop wireshark capture

Stop the wireshark from further package capturing

Analyse DHCP ack packets of wireshark capture

Analyse DHCP ack packets of the wireshark capture for the parameters
- IP address,
- Subnet Mask,
- Router
- Domain Name Servers

Post Condition: Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

8.6.6 Stop Using IP Address If DHCP Lease Not Renewed

Category: IPv4, Device Specification

Test Type: Kerberos Test, automated

Rule: Stop Using IP Address If DHCP Lease Not Renewed

Explanation: If an LXI Device is unable to renew its DHCP lease it shall stop using the DHCP supplied IP configuration that failed to be renewed and, if so equipped, offer an alarm or error message.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

	Connect DUT	
		Connect the DUT to the test network
Test Procedure	Get IP from mdns	
		Search via mdns for a single lxi service and retrieve its IP address
	Stop IPv4 DHCP router	
		Stop the IPv4 DHCP router, so that no IPv4 DHCP addresses given for lease
	Wait for DUT to loose IPv4	
		Depending on the lease time (in general 5min), wait until the IP address is lost
	Get IP from mdns	
		Search via mdns for a single lxi service and retrieve its IP address

8.6.7 Honor New DHCP Options at Lease Renewal

Category	IPv4, Device Specification
Test Type	Kerberos Test, automated
Rule	Honor New DHCP Options at Lease Renewal
Explanation	LXI Devices shall honor new DHCP options provided when renewing a lease.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Disconnect DUT
	Disconnect the DUT from the test network
	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	Change IPv4 DHCP range router
	Change the range of the IPv4 DHCP server
	Wait for DUT to accept new range
	Depending on the lease time (in general 5min), wait until the IP address has changed
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address

8.6.10 Dynamic Link-Local Address

Category	IPv4, Device Specification
Test Type	Kerberos Test, automated
Rule	Dynamic Link-Local Address

Explanation	LXI Devices shall conform to RFC 3927 Section 2.6.2: ... If the destination address is a unicast address outside the 169.254/16 prefix ... and the host (LXI Device) chooses to send the packet with an IPv4 Link-Local source address, then it MUST ARP for the destination address and then send its packet, with an IPv4 Link-Local source address and a routable destination IPv4 address, directly to its destination on the same physical link. The host MUST NOT send the packet to any router for forwarding. In the case of a device with a single interface and only a Link-Local IPv4 address, this requirement can be paraphrased as "ARP for everything". In many network stacks, achieving this "ARP for everything" behaviour may be as simple as having no primary IP router configured, having the primary IP router address configured to 0.0.0.0, or having the primary IP router address set to be the same as the host`s own Link-Local IPv4 address.
Pre Condition	Stop IPv4 DHCP router Stop the IPv4 DHCP router, so that no IPv4 DHCP addresses given for lease Disconnect DUT Disconnect the DUT from the test network Connect DUT Connect the DUT to the test network
Test Procedure	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Open web page Open the web page of DUT with IPv4 or IPv6 address, depending on the test.

8.7 Duplicate IP Address Detection

Category	IPv4
Test Type	Kerberos Test, manual
Rule	Duplicate IP Address Detection
Explanation	LXI Devices shall perform duplicate IP address detection to ensure an LXI Device does not start using an IP address that is already in use on that network. LXI Devices shall disconnect from the network when a duplicate IP address is detected.
Pre Condition	Connect DUT Connect the DUT to the test network
Test Procedure	Cause duplicate IP Cause the device to issue a duplicate IP warning by setting the device to the same address as the test hardware. This may be done via he webpage LAN configuration or via the devices frontpanel. Is LAN Status Indicator showing FAULT Prompt the Tester to check the LAN Status indicator for FAULT.

Evaluate duplicate IP correction

What the device does when it has detected a duplicate address can be one of the following options but whichever method you use the device must not use the duplicate IP address:

1. When the duplicate address has been detected, the device should show an assigned IP address of 0.0.0.0, in the case of IPv4, and show a LAN fault on the LXI LAN Status Indicator.

2. When the duplicate address has been detected, the device can fall back to the currently valid IP address and not show a fault on the LXI LAN Status Indicator.

3. When the duplicate address has been detected the device can fall back to an Auto-IP address (169.254.x.x) and show a fault on the LXI LAN Status Indicator.

8.10 Provide an Error Indicator for LAN Configuration Faults

Category IPv4, Device Specification

Test Type Kerberos Test, manual

Rule Provide an Error Indicator for LAN Configuration Faults

Explanation LXI Devices shall make use of the LXI LAN Status Indicator to inform the user of a LAN fault or error caused by:
o failure to acquire a valid IP address
o detection of a duplicate IP address
o failure to renew an already acquired DHCP lease (failure to obtain an initial DHCP lease is not a failure)
o LAN cable disconnected (as reported by Ethernet connection monitoring)

See 2.5.2 LAN Status Indicator for annunciation details.

The LXI LAN Status indicator indicates both the LAN error conditions above and provides an identify indication as described in Section 2.5.2. This identifying indication is initiated by the user via the Web interface, Section 9.3, or by the programmatic interface, 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 behaviour of the indicator is not specified.

Pre Condition Stop IPv4 DHCP router

Stop the IPv4 DHCP router, so that no IPv4 DHCP addresses given for lease

Disconnect DUT

Disconnect the DUT from the test network

Test Procedure Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Connect DUT

Connect the DUT to the test network

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Stop IPv4 DHCP router

Stop the IPv4 DHCP router, so that no IPv4 DHCP addresses given for lease

Wait for DUT to loose IPv4

Depending on the lease time (in general 5min), wait until the IP address is lost

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Post Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

8.11.1.1 If Dynamic DNS Can Be Disabled, Its Default State Is Enabled

Category: DDNS, Device Specification

Test Type: Kerberos Test, manual

Rule: If Dynamic DNS Can Be Disabled, Its Default State Is Enabled

Explanation: LXI Devices that allow Dynamic DNS to be turned off shall have the Dynamic DNS capability enabled by default

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Disable Dynamic DNS

Prompt the tester to disable dynamic DNS

Disconnect DUT

Disconnect the DUT from the test network

Start wireshark capture: Filter "bootp"

Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured

Connect DUT

Connect the DUT to the test network

Stop wireshark capture

Stop the wireshark from further package capturing

Analyse DHCP request packets for absence of DDNS options

Analyse DHCP request packets of the wireshark capture for the absence of option 12 and option 83.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Disconnect DUT

Disconnect the DUT from the test network

Start wireshark capture: Filter "bootp"

Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured

Connect DUT

Connect the DUT to the test network

Stop wireshark capture

Stop the wireshark from further package capturing

Analyse DHCP request packets for presence of DDNS options

Analyse DHCP request packets of the wireshark capture for the presence of option 12 and option 83

8.13 LAN Configuration Initialize (LCI)

Category	IPv4, Device Specification
Test Type	Kerberos Test, manual
Rule	LAN Configuration Initialize (LCI)

Explanation

LXI Devices shall provide a LCI reset mechanism, as defined in 2.4.5, that when activated places the LXI Device`s network settings to 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.
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.

Item	Value	Section
IP address configuration DHCP AutoIP	 Enabled Enabled	8.6
ICMP Ping Responder	Enabled	8.3
Web Password for configuration	Factory Default	9.8
Dynamic DNS (if implemented)	Enabled	8.11.1.1
mDNS and DNS-SD	Enabled	10.2, 10.4, 10.5.1, 10.7.1

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Set static IP manually

Prompt the tester to set a static IP address

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Disable Dynamic DNS

Prompt the tester to disable dynamic DNS

Disable mDNS

Prompt the tester to disable mDNS

Disable ICMP Ping Responder

Prompt the tester to disable ICMP Ping Responder

Change web password

Prompt the tester to change web password away from the default value. If LXI Security is configured, then this step is skipped as passwords are handled differently.

Start wireshark capture: Filter "bootp"

Start a wireshark capture and set the filter to "bootp", so that only bootp protocol packages are captured

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Stop wireshark capture

Stop the wireshark from further package capturing

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

Is IPv4 DHCP enabled

Prompt the tester to get IPv4 DHCP is enabled or not

Is Dynamic DNS enabled

Prompt the tester to get dynamic dns enabled or not

Is web password reset

Prompt the tester to get password is reset to default or not. If LXI Security is configured, then this step is skipped as passwords are handled differently.

9.0 Web Interface

Categories: Web Interface

9.1 Web Pages Using W3C Compliant Browsers

Category	Web Interface, Device Specification
Test Type	Kerberos Test, automated
Rule	Web Pages Using W3C Compliant Browsers
Explanation	LXI Devices shall serve a HTML web page that works correctly with all W3C compliant browsers. LXI Device web servers shall conform to HTTP (version 1.0 or greater). The HTML pages served shall conform to HTML (version 4.01 or greater) or XHTML (version 1.0 or greater).
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Validate all given web pages as W3C compliant Validate all configured web pages as W3C compliant. These web pages are given during the configuration process. If any web pages are missing, reconfigure test data.

9.1.4 HTTP Transport and Port Number

Category	Web Interface, Device Specification
Test Type	Kerberos Test, automated
Rule	HTTP Transport and Port Number
Explanation	The default port number for the web server shall be 443. The default web server shall use HTTP over a TLS connection, colloquially referred to as HTTPS.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page Open the web page of DUT with IPv4 or IPv6 address, depending on the test.

9.1.7 Alias for Welcome Page

Category	Web Interface
Test Type	Kerberos Test, manual
Rule	Alias for Welcome Page
Explanation	All LXI Devices shall provide an alias or redirect for the LXI Welcome Web Page document that can be queried via a GET at: https:///lxi.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address

Test Procedure	Query LXI Welcome Page Alias
	Query the LXI Welcome Page Alias from the DUT and ensure it is the correct page. /lxi is the alias for the LXI welcome page.

9.2 Welcome Web Page Display Items

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Welcome Web Page Display Items
Explanation	The primary LXI welcome page shall display the following information in a read-only format. o LXI Device Model o Manufacturer o Serial Number o Description o LXI Extended Functions o LXI version o Hostname o MAC Address o TCP/IP Address o Firmware and/or Software Revision o LXI Device Address String [VISA]
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser
	Prompt tester to open the devices web page
	Query Home Item LXI Device Model
	Prompt tester to check availability of the 'LXI Device Model' on the 'Welcome Web Page'
	Query Home Item Manufacturer
	Prompt tester to check availability of the 'LXI Device Manufacturer' on the 'Welcome Web Page'
	Query Home Item Serial Number
	Prompt tester to check availability of the 'LXI Device Serial Number' on the 'Welcome Web Page'
	Query Home Item Description
	Prompt tester to check availability of the 'LXI Device Description' on the 'Welcome Web Page'
	Query Home Item LXI Extended Functions
	Prompt tester to check availability of the 'LXI Extended Functions' on the 'Welcome Web Page'
	Query Home Item LXI version
	Prompt tester to check availability of the 'LXI Version' on the 'Welcome Web Page'
	Query Home Item Hostname
	Prompt tester to check availability of the 'Hostname' on the 'Welcome Web Page'

Query Home Item MAC Address

Prompt tester to check availability of the 'MAC Address' on the 'Welcome Web Page'

Query Home Item TCP/IP Address

Prompt tester to check availability of the 'TCP/IP Address' on the 'Welcome Web Page'

Query Home Item Firmware and/or Software Revision

Prompt tester to check availability of the 'Firmware and/or Software Revision' on the 'Welcome Web Page'

Query Home Item LXI Device Address String [VISA]

Prompt tester to check availability of the 'LXI Device Address String [VISA]' on the 'Welcome Web Page'

9.2.1 LXI Device Address String on Welcome Page

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	LXI Device Address String on Welcome Page
Explanation	The primary LXI welcome page shall contain an IVI I/O Resource Descriptor (a string such as a VISA Resource Descriptor), which is a string that specifies the address of the hardware asset that can be recognized by the I/O used by a software module that accesses the hardware. An example of such a Resource Descriptor is a VISA Resource. For VISA Resources of the form TCPIP[board]::host address[::LAN device name]::INSTR or TCPIP[board]::host address::port::SOCKET The value of "[board]" must be empty since the instrument cannot know which interface board a client may be using.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser Prompt tester to open the devices web page Query Home Item Value LXI Device Address String Prompt tester for the 'LXI Device Address String' on the 'Welcome Web Page'

9.2.3 Actual Hostname Display

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Actual Hostname Display
Explanation	LXI Devices shall display the validated hostname(s) (DNS and/or mDNS) on the LXI Welcome Web page. The hostname(s) displayed on the LAN Configuration page need not be validated since they represent desired configuration values.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address

Test Procedure	Open web page in browser
	Prompt tester to open the devices web page
	Query Home Item Value Hostname
	Prompt tester for the 'Hostname' on the 'Welcome Web Page'

9.2.3.2 Hostname Display

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Hostname Display
Explanation	If an LXI Device does not support recommendation 9.2.3.1 or if mDNS is disabled then it shall show the assigned IP address or a blank field for the hostname.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Disable mDNS
	Prompt the tester to disable mDNS
	Open web page in browser
	Prompt tester to open the devices web page
	Query Home Item Value Hostname
	Prompt tester for the 'Hostname' on the 'Welcome Web Page'

9.2.3.3 mDNS Hostname Format

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	mDNS Hostname Format
Explanation	When displaying an mDNS hostname on the LXI Welcome Web page, the fully qualified mDNS hostname shall be displayed with its domain of .local.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser
	Prompt tester to open the devices web page
	Query Home Item Value Hostname
	Prompt tester for the 'Hostname' on the 'Welcome Web Page'

9.2.3.5 Description Field contains Resolved Service Name

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Description Field contains Resolved Service Name
Explanation	The unique and resolved service name shall be shown in the description field of the Welcome page defined in section 9.2.
Pre Condition	Connect DUT
	Connect the DUT to the test network

	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser Prompt tester to open the devices web page Query Home Item Value Description Prompt tester for the 'Description' on the 'Welcome Web Page' Get service name from mdns Get the service name for the device under test from mDNS. Disconnect DUT Disconnect the DUT from the test network Register service name for Conflict Register a service name for the device under test to conflict against by assigning the DUTs servicename to the Kerberos device/IP address. Connect DUT Connect the DUT to the test network Remove service name for Conflict Remove the service name registered by the testsuite. Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Open web page in browser Prompt tester to open the devices web page Query Home Item Value Description Prompt tester for the 'Description' on the 'Welcome Web Page'

9.3 Device Identification Functionality on the Web Page

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Device Identification Functionality on the Web Page
Explanation	There shall be a device identification indicator functionality on the web page to control the LAN Status Indicator (see Sections 2.5.2 and 8.10).
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser Prompt tester to open the devices web page Activate LAN ID indicator Prompt tester to activate the LAN ID indicator on web page Is LAN ID indicator active Query tester if LAN ID indicator is showing on device Deactivate LAN ID indicator Prompt tester to deactivate the LAN ID indicator on web page Is LAN ID indicator deactivated Query tester if LAN ID indicator is not showing on device

9.4 LAN and Sync Configuration Links on the Welcome Page

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	LAN and Sync Configuration Links on the Welcome Page
Explanation	The Welcome page shall contain at least two hyperlinks/buttons to provide further information or to allow the user to configure LXI Device settings. The first linked web page shall contain the information as described in section 9.5 and the second linked webpage shall contain the information as described in Section 9.6. The second link (Synchronization web page contents) is applicable for LXI Devices implementing any of following LXI Extended Functions: LXI Clock Synchronization (IEEE 1588), LXI Event Messaging, or the LXI Device Wired Trigger Bus. Refer to those external documents for more specific information.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser Prompt tester to open the devices web page Open LAN configuration web page Prompt tester to open the LAN configuration web page Open 1588 Sync configuration web page Prompt tester to open the 1588 Sync configuration web page Open Event Sync configuration web page Prompt tester to open the Event Messaging Sync configuration web page Open WTB Sync configuration web page Prompt tester to open the Wired Trigger Bus Sync configuration web page

9.5 LAN Configuration Web Page Contents

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	LAN Configuration Web Page Contents
Explanation	The LAN configuration page shall contain the following parameters to configure the LAN settings: o Hostname o Description o TCP/IP Configuration Mode o Static IP address o Subnet mask o Default Gateway o DNS Server(s) The TCP/IP configuration field controls how the IP address for the instrument is assigned. For the manual configuration mode, the static IP address, subnet mask, and default gateway are used to configure the LAN. The automatic configuration mode uses DHCP server or Dynamic Link Local Addressing (Automatic IP), as described in Rule 8.6 to obtain the instrument IP address.
Pre Condition	Connect DUT Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Open web page in browser

Prompt tester to open the devices web page

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Query LAN Item Hostname

Prompt tester to check availability to configure the 'Hostname' on the 'LAN Configuration Web Page'

Query LAN Item Description

Prompt tester to check availability to configure the 'Description' on the 'LAN Configuration Web Page'

Query LAN Item TCP/IP Configuration Mode

Prompt tester to check availability to configure the 'TCP/IP Configuration Mode' on the 'LAN Configuration Web Page'

Query LAN Item Static IP address

Prompt tester to check availability to configure the 'Static IP address' on the 'LAN Configuration Web Page'

Query LAN Item Subnet mask

Prompt tester to check availability to configure the 'Subnet mask' on the 'LAN Configuration Web Page'

Query LAN Item Default Gateway

Prompt tester to check availability to configure the 'Default Gateway' on the 'LAN Configuration Web Page'

Query LAN Item DNS Server(s)

Prompt tester to check availability to configure the 'DNS Server(s)' on the 'LAN Configuration Web Page'

9.5.6 mDNS Enable/Disable Through Web Page

Category: Web Interface, Device Specification

Test Type: Kerberos Test, manual

Rule: mDNS Enable/Disable Through Web Page

Explanation: If the LXI Device implements mDNS enable/disable, then it shall be exposed through the web page.

Pre Condition

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Open web page in browser

Prompt tester to open the devices web page

Disable mDNS

Prompt the tester to disable mDNS

Wait for service name to disappear from mdns

Wait until the service name has disappeared from mdns.

Enable mDNS

Prompt the tester to enable mDNS

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

9.5.7 Reverting Hostname to Factory Default

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Reverting Hostname to Factory Default
Explanation	Setting the hostname field to the empty string (i.e., a string of length zero, or one consisting entirely of whitespace characters) shall revert the hostname to the factory default value.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Get hostname from mdns Get the hostname for the device under test from mDNS. Open web page in browser Prompt tester to open the devices web page Open LAN configuration web page Prompt tester to open the LAN configuration web page Modify hostname Prompt tester to modify the hostname to another value Get hostname from mdns Get the hostname for the device under test from mDNS. Open LAN configuration web page Prompt tester to open the LAN configuration web page Clear hostname Prompt tester to configure hostname to 'empty' or a 'single blank space' on the 'LAN Configuration Web Page' Get hostname from mdns Get the hostname for the device under test from mDNS. Is hostname factory default Query if the hostname on the welcome page is factory default value

9.5.8 Reverting Device Description to Factory Default

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Reverting Device Description to Factory Default
Explanation	Setting the Device Description field to the empty string (i.e., a string of length zero, or one consisting entirely of whitespace characters) shall revert the Device Description to the factory default.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Get service name from mdns Get the service name for the device under test from mDNS.

Open web page in browser

Prompt tester to open the devices web page

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Modify service name

Prompt the tester to modify the service name via the webpage or interface.

Get service name from mdns

Get the service name for the device under test from mDNS.

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Clear service name

Prompt tester to configure service name to 'empty' or a 'single blank space' on the 'LAN Configuration Web Page'

Get service name from mdns

Get the service name for the device under test from mDNS.

Is service name factory default

Query if the service name on the welcome page is factory default value

9.6 Sync Configuration Web Page Contents

Category	LXI Clock Synchronization, LXI Event Messaging, LXI Wired Trigger Bus
Test Type	Kerberos Test, manual
Rule	Sync Configuration Web Page Contents

Explanation

For LXI Devices implementing any of the following Extended Functions, the sync configuration web page is required and shall be populated with information as in the table below:
LXI Clock Synchronization Extended Function (IEEE 1588)
LXI Event Messages Extended Function
LXI Wired Trigger Bus Extended Function

IEEE 1588 Parameters	
Current grandmaster clock	Hostname, IP address, or MAC address
Parent clock	Hostname, IP address, or MAC address
State	Master, Slave, Faulty, Disabled, Passive, Uncalibrated, Other (Initializing, Listening, Pre-master)
Current PTP time	Seconds since 0 hours, 1 January 1970 TAO (represented as a string of the form "seconds.fractional seconds")
Current local time (if available)	Date/time
Current grandmaster traceability to UTC	The string corresponding to the value of the timeSource field of the Announce message as defined in Table 7 of IEEE 1588, e.g. GPS, NTP, HAND_SET or ATOM...
Current observed variance of parent clock	In (nanoseconds)^2
Current source of time	String representing clock in use (e.g. IEEE-1588 PTP)
IEEE 1588 Domain	The integer, domainNumber, as defined by IEEE 1588.
IEEE 1588 Version	The integer, versionNumber, as defined by IEEE 1588, e.g. 2 for IEEE 1588-2008.
LXI Event Parameters	
LXI Domain	As defined in Section 4 of the LXI Event Messaging Extended Function document.
LXI Wired Trigger Bus Parameters	
Wired-Or Bias	Enabled or Disabled(default) for each LXI0 to LXI7

Pre Condition

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Open web page in browser

Prompt tester to open the devices web page

Open 1588 Sync configuration web page

Prompt tester to open the 1588 Sync configuration web page

Query 1588 Sync Item Grandmaster Clock

Prompt tester to check availability of the 'Grandmaster Clock' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Parent Clock

Prompt tester to check availability of the 'Parent Clock' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item State

Prompt tester to check availability of the 'State' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item PTP Time

Prompt tester to check availability of the 'PTP Time' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Local Time

Prompt tester to check availability of the 'Local Time' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Traceability To UTC

Prompt tester to check availability of the 'Traceability To UTC' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Observed Variance

Prompt tester to check availability of the 'Observed Variance' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Time Source

Prompt tester to check availability of the 'Time Source' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Domain

Prompt tester to check availability of the 'Domain' on the '1588 Sync Configuration Web Page'

Query 1588 Sync Item Version

Prompt tester to check availability of the 'Version' on the '1588 Sync Configuration Web Page'

Open Event Sync configuration web page

Prompt tester to open the Event Messaging Sync configuration web page

Query Event Sync Item Domain

Prompt tester to check availability of the 'Domain' on the 'Event Sync Configuration Web Page'

Open WTB Sync configuration web page

Prompt tester to open the Wired Trigger Bus Sync configuration web page

Query WTB Sync Item WiredOr Bias

Prompt tester to check availability of the 'Wired-Or Bias' on the 'WTB Sync Configuration Web Page'

9.8 Web Page Password Protection

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	Web Page Password Protection
Explanation	Any page(s) that allows user to change the instrument's settings shall be password protected; user changeable default passwords are acceptable. Blank passwords are forbidden.
Pre Condition	Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Open web page in browser

Prompt tester to open the devices web page

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open 1588 Sync configuration web page

Prompt tester to open the 1588 Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open Event Sync configuration web page

Prompt tester to open the Event Messaging Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open WTB Sync configuration web page

Prompt tester to open the Wired Trigger Bus Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open Any Other configuration web pages

Prompt tester to open any other web pages which can change device settings

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Modify password

Prompt tester to modify the password, either on the device or if available on the web page

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open 1588 Sync configuration web page

Prompt tester to open the 1588 Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open Event Sync configuration web page

Prompt tester to open the Event Messaging Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open WTB Sync configuration web page

Prompt tester to open the Wired Trigger Bus Sync configuration web page

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

Open Any Other configuration web pages

Prompt tester to open any other web pages which can change device settings

Is password requested

Query if password was requested when opening the web page. This may be on load, meaning that before the webpage is shown a password is requested or on submit where the password is first requested once cahnged datat is submitted to the device, e.g. via submit button.

9.9 LXI Logo

Category	Web Interface, Device Specification
Test Type	Kerberos Test, manual
Rule	LXI Logo
Explanation	All the required web pages for an LXI Device shall contain the LXI Logo (see LXI Consortium Trademark and Logo Usage Guidelines).
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser
	Prompt tester to open the devices web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open LAN configuration web page

Prompt tester to open the LAN configuration web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open 1588 Sync configuration web page

Prompt tester to open the 1588 Sync configuration web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open Event Sync configuration web page

Prompt tester to open the Event Messaging Sync configuration web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open WTB Sync configuration web page

Prompt tester to open the Wired Trigger Bus Sync configuration web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open logging web page

Prompt tester to open the logging web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

Open LANv6 configuration web page

Prompt tester to open the IPv6 LAN configuration web page

Is LXI Logo on web page

Query if LXI Logo is on the web page

9.14 All URLs Beginning With “LXI” Are Reserved by the LXI Consortium

Category	Web Interface
Test Type	Vendor Declaration
Rule	All URLs Beginning With “LXI” Are Reserved by the LXI Consortium
Explanation	RFC 1738 defines the HTTP URL as the following: http://<host>:Any URL with a that begins with the strings 'lxi' or 'LXI' or any combination of lowercase and uppercase letters combined to spell LXI are reserved for Consortium-defined uses. This includes the directory-like syntax in which the first part of is any combination of lowercase and uppercase letters that spell LXI terminated with a '/': http://<host>:<port>/lxi/<path>?<searchpart>

10.0 LAN Discovery and Identification

Categories: mDNS Identification

10.1 Support VXI-11 Discovery Protocol

Category: LXI VXI-11 Discovery and Identification

Test Type: Kerberos Test, automated

Rule: Support VXI-11 Discovery Protocol

Explanation: The VXI-11 protocol should be supported by all LXI Devices for discovery purposes. If an LXI Device supports the VXI-11 Discovery Protocol, it shall be accomplished by issuing a broadcast RPC call on the host's subnet. The broadcast RPC shall be to either the port-mapper itself on port 111 (querying for VXI-11 support) or the NULL procedure (procedure 0) on the Program Number assigned to the VXI-11 Core Service (0x0607AF).

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: Discover DUT via VXI-11

Discover the device under test (DUT) using the VXI-11 protocol.

Evaluate VXI-11 Discovery response

Evaluate the responses received from the VXI-11 Discovery.
During testing only one device should be found, the device under test (DUT).

10.1.1 VXI-11 Servers Respond Within One Second

Category: LXI VXI-11 Discovery and Identification

Test Type: Kerberos Test, automated

Rule: VXI-11 Servers Respond Within One Second

Explanation: If the VXI-11 discovery protocol is supported, it shall respond to a broadcast RPC to the NULL procedure within 1 second.

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: Discover DUT via VXI-11

Discover the device under test (DUT) using the VXI-11 protocol.

Evaluate VXI-11 Discovery response time

Evaluate the time frame from when the VXI-11 discovery was initiated until the device responded.
This should not be more than 1 second.

10.1.2 SCPI *IDN?

Category: LXI VXI-11 Discovery and Identification

Test Type: Kerberos Test, automated

Rule: SCPI *IDN?

Explanation	If the LXI Device support the VXI-11 Discovery Protocol at a minimum an LXI Device that supports VXI-11 shall be able to respond to the IEEE 488.2 '*IDN?' command. This is a simple query that returns four comma-separated fields, which indicate manufacturer, model, serial number, and firmware version.
Pre Condition	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Establish VXI-11 connection Establish a connection to the DUT using the VXI-11 protocol.
Test Procedure	Send '*IDN?' command over VXI-11 Send a '*IDN?'-request via the VXI-11 protocol to the device under test (DUT). Evaluate VXI-11 response Evaluate the response to a send command which was received via the VXI-11 protocol.

10.1.3 Include 'LXI VXI-11 Discovery and Identification' in Welcome Web Page "LXI Extended

Category	LXI VXI-11 Discovery and Identification
Test Type	Kerberos Test, automated
Rule	Include 'LXI VXI-11 Discovery and Identification' in Welcome Web Page "LXI Extended Functions"
Explanation	Devices implementing the LXI VXI-11 Discovery and Identification extended function shall include 'LXI VXI-11 Discovery and Identification' in the 'LXI Extended Functions' display item of the welcome web page.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	1.4.6

10.1.4 Include the LXI VXI-11 Function in the <LxiExtendedFunctions> element

Category	LXI VXI-11 Discovery and Identification
Test Type	Kerberos Test, automated
Rule	Include the LXI VXI-11 Function in the element
Explanation	LXI devices implementing VXI-11 Discovery and Identification extended function shall include a element in the XML element with the FunctionName attribute of "LXI VXI-11 Discovery and Identification" and a Version attribute containing the version number of the documentation.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	10.2.5

10.2 LXI API Identification Methods

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	LXI API Identification Methods
Explanation	Devices shall provide the following REST API as defined in the LXI API Extended Function: - /lxi/identification.

Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies

23.10.7	23.10.7.1	23.10.7.2
23.11.2-1	23.11.2.1-1	23.11.2.1-1

10.2.5 LXI Extended Function Elements

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	LXI Extended Function Elements
Explanation	Devices that support LXI Extended Functions shall provide Function elements within the LXIExtendedFunctions element, and a string containing the version number specifying the implementation of that extended function. In addition, some extended functions may provide additional information within their Function element. This allows clients to enumerate the set of extended functions associated with the device.
Pre Condition	Connect DUT Connect the DUT to the test network Get identification file Get the identification file from the device under test
Test Procedure	Validate Extended Functions Validate the Extended Functions given by the identification file Check Extended Functions Version Check the Extended Function version for each listed Extended Function.

10.3 Support mDNS

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Support mDNS
Explanation	LXI Devices shall support Multicast DNS (mDNS) as defined by RFC6762 and RFC6763
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies

10.3.1	10.3.1.1	10.3.3
10.3.4		

10.3.1 Claiming Hostnames

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Claiming Hostnames
Explanation	LXI Devices shall assign themselves an mDNS hostname and shall automatically resolve mDNS hostname conflicts.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network
Test Procedure	Get hostname from mdns Get the hostname for the device under test from mDNS.

10.3.1.1 Hostname Conflicts

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Hostname Conflicts
Explanation	If an mDNS hostname conflict occurs, the LXI Device shall assign itself a new hostname and retry until the conflict is resolved. New hostnames shall be generated by appending a number to the end of the hostname. For example, a conflict on “Instr-ABC” would become “Instr-ABC-2” after the first collision, “Instr-ABC-3” on the second, and so on.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network
Test Procedure	Get hostname from mdns Get the hostname for the device under test from mDNS. Disconnect DUT Disconnect the DUT from the test network Register hostname for Conflict Register a hostname for the device under test to conflict against by assigning the DUTs hostname to the Kerberos device/IP address. Connect DUT Connect the DUT to the test network Get hostname from mdns Get the hostname for the device under test from mDNS. Evaluate for resolved hostname Evaluate the hostname retrieved from mdns has resolved after creating a conflict.
Post Condition	Remove hostname for Conflict Remove the hostname registered by the testsuite.

10.3.3 Dynamic DNS Update and mDNS Hostname

Category	DDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Dynamic DNS Update and mDNS Hostname
Explanation	LXI Devices that support Dynamic DNS Update shall use the user-configured hostname as the mDNS hostname.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	10.3.4

10.3.4 DHCP “Host Name” Option and mDNS Hostname

Category	mDNS, Device Specification
Test Type	Kerberos Test, manual
Rule	DHCP “Host Name” Option and mDNS Hostname

Explanation	Regardless of any value, a DHCP server may return as the DHCP "Host Name" option (option code 12); an LXI Device shall use the user configured or factory default hostname for mDNS hostname registration. (See Section 10.7)
Test Procedure	Open web page Open the web page of DUT with IPv4 or IPv6 address, depending on the test. Compare hostname on Welcome Page and Configuration Page Compare hostname on Welcome Page and Configuration Page. The welcome page should match the Configuration page hostname entry with an added ".local." suffix.

10.4 Support mDNS Service Discovery

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Support mDNS Service Discovery
Explanation	LXI Devices shall support shall support Service discovery based on mDNS and DNS as defined by RFC6762 (Multicast mDNS) and RFC6763 (DNS based Service Discovery).
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies			
	10.4.1	10.4.2	10.4.2.3

10.4.1 Claiming Service Name

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Claiming Service Name
Explanation	LXI Devices shall assign themselves a service name used to advertise services defined within this standard and shall automatically resolve service name conflicts.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network
Test Procedure	Get service name from mdns Get the service name for the device under test from mDNS.

10.4.2 Single Service Instance Name for LXI Defined Services

Category	mDNS
Test Type	Kerberos Test, automated
Rule	Single Service Instance Name for LXI Defined Services
Explanation	LXI Devices shall assign themselves a single service name for use in advertising all required and recommended LXI services, as below, and shall resolve service name conflicts. The service instance name is the "instance" portion of a service name as follows: . . Thus, an HTTP service with an instance name of "Instrument ABC" in the ".local" domain will have "Instrument ABC._http._tcp.local" as the service name.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4

	Connect DUT
	Connect the DUT to the test network
	Get service name from mdns
	Get the service name for the device under test from mDNS.
Test Procedure	Validate service name against all registered services
	All registered services for the device under test must have matching service-names.

10.4.2.1 User Configurable Service Name

Category	mDNS, Device Specification
Test Type	Kerberos Test, manual
Rule	User Configurable Service Name
Explanation	LXI Devices shall allow a user to modify the non-volatile service name via the web interface, truncated to the first 63 bytes of UTF-8. When a user modifies a service name, the LXI Device shall unregister all services and then reregister using the new service name.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get service name from mdns
	Get the service name for the device under test from mDNS.
	Modify service name
	Prompt the tester to modify the service name via the webpage or interface.
	Get service name from mdns
	Get the service name for the device under test from mDNS.
	Query tester if new service name is the modified service name
	Prompt the tester to inquire whether the new service name is the recently entered modified service name.

10.4.2.3 Service Name Conflicts

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Service Name Conflicts
Explanation	If an mDNS service name conflict occurs, the LXI Device shall assign itself a new service name and retry until the conflict is resolved. New service names shall be generated by appending a number to the end of the service name. For example, a conflict on “Vendor Instrument” would become “Vendor Instrument (2)” after the first collision, “Vendor Instrument (3)” on the second, and so on.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get service name from mdns
	Get the service name for the device under test from mDNS.

	Disconnect DUT
	Disconnect the DUT from the test network
	Register service name for Conflict
	Register a service name for the device under test to conflict against by assigning the DUTs servicename to the Kerberos device/IP address.
	Connect DUT
	Connect the DUT to the test network
	Get service name from mdns
	Get the service name for the device under test from mDNS.
	Evaluate for resolved servicename
	Evaluate the servicenam retrieved from mdns has resolved after creating a conflict.
Post Condition	Remove service name for Conflict
	Remove the service name registered by the testsuite.

10.4.3 Required Service Advertisements and TXT Record Keys

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Required Service Advertisements and TXT Record Keys
Explanation	LXI Devices shall, at a minimum, advertise the following services via mDNS and shall provide the related keys in the TXT records for the service. Please refer to 10.4.3.5 for Permission on TXT Record Keys with default values. _http._tcp txtvers=1 path=/ (default values) _lxi._tcp txtvers=1 Manufacturer=... Model=... SerialNumber=... FirmwareVersion=...
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get txt records from required services from mdns
	Get the txt records from the required services: _lxi._tcp and _http._tcp
	Validate txt records
	Validate the given txt records for required keys

10.4.3.1 TXT Records Are Required

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	TXT Records Are Required
Explanation	The LXI Device shall provide a TXT record for every service instance being advertised. If there are no TXT record entries for a service (see Permission 10.4.3.5), an empty TXT record shall be provided.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network

Test Procedure	Get txt records for all advertised services from mdns Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp Validate txt records Validate the given txt records for required keys

10.4.3.2 TXT Records Consist of Key/Value Pairs

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	TXT Records Consist of Key/Value Pairs
Explanation	TXT records shall consist of key/value pairs of the form “name=value” (without quotes). The value begins after the first ASCII equal sign “=” and continues to the end of the string. The maximum length of a key/value pair is 255 bytes.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network
Test Procedure	Get txt records for all advertised services from mdns Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp Validate txt record entries Validate the given txt records for key/value entries. The maximum length is 255 bytes. name=value

10.4.3.3 TXT Record Keys Are Case-Insensitive ASCII

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	TXT Record Keys Are Case-Insensitive ASCII
Explanation	All TXT record keys (names) shall be printable ASCII characters (0x20-0x7E), excluding “=” (0x3D), and shall be case-insensitive.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Test Procedure	Get txt records for all advertised services from mdns Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp Validate txt record keys Validate the given txt records keys for printable ASCII characters (0x20-0x7E), excluding "=" (0x3D) and shall be case-insensitive.

10.4.3.4 TXT Record Values

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	TXT Record Values
Explanation	TXT record values (data beginning after the ASCII equal sign "=" [0x3D]) in general shall be opaque binary data, but may be ASCII or UTF-8 for particular keys.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network
Test Procedure	Get txt records for all advertised services from mdns Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp Validate txt record values Validate the given txt records values for opaque binary data, but may be ASCII or UTF-8 for particular keys.

10.4.3.6 TXT Record Key Order

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	TXT Record Key Order
Explanation	For any service that has a defined TXT record key of "txtvers" the "txtvers" key, if present, shall be the first key in the TXT record.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Test Procedure	Get txt records for all advertised services from mdns
	Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp
	Validate txt record order
	Validate the given txt records that, if present, the key "txtvers" is the first TXT record.

10.4.3.7 LXI Consortium TXT Record Keys

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	LXI Consortium TXT Record Keys
Explanation	All TXT record keys beginning with “LXI” or “lxi” are reserved for Consortium-defined usage.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get txt records for all advertised services from mdns
	Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp
	Validate txt record lxi keys
	Validate the given txt records that none start with the reserved beginnings of "LXI" or "lxi"

10.4.3.8 Vendor Defined TXT Record Keys

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Vendor Defined TXT Record Keys
Explanation	All TXT record keys (names) used with LXI Consortium required or recommended services shall be either keys (names) as defined by this standard or vendor-specific keys. Vendor-specific keys shall end with the vendor’s domain name in accordance with section 6.4 of http://files.dns-sd.org/draft-cheshire-dnsext-dns-sd.txt. That is, vendor-defined keys shall be of the form “keyname.company.com=.”
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network

Test Procedure	Get txt records for all advertised services from mdns
	Get the txt records from all services advertised by the device under test: _http._tcp _lxi._tcp _hislip._tcp _scpi-raw._tcp _vxi-11._tcp _scpi-telnet._tcp
	Validate txt record vendor keys
	Validate the given txt records that vendor keys are formatted as following: "keyname.company.com=..."

10.5 mDNS and DNS-SD Enabled by Default

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	mDNS and DNS-SD Enabled by Default
Explanation	Both mDNS and DNS-SD shall be enabled by default on LXI Devices.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.

Dependencies		
	10.3	10.4

10.5.1 mDNS and DNS-SD Enabled by LAN Configuration Initialize (LCI)

Category	mDNS, Device Specification
Test Type	Kerberos Test, manual
Rule	mDNS and DNS-SD Enabled by LAN Configuration Initialize (LCI)
Explanation	When the LCI reset mechanism is activated, it shall enable mDNS and DNS-SD.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get hostname from mdns
	Get the hostname for the device under test from mDNS.
	Get service name from mdns
	Get the service name for the device under test from mDNS.
	Disable mDNS
	Prompt the tester to disable mDNS
	Wait for service name to disappear from mdns
	Wait until the service name has disappeared from mdns.
Test Procedure	Do LCI
	The tester is prompted to do a manual LAN reset on the DUT.
	Get hostname from mdns
	Get the hostname for the device under test from mDNS.
	Get service name from mdns
	Get the service name for the device under test from mDNS.

10.5.2 Provide way to Disable mDNS and DNS-SD

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Provide way to Disable mDNS and DNS-SD
Explanation	Devices shall provide a way to enable and disable mDNS and DNS-SD.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	9.5.6

10.6 mDNS Name Resolution

Category	mDNS
Test Type	Vendor Declaration
Rule	mDNS Name Resolution
Explanation	LXI Devices shall use mDNS for name resolution of hostnames in the ".local." domain. Reverse lookups of addresses in the 169.254/16 subnet (Dynamic Link-Local Addresses) shall be resolved via mDNS.

10.7 Nonvolatile Hostnames and Service Names

Category	mDNS, Device Specification
Test Type	Kerberos Test, manual
Rule	Nonvolatile Hostnames and Service Names
Explanation	To promote stability, if a hostname conflict occurs and the LXI Device chooses a new hostname, the device shall save the new hostname in nonvolatile storage for use the next time the device is powered on. Similarly, if a service name conflict occurs and the LXI Device chooses a new service name, it shall save the new service name in nonvolatile storage for use the next time the device is powered on.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get hostname from mdns Get the hostname for the device under test from mDNS. Get service name from mdns Get the service name for the device under test from mDNS. Disconnect DUT Disconnect the DUT from the test network Register hostname for Conflict Register a hostname for the device under test to conflict against by assigning the DUTs hostname to the Kerberos device/IP address. Register service name for Conflict Register a service name for the device under test to conflict against by assigning the DUTs servicename to the Kerberos device/IP address. Connect DUT Connect the DUT to the test network

Remove hostname for Conflict

Remove the hostname registered by the testsuite.

Remove service name for Conflict

Remove the service name registered by the testsuite.

Test Procedure

Get hostname from mdns

Get the hostname for the device under test from mDNS.

Get service name from mdns

Get the service name for the device under test from mDNS.

Cycle power on device

Prompt the tester to cycle the power on the device.

Get hostname from mdns

Get the hostname for the device under test from mDNS.

Get service name from mdns

Get the service name for the device under test from mDNS.

10.7.1 Hostname and Service Name Revert to Default

Category: mDNS, Device Specification

Test Type: Kerberos Test, manual

Rule: Hostname and Service Name Revert to Default

Explanation: When the LCI mechanism is activated, the hostname and the service name shall revert to the last user-configured values, if available, or factory defaults otherwise.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get hostname from mdns

Get the hostname for the device under test from mDNS.

Get service name from mdns

Get the service name for the device under test from mDNS.

Disconnect DUT

Disconnect the DUT from the test network

Register hostname for Conflict

Register a hostname for the device under test to conflict against by assigning the DUTs hostname to the Kerberos device/IP address.

Register service name for Conflict

Register a service name for the device under test to conflict against by assigning the DUTs servicename to the Kerberos device/IP address.

Connect DUT

Connect the DUT to the test network

Remove hostname for Conflict

Remove the hostname registered by the testsuite.

Remove service name for Conflict

Remove the service name registered by the testsuite.

Test Procedure

Get hostname from mdns

Get the hostname for the device under test from mDNS.

Get service name from mdns

Get the service name for the device under test from mDNS.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Get hostname from mdns

Get the hostname for the device under test from mDNS.

Get service name from mdns

Get the service name for the device under test from mDNS.

10.8 Link Changes

Category	mDNS, Device Specification
Test Type	Kerberos Test, automated
Rule	Link Changes
Explanation	When a network “link change” occurs (e.g., an Ethernet cable is plugged in), the LXI Device shall verify that its hostname and service name are unique and shall re-register its services.
Pre Condition	Connect DUT Connect the DUT to the test network Get service name from mdns Get the service name for the device under test from mDNS.
Test Procedure	Disconnect DUT Disconnect the DUT from the test network Wait for service name to disappear from mdns Wait until the service name has disappeared from mdns. Connect DUT Connect the DUT to the test network Get service name from mdns Get the service name for the device under test from mDNS.

11.0 Documentation

Categories: General Device

11.1 Full Documentation on IVI Interface

Category	General Device
Test Type	Vendor Declaration
Rule	Full Documentation on IVI Interface
Explanation	For each LXI Device, the manufacturer shall provide the documentation on the IVI driver, which is required in the Conformance Requirements section of the IVI 3.1 Driver Architecture Specification.

11.2 Registration of the IVI Driver

Category	General Device
Test Type	Vendor Declaration
Rule	Registration of the IVI Driver
Explanation	The IVI driver shall be registered at the IVI Foundation website and be listed on the IVI Foundation driver registration database.

20.0 LXI HiSLIP Extended Function

Categories: LXI HiSLIP

20.4.1 Comply with LXI Device Specification

Category: LXI HiSLIP

Test Type: Kerberos Test, automated

Rule: Comply with LXI Device Specification

Explanation: Devices implementing the LXI HiSLIP extended function shall comply with the LXI Device Specification.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: Device Specification

20.4.2 Devices that implement IPv6 shall conform to LXI IPv6 Extended Function connections on IPv6

Category: LXI HiSLIP

Test Type: Kerberos Test, automated

Rule: Devices that implement IPv6 shall conform to LXI IPv6 Extended Function connections on IPv6

Explanation: If devices support IPv6 HiSLIP connections, they shall also conform to the LXI IPv6 Extended Function.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: LXI IPv6

20.4.4 Do not change HiSLIP on LCI

Category: LXI HiSLIP

Test Type: Kerberos Test, manual

Rule: Do not change HiSLIP on LCI

Explanation: The devices HiSLIP configuration shall not be impacted by LCI. The state of the connection and HiSLIP locks should not be changed by LCI unless necessary as part of network reconfiguration.

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Disable HiSLIP attributes mustStartEncrypted and encryptionMandatory

Disable the HiSLIP attribues mustStartEncrypted and encryptionMandatory attributes to establish HiSLIP connection without encryption. This may only be required if LXI Security is supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Modify HiSLIP port

Prompt tester to modify the HiSLIP port to anything other than the default port number (4880).

Note: This step might not be executed if test configuration claims the device is not able to modify HiSLIP port.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Create HiSLIP connection, expect success

Create a HiSLIP connection to the device-under-test (DUT) and expect a valid connection.

Test Procedure

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Evaluate Port and Connection

Evaluate the advertised HiSLIP port and check that the open HiSLIP connections to the DUT have been closed.

20.5.1 Conformance Requirements

Category: LXI HiSLIP

Test Type: Kerberos Test, automated

Rule: Conformance Requirements

Explanation: The LXI HiSLIP function is an optional function for devices conforming to the LXI Core Device specification, as defined in section 1.4.4.2 of 'LXI Device Specification 2011'.

All LXI Devices implementing the LXI HiSLIP function as permitted by 1.4.4.1 of the 'LXI Device Specification 2011' shall implement and conform to the requirements of all sections in this document in addition to any relevant requirements of 'LXI Device Specification 2011'.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

Device Specification	LXI HiSLIP

20.6.1 Implement the IVI 6.1 HiSLIP Protocol

Category: LXI HiSLIP

Test Type: Kerberos Test, automated

Rule: Implement the IVI 6.1 HiSLIP Protocol

Explanation

Devices implementing the LXI HiSLIP Function shall implement the HiSLIP protocol version 1.1, as defined in 'IVI 6.1: High-speed LAN Instrument Protocol (HiSLIP) February 24, 2011'.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Disable HiSLIP attributes mustStartEncrypted and encryptionMandatory

Disable the HiSLIP attribues mustStartEncrypted and encryptionMandatory attributes to establish HiSLIP connection without encryption. This may only be required if LXI Security is supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Test SRQ and status byte

- Connect using a HiSLIP address string.
- Enable SRQ for data-available (MAV): Send "*ESE 32;*SRE 48"
- Send *IDN?
- Wait to observe SRQ sent to RQ handler in VISA program.
- Read the status byte (viReadSTB). The MAV bit (0x10) should be set.
- Read the response.
- Read the status byte (viReadSTB). The MAV bit (0x10) should not be set.

Test Device Clear

- Connect using a HiSLIP address string.
- Send *IDN?
- Perform Device Clear (viClear)
- Observe viRead times out (response no longer waiting).

Test Interrupted handling

- Connect using a HiSLIP address string.
- Set VI_ATTR_TCPIP_HISLIP_OVERLAP_EN = VI_FALSE
- Get VI_ATTR_TCPIP_HISLIP_OVERLAP_EN. If = VI_FALSE, continue test (device supports Synchronous mode, so test it).
- Send *IDN?
- Send *OPC?
- viRead „1" (and not the identification string).

Test Overlapped mode

- Connect using HiSLIP address string.
- Set VI_ATTR_TCPIP_HISLIP_OVERLAP_EN = VI_TRUE
- Get VI_ATTR_TCPIP_HISLIP_OVERLAP_EN. If = VI_TRUE, continue test (device supports Overlapped mode, so test it).
- Send *IDN?
- Send *OPC?
- viRead ID string
- viRead „1"

Test Locking

- Connect using a HiSLIP address string.
- viLock (exclusive lock).
- Start a child process: (test exclusive lock works)
  - Connect using same HiSLIP address string.
  - Send *IDN?
  - viRead returns VI_ERROR_RSRC_LOCKED after a delay (>= VISA timeout)
  - Get the status byte (viReadSTB). Observe this returns with no error.
  - Set the device to local (viGpibControlRen(go to remote). Observe this returns with no error. (note the change is deferred until after the parent lock is released)
- viUnlock
- Start a child process: (test exclusive lock released)
  - Connect using same HiSLIP address string.
  - Send *IDN?
  - viRead response should get the ID string.
- viLock(shared lock)
- Start a child process: (test shared lock works)
  - Connect using same HiSLIP address string.
  - Send *IDN?
  - viRead returnsVI_ERROR_RSRC_LOCKED after a delay (>= VISA timeout)
- Start a child process: (shared lock can be shared)
  - Connect using same HiSLIP address string.
  - viLock (same shared lock ID)
  - Send *IDN?
  - viRead response should get the ID string.
  - viUnlock
- viUnlock
- Start a child process:(test shared lock released)
  - Connect using same HiSLIP address string.
  - Send *IDN?
  - viRead response should get the ID string.
- viLock (sharedlock)
- viLock (exclusivelock)
- end connection(without unlocking)
- Start a child process:(test locks are released when connections end)
  - Connect using same HiSLIP address string.
  - Send *IDN?
  - viReadresponse should get the ID string

Test Lock Info

- Connect using HiSLIP address string.
- viLock(Shared lock)
- Check viGetAttr(VI_ATTR_RSRC_LOCK_STATE) returns VI_SHARED_LOCK
- viLock (Exclusive lock)
- Check viGetAttr(VI_ATTR_RSRC_LOCK_STATE) returns VI_EXCLUSIVE_LOCK
- viUnlock
- Check viGetAttr(VI_ATTR_RSRC_LOCK_STATE) returns VI_ SHARED_LOCK
- viUnlock
- Check viGetAttr(VI_ATTR_RSRC_LOCK_STATE) returns VI_ NO_LOCK

20.6.2 Accept IPv4 HiSLIP Connections

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Accept IPv4 HiSLIP Connections
Explanation	LXI HiSLIP Devices shall accept HiSLIP connections over the IPv4 network.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check the device supports HiSLIP Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester. Enable HiSLIP Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported. Disable HiSLIP attributes mustStartEncrypted and encryptionMandatory Disable the HiSLIP attribues mustStartEncrypted and encryptionMandatory attributes to establish HiSLIP connection without encryption. This may only be required if LXI Security is supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Test for basic HiSLIP connection • Connect using a HiSLIP address string (viOpen). • Send *IDN? (viWrite) • Read ID string response (pass if any string is returned).

20.7.1 Advertise the HiSLIP DNS-SD Service

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Advertise the HiSLIP DNS-SD Service
Explanation	Devices implementing the LXI HiSLIP Function shall advertise that they accept HiSLIP connections via the HiSLIP DNS-SD service announcement.
Pre Condition	Connect DUT Connect the DUT to the test network
Test Procedure	Get HiSLIP service name Get the service name which was used to advertise the HiSLIP service (_hislip._tcp).

20.7.2 Use the LXI Single Service Instance Name

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Use the LXI Single Service Instance Name
Explanation	LXI devices shall use the same service name for all LXI DNS-SD services, including HiSLIP.
Pre Condition	Connect DUT Connect the DUT to the test network Get service name from mdns Get the service name for the device under test from mDNS.
Test Procedure	Get HiSLIP service name Get the service name which was used to advertise the HiSLIP service (_hislip._tcp).

20.7.3 Use Service Type Name '_hislip._tcp'

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Use Service Type Name '_hislip._tcp'
Explanation	HiSLIP DNS-SD service announcements shall use the mDNS service type name '_hislip._tcp'.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	20.7.1

20.7.4 Include Required TXT Record Keys

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Include Required TXT Record Keys
Explanation	HiSLIP DNS-SD service announcements shall have the following TXT record keys: - txtvers= o Recommended, but may be omitted if the version is '1'. If omitted defaults to: 'txtvers=1' o If included, must be the first TXT record key - Manufacturer= - Model= - SerialNumber= - FirmwareVersion=

Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get txt records for HiSLIP service from mdns
	Get the TXT records attached to the advertised HiSLIP service.
	Validate txt records
	Validate the given txt records for required keys

20.7.6 Advertise HiSLIP DNS-SD Service with HiSLIP Port

Category	LXI HiSLIP
Test Type	Kerberos Test, manual
Rule	Advertise HiSLIP DNS-SD Service with HiSLIP Port
Explanation	The HiSLIP DNS-SD service advertisement shall use the currently-configured HiSLIP port.
Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get HiSLIP Port
	Get the HiSLIP port, which is advertised via the mDNS service.
	Query LAN Item Value HiSLIP port
	Prompt tester for the 'HiSLIP port' on the 'LAN Configuration Web Page'

20.8.1 Include ‘LXI HiSLIP’ in Welcome Web Page “LXI Extended Functions”

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Include ‘LXI HiSLIP’ in Welcome Web Page “LXI Extended Functions”
Explanation	Devices implementing the LXI HiSLIP function shall include ‘LXI HiSLIP’ in the ‘LXI Extended Functions’ display item of the welcome web page.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	1.4.6

20.8.2 Include HiSLIP Address String in Welcome Web Page “LXI Device Address String”

Category	LXI HiSLIP
Test Type	Kerberos Test, manual
Rule	Include HiSLIP Address String in Welcome Web Page “LXI Device Address String”
Explanation	The Welcome Web Page 'LXI Device Address String' display item shall contain the HiSLIP address string necessary to request a HiSLIP connection that conforms with the VISA 5.0 HiSLIP address string format as specified in section 4.3.1 of 'VPP-4.3: The VISA Library'.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser
	Prompt tester to open the devices web page
	Query Home Item Value LXI Device Address String
	Prompt tester for the 'LXI Device Address String' on the 'Welcome Web Page'

Evaluate LXI Device Address Strings for HiSLIP Address String

Evaluate the given LXI Device Address Strings for HiSLIP Address Strings.
Searching for following format:
TCPIP[board]::host address[::HiSLIP device name[,HiSLIP port]][::INSTR]
Where:
Board is the network interface number (default 0).
Host address is the hostname or IP address of the LXI device.
HiSLIP device name begins with 'hislip'. Typically, 'hislip0' is used.
HiSLIP port is the port number to use for connections, defaulting to 4880.

20.8.3 Include HiSLIP port on the LXI LAN Configuration Web Page

Category	LXI HiSLIP
Test Type	Kerberos Test, manual
Rule	Include HiSLIP port on the LXI LAN Configuration Web Page
Explanation	The HiSLIP port shall be displayed on the LAN Configuration Web Page.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Open web page in browser
	Prompt tester to open the devices web page
	Query LAN Item HiSLIP port
	Prompt tester to check if the 'HiSLIP port' is displayed on the 'LAN Configuration Web Page'

20.8.4 Preserve HiSLIP port across power cycles

Category	LXI HiSLIP
Test Type	Kerberos Test, manual
Rule	Preserve HiSLIP port across power cycles
Explanation	The HiSLIP port setting shall be preserved across power cycles.
Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Modify HiSLIP port
	Prompt tester to modify the HiSLIP port to anything other than the default port number (4880). Note: This step might not be executed if test configuration claims the device is not able to modify HiSLIP port.
	Get HiSLIP Port
	Get the HiSLIP port, which is advertised via the mDNS service.
	Cycle power on device
	Prompt the tester to cycle the power on the device.
	Get HiSLIP Port
	Get the HiSLIP port, which is advertised via the mDNS service.
	Ensure unchanged port
	Ensure the port did not change after the power cycle.

20.9.1 Include the HiSLIP Address String in LXI Identification XML

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Include the HiSLIP Address String in LXI Identification XML
Explanation	LXI devices implementing HiSLIP shall include an 'InstrumentAddressString' XML element with the HiSLIP address string.
Pre Condition	Connect DUT Connect the DUT to the test network
Test Procedure	Get identification file Get the identification file from the device under test Get all 'InstrumentAddressString' tags Get all the LXI Device Strings given by the LXI identification file. Evaluate LXI Device Address Strings for HiSLIP Address String Evaluate the given LXI Device Address Strings for HiSLIP Address Strings. Searching for following format: TCPIP[board]::host address[::HiSLIP device name[,HiSLIP port]][::INSTR] Where: **Board** is the network interface number (default 0). **Host address** is the hostname or IP address of the LXI device. **HiSLIP device name** begins with 'hislip'. Typically, 'hislip0' is used. **HiSLIP port** is the port number to use for connections, defaulting to 4880.

20.9.2 Include the LXI HiSLIP Function in the <LxiExtendedFunctions> element

Category	LXI HiSLIP
Test Type	Kerberos Test, automated
Rule	Include the LXI HiSLIP Function in the element
Explanation	LXI devices implementing HiSLIP shall include a element in the XML element with the FunctionName attribute of 'LXI HiSLIP' and a Version attribute containing the version number of this document. If the port number used for HiSLIP is other than the standard HiSLIP port (4880), the element shall include a element with the value of the custom port number.
Pre Condition	Connect DUT Connect the DUT to the test network Get identification file Get the identification file from the device under test
Test Procedure	Get 'ExtendedFunctions' Get all Extended Functions given by the LXI identification file. Evaluate HiSLIP extended function Evaluate the HiSLIP extended function tag from the XML identification file. Ensure the port is given if the currently configured port is anything other than the default value 4880.

21.0 IPv6 LAN Configuration

Categories: LXI IPv6

21.1.1 IPv6 Network Stack Compliance

Category: LXI IPv6

Test Type: Vendor Declaration

Rule: IPv6 Network Stack Compliance

Explanation: 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.

21.1.2 Interoperate with IPv4 networks

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Interoperate with IPv4 networks

Explanation: 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.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

IPv4	LXI IPv6

21.1.3 IPv6 Instrument Control Connections

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: IPv6 Instrument Control Connections

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

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get IPv6 from mdns

Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Get service name from mdns

Get the service name for the device under test from mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Disable HiSLIP attributes mustStartEncrypted and encryptionMandatory

Disable the HiSLIP attribues mustStartEncrypted and encryptionMandatory attributes to establish HiSLIP connection without encryption. This may only be required if LXI Security is supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Evaluate IPv6 HiSLIP Connection

Only run if IPv6 HiSLIP is configured.
1. Get HiSLIP port via mDNS
2. For each IPv6 address:
a) Create a HiSLIP connection to the device-under-test (DUT):
b) Query *IDN:
c) Close Connection

Evaluate IPv6 TCP Connection

1. Get TCP port via mDNS (using _scpi-raw)
2. For each IPv6 address:
a) Create a TCP connection to the device-under-test (DUT):
b) Query *IDN:
c) Close Connection

Evaluate TCP/IP IPv6-based connection

Evaluate the TCP/IP IPv6-based connections such as HiSLIP, raw TCP. At least one connection method must be possible.

21.1.6 IPv6 HTTP Web Access

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: IPv6 HTTP Web Access

Explanation: 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).

Pre Condition: Connect DUT

Connect the DUT to the test network

Get IPv6 from mdns

Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Test Procedure: Open web page

Open the web page of DUT with IPv4 or IPv6 address, depending on the test.

21.1.7 Support IPv6 Operations with Extended Functions

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Support IPv6 Operations with Extended Functions

Explanation: 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.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

21.12.2	21.12.3	21.12.4
21.13.2		

21.1.8 Provide Way to Disable IPv6

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: Provide Way to Disable IPv6

Explanation: 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.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable IPv6 stack	
		Prompt the tester to disable the IPv6 stack on the DUT. This may not be possible. Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.
	Ping the DUT via IPv6 for failure	
		Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail.
	Call webpage via IPv6 and expect failure response	
		Call webpage via IPv6 and expect failure response.
	Enable IPv6 stack	
		Enable the IPv6 stack. Prompt the user to enable the stack via webpage, GUI or API.
	Ping the DUT via IPv6 for success	
		Ping the DUT via IPv6 for success using the global IPv6 address.
	Call webpage via IPv6 and expect success response	
		Call webpage via IPv6 and expect success response.

21.1.9 IPv6 Enabled by Default or LCI

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	IPv6 Enabled by Default or LCI
Explanation	IPv6 traffic shall be enabled by default. LCI shall enable IPv6 if disabled.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable IPv6 stack	
		Prompt the tester to disable the IPv6 stack on the DUT. This may not be possible. Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.
	Ping the DUT via IPv6 for failure	
		Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail.
	Call webpage via IPv6 and expect failure response	
		Call webpage via IPv6 and expect failure response.
	Do LCI	
		The tester is prompted to do a manual LAN reset on the DUT.

Ping the DUT via IPv6 for success

Ping the DUT via IPv6 for success using the global IPv6 address.

Call webpage via IPv6 and expect success response

Call webpage via IPv6 and expect success response.

21.1.10 Provide Way to Disable IPv4

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Provide Way to Disable IPv4
Explanation	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.
Pre Condition	Connect DUT

Connect the DUT to the test network

Get IPv6 from mdns

Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Test Procedure

Disable IPv4 stack

Prompt the tester to disable the IPv4 stack on the DUT.
Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.

Ping the DUT for failure

Ping the DUT via IPv4 which is expected to fail.

Call webpage via IPv4 and expect failure response

Call webpage via IPv4 and expect failure response.

Enable IPv4 stack

Enable IPv4 stack. If LXI Security selected this can be done via Common Configuration, else manual interaction via LAN Reset/webpage or front panel required.

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

Call webpage via IPv4 and expect success response

Call webpage via IPv4 and expect success response.

21.1.11 IPv4 Enabled by Default

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	IPv4 Enabled by Default
Explanation	IPv4 traffic shall be enabled by default. LCI shall enable IPv4 if disabled.
Pre Condition	Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure	Disable IPv4 stack
	Prompt the tester to disable the IPv4 stack on the DUT. Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.
	Ping the DUT for failure
	Ping the DUT via IPv4 which is expected to fail.
	Call webpage via IPv4 and expect failure response
	Call webpage via IPv4 and expect failure response.
	Do LCI
	The tester is prompted to do a manual LAN reset on the DUT.
	Ping the DUT for success
	Ping the DUT via IPv4 which is expected to succeed
	Call webpage via IPv4 and expect success response
	Call webpage via IPv4 and expect success response.

21.2.1 Create a Link-local address

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Create a Link-local address
Explanation	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.
Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get Link-local IPv6 from mdns
	Get the IPv6 link-local address only via mDNS.

21.2.2 Support Stateless Address Autoconfiguration (RA)

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Support Stateless Address Autoconfiguration (RA)
Explanation	LXI devices shall support RFC 4862 - IPv6 Stateless Address Autoconfiguration that supersedes RFC 2462.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	Enable IPv6 via Common Configuration
	Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)
	Enable IPv6 DHCPEnabled attribute
	Enable IPv6 DHCPEnabled attribute via Common Configuration.
	Enable IPv6 RAEnabled attribute
	Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Test Procedure

Get RA IPv6 from mdns

Get the RA address only via mDNS.

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

Category: LXI IPv6

Test Type: Kerberos Test, automated

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

Explanation: 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.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Test Procedure

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Stop IPv6 RA router

Stop the IPv6 RA assignment on the router.

Wait for DUT to loose RA IPv6

Wait for the device-under-test (DUT) to stop using the RA address.

21.2.5 Support Static IP Address Assignment

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: Support Static IP Address Assignment

Explanation

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 (RA) and Duplicate Address Detection (DAD)

Test Procedure

Is there a way to enter the IPv6 address

Prompt Tester: Is there a way to enter the IPv6 address

Is there a way to enter the IPv6 Network Prefix Length

Prompt Tester: Is there a way to enter the IPv6 Network Prefix Length

Is there a way to enter the IPv6 default gateway

Prompt Tester: Is there a way to enter the IPv6 default gateway

Is there a way to enter the IPv6 DNS IP addresses

Prompt Tester: Is there a way to enter the IPv6 DNS IP addresses

21.2.6 Support DHCPv6

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Support DHCPv6

Explanation: Devices shall support both Stateless and Stateful DHCPv6 addressing.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

21.2.7	21.2.8

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

Category: LXI IPv6

Test Type: Kerberos Test, automated

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

Explanation

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.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 DHCP router

Enable IPv6 DHCP address assignment on the router.
Ensure the DUT has no RA address any more.
Ensure the DUT has a DHCP address.

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Test Procedure

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Stop IPv6 DHCP router

Stop the IPv6 DHCP assignment on the router.

Wait for DUT to loose DHCP IPv6

Wait for the device-under-test (DUT) to stop using the DHCP address.

21.2.8 Honor New DHCP Options at Lease Renewal

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Honor New DHCP Options at Lease Renewal

Explanation: 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.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 DHCP router

Enable IPv6 DHCP address assignment on the router.
Ensure the DUT has no RA address any more.
Ensure the DUT has a DHCP address.

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Test Procedure

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Change IPv6 DHCP range router

Change the range of the IPv6 DHCP server.

Wait for DUT to accept new range

Depending on the lease time (in general 5min), wait until the IP address has changed

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Validate IP has new range

Validate the IP address matches the expected DHCP range.

21.2.9 Selection of IP Configuration Modes

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: Selection of IP Configuration Modes

Explanation: 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:
o Automatic (implying RA, DHCP)
o Manual (Static IP address only).

- Individual configuration settings to enable or disable the following options :
o RA
o DHCP
o 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.

Pre Condition

Connect DUT

Connect the DUT to the test network

Get IPv6 from mdns

Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Test Procedure — Check IPv6 configuration options

Prompt the Tester to check IPv6 configuration options.
Either a "Automatic" selection method must be found or a way to individually set RA/DHCP/Static must be available. It is also possible to have a "Static only" selection method.

21.2.10 Ability to Enable/Disable Privacy Setting

Category — LXI IPv6

Test Type — Kerberos Test, manual

Rule — Ability to Enable/Disable Privacy Setting

Explanation — 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 RA RFCs for privacy extensions in the NIST IPv6 Profile.

Pre Condition — Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Test Procedure — Disable Privacy Settings

Prompt the tester to disable privacy masking on the device-under-test (DUT).

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Validate IP address is not masked

Validate the IP address is not masked and the MAC address can be recognized within the IP address.

Enable Privacy Settings

Prompt the tester to enable privacy masking on the device-under-test (DUT).

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Validate IP address is masked

Validate the IP addresshas been masked by the privacy setting.

21.2.11 Privacy Setting Enabled by Default

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: Privacy Setting Enabled by Default

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

Pre Condition:

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Test Procedure:

Disable Privacy Settings

Prompt the tester to disable privacy masking on the device-under-test (DUT).

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Validate IP address is not masked

Validate the IP address is not masked and the MAC address can be recognized within the IP address.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Verify Privacy Setting is enabled

Verify the Privacy Setting is enabled by investigating the RA IPv6 address.

Validate IP address is masked

Validate the IP addresshas been masked by the privacy setting.

21.3.1 Display Link-local Address

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Display Link-local Address
Explanation	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.
Pre Condition	Connect DUT Connect the DUT to the test network Get IPv6 from mdns Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Query Home Item TCP/IP Address Prompt tester to check availability of the 'TCP/IP Address' on the 'Welcome Web Page' Evaluate IPv6 addresses Evaluate the given IPv6 addresses for link-local, RA and/or DHCP address. Query front panel link-local address Prompt the tester to enter the front-panel link-local address.
Post Condition	Match Displayed with mDNS IPv6 addresses Match the displayed/entered mDNS IPv6 addresses with the addresses given by mDNS.

21.3.2 Display a minimum of one other Preferred Address

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Display a minimum of one other Preferred Address
Explanation	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).
Pre Condition	Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Connect DUT Connect the DUT to the test network Get IPv6 from mdns Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Test Procedure	Query Home Item TCP/IP Address
	Prompt tester to check availability of the 'TCP/IP Address' on the 'Welcome Web Page'
	Evaluate IPv6 addresses
	Evaluate the given IPv6 addresses for link-local, RA and/or DHCP address.
	Query front panel global address
	Prompt the tester to enter the front-panel global address.
Post Condition	Match Displayed with mDNS IPv6 addresses
	Match the displayed/entered mDNS IPv6 addresses with the addresses given by mDNS.

21.4.1 Support Multicast DNS

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Support Multicast DNS
Explanation	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.
Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get IPv6 from mdns
	Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

21.4.2 Support mDNS on IPv6 only networks

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Support mDNS on IPv6 only networks
Explanation	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.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	Enable IPv6 via Common Configuration
	Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)
	Enable IPv6 DHCPEnabled attribute
	Enable IPv6 DHCPEnabled attribute via Common Configuration.
	Enable IPv6 RAEnabled attribute
	Enable IPv6 RAEnabled attribute via Common Configuration.

	Disable IPv6 staticAddressEnabled
	Disable IPv6 staticAddressEnabled attribute via Common Configuration.
	Connect DUT
	Connect the DUT to the test network
	Get IPv6 from mdns
	Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable IPv4 stack
	Prompt the tester to disable the IPv4 stack on the DUT. Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.
	Disconnect DUT
	Disconnect the DUT from the test network
	Start wireshark capture: Filter "mdns && ipv6"
	Start a wireshark capture filtering for mDNS and IPv6 protocol. Filter: "mdns && ipv6"
	Connect DUT
	Connect the DUT to the test network
	Stop wireshark capture
	Stop the wireshark from further package capturing
	Analyse wireshark capture for AAAA records
	Analyse the given wireshark capture for AAAA records advertised by the DUT.

21.4.5 Provide Manual DNS IP Address Entry

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Provide Manual DNS IP Address Entry
Explanation	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.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get IPv6 from mdns
	Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Is there a way to enter the IPv6 DNS IP addresses
	Prompt Tester: Is there a way to enter the IPv6 DNS IP addresses

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

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Provide way to Disable mDNS and DNS-SD for IPv6
Explanation	Devices shall provide a way to enable and disable mDNS and DNS-SD for IPv6.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable mDNS	
		Prompt the tester to disable mDNS
	Wait for service name to disappear from mdns	
		Wait until the service name has disappeared from mdns.
	Enable mDNS	
		Prompt the tester to enable mDNS
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

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

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	mDNS and DNS-SD Enabled by LAN Configuration Initialize (LCI)
Explanation	When the LCI reset mechanism is activated, it shall enable mDNS and DNS-SD for IPv4 and IPv6.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable mDNS	
		Prompt the tester to disable mDNS
	Wait for service name to disappear from mdns	
		Wait until the service name has disappeared from mdns.
	Do LCI	
		The tester is prompted to do a manual LAN reset on the DUT.
	Get IPv6 from mdns	
		Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

21.5.1 ICMPv6 Ping Reply

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	ICMPv6 Ping Reply

Explanation	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 ' or 'ping -6 ' 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.
Pre Condition	Connect DUT Connect the DUT to the test network Get IPv6 from mdns Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Ping the DUT via IPv6 for success Ping the DUT via IPv6 for success using the global IPv6 address.

21.5.3 Provide Way to Disable ICMPv6 Echo Reply Message

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Provide Way to Disable ICMPv6 Echo Reply Message
Explanation	LXI devices shall have a way to enable and disable the ICMP Echo Reply messages.
Pre Condition	Connect DUT Connect the DUT to the test network Get IPv6 from mdns Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Disable ICMPv6 Ping Responder Prompt the tester to disable ICMP Ping Responder for IPv6 Ping the DUT via IPv6 for failure Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail. Enable ICMPv6 Ping Responder Prompt the tester to enable ICMP Ping Responder for IPv6 Ping the DUT via IPv6 for success Ping the DUT via IPv6 for success using the global IPv6 address.

21.5.4 ICMPv6 Echo Reply Enabled by Default

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	ICMPv6 Echo Reply Enabled by Default
Explanation	ICMP Ping service ("Ping Responder") shall be enabled by default.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Disable Ping Responder

Prompt the Tester to disable the ICMP Ping Responder

Test Procedure

Ping the DUT via IPv6 for failure

Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Ping the DUT via IPv6 for success

Ping the DUT via IPv6 for success using the global IPv6 address.

21.6 Duplicate IP Address Detection

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: Duplicate IP Address Detection

Explanation: If a duplicate address is detected, the Device shall use the LXI LAN Status Indicator to signal a fault condition.

Pre Condition

Connect DUT

Connect the DUT to the test network

Get IPv6 from mdns

Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.

Test Procedure

Cause duplicate IP

Cause the device to issue a duplicate IP warning by setting the device to the same address as the test hardware. This may be done via he webpage LAN configuration or via the devices frontpanel.

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Evaluate duplicate IPv6 correction

When a duplicate IPv6 address detection occurs the device must not use the IPv6 address. It shall not be advertised by Mdns, nor shown elsewhere as active. The device wills till be reachable via other global mechanisms or via the link-local address. The LAN status indicator shall show as fault.

21.8 Provide an Error Indicator for LAN Configuration Faults

Category

LXI IPv6

Test Type

Kerberos Test, manual

Rule

Provide an Error Indicator for LAN Configuration Faults

Explanation

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

\u27A4 Failure to acquire a valid IP address
\u27A4 Detection of a duplicate IP address
\u27A4 Failure to renew an already acquired auto-configured address (RA or DHCP) valid lifetime (lease). Failure to obtain an initial RA or DHCP lifetime is not a failure.
\u27A4 LAN cable disconnected (as reported by Ethernet connection monitoring)

Pre Condition

Stop IPv6 DHCP router

Stop the IPv6 DHCP assignment on the router.

Stop IPv6 RA router

Stop the IPv6 RA assignment on the router.

Disconnect DUT

Disconnect the DUT from the test network

Test Procedure

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Connect DUT

Connect the DUT to the test network

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Stop IPv6 RA router

Stop the IPv6 RA assignment on the router.

Wait for DUT to loose RA IPv6

Wait for the device-under-test (DUT) to stop using the RA address.

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Enable IPv6 DHCP router

Enable IPv6 DHCP address assignment on the router.
Ensure the DUT has no RA address any more.
Ensure the DUT has a DHCP address.

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Stop IPv6 DHCP router

Stop the IPv6 DHCP assignment on the router.

Wait for DUT to loose DHCP IPv6

Wait for the device-under-test (DUT) to stop using the DHCP address.

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Open web page in browser

Prompt tester to open the devices web page

Activate LAN ID indicator

Prompt tester to activate the LAN ID indicator on web page

Is LAN ID indicator active

Query tester if LAN ID indicator is showing on device

Deactivate LAN ID indicator

Prompt tester to deactivate the LAN ID indicator on web page

Is LAN ID indicator deactivated

Query tester if LAN ID indicator is not showing on device

21.8.1 Combined IPv4 and IPv6 LAN Status Indicator

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Combined IPv4 and IPv6 LAN Status Indicator

Explanation	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 (RA). 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.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	21.8

21.8.2 IPv6 Link-Local address is not an error condition

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	IPv6 Link-Local address is not an error condition
Explanation	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 behaviour.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	21.8

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

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	LAN Status Indicator enabled by default for both IPv4 and IPv6

Explanation

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

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Test Procedure

Disable LAN status Indicator

Disable the LAN status indicator for IPv6 or IPv4 or both if possible.

Stop IPv6 RA router

Stop the IPv6 RA assignment on the router.

Wait for DUT to loose RA IPv6

Wait for the device-under-test (DUT) to stop using the RA address.

Is LAN Status Indicator showing OK

Prompt the Tester to check the LAN Status indicator for OK.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Stop IPv6 RA router

Stop the IPv6 RA assignment on the router.

Wait for DUT to loose RA IPv6

Wait for the device-under-test (DUT) to stop using the RA address.

Is LAN Status Indicator showing FAULT

Prompt the Tester to check the LAN Status indicator for FAULT.

21.9 LAN Configuration Initialize (LCI)

Category: LXI IPv6

Test Type: Kerberos Test, manual

Rule: LAN Configuration Initialize (LCI)

Explanation: 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. RA** **2. DHCPv6** **3. Static**	**1. Enabled** **2. Enabled if implemented** **3. Disabled if implemented**	**21.2.9**
Privacy Setting	**Disabled**	**21.2.11**
LAN Status Indicator	**Enabled for both IPv4 and IPv6**	**21.8.5**
ICMPv6 Echo Reply Message	**Enabled**	**21.5.4**
Web Password for configuration	**Factory Default**	**9.8**
mDNS and DNS-SD	**Enabled**	**10.3** **10.4** **10.7.1** **21.4.1**

Pre Condition:

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Get identification file

Get the identification file from the device under test

Test Procedure

Disable Privacy Settings

Prompt the tester to disable privacy masking on the device-under-test (DUT).

Change web password

Prompt the tester to change web password away from the default value. If LXI Security is configured, then this step is skipped as passwords are handled differently.

Disable mDNS

Prompt the tester to disable mDNS

Disable ICMPv6 Ping Responder

Prompt the tester to disable ICMP Ping Responder for IPv6

Disable LAN status Indicator

Disable the LAN status indicator for IPv6 or IPv4 or both if possible.

Disable IPv6 stack

Prompt the tester to disable the IPv6 stack on the DUT. This may not be possible.
Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.

Disable IPv4 stack

Prompt the tester to disable the IPv4 stack on the DUT.
Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

Validate IP address is masked

Validate the IP addresshas been masked by the privacy setting.

Is web password reset

Prompt the tester to get password is reset to default or not. If LXI Security is configured, then this step is skipped as passwords are handled differently.

21.11.1 Implement all Rules in the Web Interface Section

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Implement all Rules in the Web Interface Section
Explanation	Implement all the Rules in Section 9 – Web Interface.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	Web Interface

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

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Include 'LXI IPv6' in Welcome Web Page "LXI Extended Functions"
Explanation	Devices implementing the LXI IPv6 function shall include 'LXI IPv6' in the 'LXI Extended Functions' display item of the welcome web page.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	1.4.6

21.11.3 Show LinkLocal and Preferred IPv6 Addresses on Welcome Web Page

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Show LinkLocal and Preferred IPv6 Addresses on Welcome Web Page
Explanation	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 RA, 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 RA, DHCPv6 or Static addressing such as Unique-Local addresses.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	21.3.1, 21.3.2

21.11.6 Show Static IPv6 Settings on LAN Configuration Web Page

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Show Static IPv6 Settings on LAN Configuration Web Page

Explanation

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 Mode1
- IPv6 address 2
- Prefix Length
- Default Gateway3
- 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 (RA and DHCPv6 ¡V if implemented), as described in section 21.2 to obtain the instrument IP address(es).

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Test Procedure

Open web page in browser

Prompt tester to open the devices web page

Open IPv6 LAN configuration web page

Prompt the tester to open the IPv6 LAN configuration webpage of the device-under-test (DUT).

Query IPv6 LAN Item IPv6 Configuration Mode

Prompt tester to check availability to configure the 'IPv6 Configuration Mode' on the 'IPv6 LAN Configuration Web Page'

Query IPv6 LAN Item IPv6 address

Prompt tester to check availability to configure the 'IPv6 address' on the 'IPv6 LAN Configuration Web Page'

Query IPv6 LAN Item Prefix Length

Prompt tester to check availability to configure the 'Prefix Length' on the 'IPv6 LAN Configuration Web Page'

Query IPv6 LAN Item Default Gateway

Prompt tester to check availability to configure the 'Default Gateway' on the 'IPv6 LAN Configuration Web Page'

Query IPv6 LAN Item DNS Server(s)

Prompt tester to check availability to configure the 'DNS Server(s)' on the 'IPv6 LAN Configuration Web Page'

21.11.7 Add a Stack Disable Option to the Configuration Mode.

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Add a Stack Disable Option to the Configuration Mode.
Explanation	Devices shall have independent options to disable IPv4 and IPv6.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.

Dependencies		
	21.1.8	21.1.10

21.11.8 Display of Status for Disabled IP Protocols

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Display of Status for Disabled IP Protocols
Explanation	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.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get RA IPv6 from mdns
	Get the RA address only via mDNS.
Test Procedure	Disable IPv6 stack
	Prompt the tester to disable the IPv6 stack on the DUT. This may not be possible. Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.

Open web page in browser

Prompt tester to open the devices web page

Query Home Item Value TCP/IP Address

Prompt tester for the 'TCP/IP Address' on the 'Welcome Web Page'

Evaluate IP addresses

Evaluate the given addresses for IPv4 addresses (DHCP, Auto-IP) and IPv6 addresses (link-local, RA and/or DHCP address).

Disable IPv4 stack

Prompt the tester to disable the IPv4 stack on the DUT.
Note: Some devices may not be able to disable the stack, but traffic can still be prevented via the firewall.

Open web page in browser

Prompt tester to open the devices web page

Query Home Item Value TCP/IP Address

Prompt tester for the 'TCP/IP Address' on the 'Welcome Web Page'

Evaluate IP addresses

Evaluate the given addresses for IPv4 addresses (DHCP, Auto-IP) and IPv6 addresses (link-local, RA and/or DHCP address).

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

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Support IEEE-1588 via UDP over IPv6 for the Link-Local Scope
Explanation	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).
Pre Condition	Connect DUT Connect the DUT to the test network Get RA IPv6 from mdns Get the RA address only via mDNS. Open web page in browser Prompt tester to open the devices web page Open 1588 Sync configuration web page Prompt tester to open the 1588 Sync configuration web page Switch to 1588 IPv6 Prompt tester to switch the 1588 to use IPv6 instead of IPv4 Start management node Start up the PTP management node Start ordinary clock Start up the PTP clock Initialize all clocks Send a management message INITIALIZE to all clocks.
Test Procedure	Set DUT to Slave Set the local clock to master by setting a high priority value (e.g. 0) and ensuring the DUT is set to a lower priority value (e.g. 128)

	Ensure DUT is Slave	
		Wait for the DUT to be slave and the local clock master.
	Wait for stable meanPathDelay of Slave	
		Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.
	Set DUT to Master	
		Set DUT as target, get local port identity and DUT announce interval plus the calculated interval. Subsequently Switch local clock to slave. Give the DUT time and Ensure DUT is Master and stable mean path delay.
	Ensure DUT is Master	
		Wait for the DUT to be master and the local clock slave.
	Wait for stable meanPathDelay of Slave	
		Wait for the meanPathDelay to be stable. Retrieve the meanPathDelay via a CURRENT_DATA_SET management message to the Slave.
Post Condition	Reset local clock	
		Reset all clock modifications done to the local clock during this test (e.g. priority, log announce interval, special stack modifications etc.)
	Shutdown ordinary clock	
		Shutdown the PTP clock
	Shutdown management node	
		Shutdown the PTP management node
	Switch to 1588 IPv4	
		IPv4 and IPv6 shall be exclusivly enabled. This teststep shall switch the DUT to use 1588 with IPv4.

21.12.3 Support selecting IPv4 or IPv6 for IEEE-1588

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Support selecting IPv4 or IPv6 for IEEE-1588
Explanation	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.

Pre Condition	Connect DUT	
		Connect the DUT to the test network
	Get RA IPv6 from mdns	
		Get the RA address only via mDNS.
Test Procedure	Open web page in browser	
		Prompt tester to open the devices web page
	Open 1588 Sync configuration web page	
		Prompt tester to open the 1588 Sync configuration web page

Query 1588 Sync Item Select IPv4/IPv6

Prompt tester to check availability to configure the 'IPv4/IPv6 mode' on the '1588 Sync Configuration Web Page'

Is Select IPv4/IPv6 mutually exclusive

Prompt tester to check the 'IPv4/IPv6 mode' on the '1588 Sync Configuration Web Page' is mutually exclusive

21.12.4 Changes to LXI Sync Web Page

Category	LXI IPv6
Test Type	Kerberos Test, manual
Rule	Changes to LXI Sync Web Page
Explanation	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.
Pre Condition	Connect DUT Connect the DUT to the test network Get RA IPv6 from mdns Get the RA address only via mDNS.
Test Procedure	Open web page in browser Prompt tester to open the devices web page Open 1588 Sync configuration web page Prompt tester to open the 1588 Sync configuration web page Switch to 1588 IPv6 Prompt tester to switch the 1588 to use IPv6 instead of IPv4 Have all IP addresses converted to IPv6 Prompt tester to check all IP addresses on the '1588 Sync Configuration Web Page' have converted to IPv6 addresses.

21.13.2 Use IPv6 Multicast Address and Port Number

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Use IPv6 Multicast Address and Port Number
Explanation	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.

Test Procedure: NOT SUPPORTED

This test is currently not implemented. If the configuration would expect this test to run, then it will fail. Otherwise it will pass with message 'not supported'.

21.14 LAN Discovery and Identification Changes

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: LAN Discovery and Identification Changes

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

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

21.14.1	21.14.2	21.14.3
21.14.5	21.14.6	21.14.7

21.14.1 Support IPv6 access to Identification XML Document

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Support IPv6 access to Identification XML Document

Explanation: The LXI XML Identification document shall be accessible via IPv6.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Test Procedure: Get identification file

Get the identification file from the device under test

21.14.2 Include LXI IPv6 Address in <Interface>

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Include LXI IPv6 Address in
Explanation	If an IPv6 global address is available devices shall include it in an XML element. If no IPv6 global address is available, devices shall include the link-local IPv6 address in an XML element.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Disable IPv6 router Disable the IPv6 router so that neither RA nor DHCPv6 addresses are being assigned. Disconnect DUT Disconnect the DUT from the test network Connect DUT Connect the DUT to the test network Get Link-local IPv6 from mdns Get the IPv6 link-local address only via mDNS. Get identification file Get the identification file from the device under test
Test Procedure	Get IPv6 tag Get the IPv6 tag from the lxi identification file. Evaluate IPv6 addresses Evaluate the given IPv6 addresses for link-local, RA and/or DHCP address. Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Get identification file Get the identification file from the device under test Get IPv6 tag Get the IPv6 tag from the lxi identification file.

Evaluate IPv6 addresses

Evaluate the given IPv6 addresses for link-local, RA and/or DHCP address.

21.14.3 IP Type is “IPv6”

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	IP Type is “IPv6”
Explanation	Devices shall use “IPv6” as the IP type for the IPv6 address element.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Connect DUT Connect the DUT to the test network Get RA IPv6 from mdns Get the RA address only via mDNS. Get identification file Get the identification file from the device under test
Test Procedure	Get IPv6 tag Get the IPv6 tag from the lxi identification file. Evaluate Interface attribute 'Type' Evaluate the IPv6 interface tag attribute Type for the value: “IPv6”

21.14.5 Include LXI IPv6 Address in <Gateway>

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Include LXI IPv6 Address in
Explanation	If an IPv6 address for the gateway is available, devices shall include it in the element of the IPv6 element.

Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Connect DUT Connect the DUT to the test network Get RA IPv6 from mdns Get the RA address only via mDNS. Get identification file Get the identification file from the device under test
Test Procedure	Get IPv6 tag Get the IPv6 tag from the lxi identification file. Evaluate element Evaluate the IPv6 interface element tag is available.

21.14.6 Show LXI Prefix length in <SubnetMask>

Category	LXI IPv6
Test Type	Kerberos Test, automated
Rule	Show LXI Prefix length in
Explanation	Devices shall show the prefix length in the element of the IPv6 element.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Get identification file

Get the identification file from the device under test

Test Procedure

Get IPv6 tag

Get the IPv6 tag from the lxi identification file.

Evaluate element

Evaluate the IPv6 interface element tag is available.

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

Category: LXI IPv6

Test Type: Kerberos Test, automated

Rule: Include the LXI IPv6 Function in the element

Explanation: LXI devices implementing IPv6 shall include a element in the XML element with the FunctionName attribute of “LXI IPv6” and a Version attribute containing the version number of this document.

Example:

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

	Enable IPv6 RA router	
		Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address.
	Connect DUT	
		Connect the DUT to the test network
	Get RA IPv6 from mdns	
		Get the RA address only via mDNS.
	Get identification file	
		Get the identification file from the device under test
Test Procedure	Get 'ExtendedFunctions'	
		Get all Extended Functions given by the LXI identification file.
	Evaluate IPv6 extended function	
		Evaluate the IPv6 extended function tag from the XML identification file. Ensure a version is given along with the function name.

22.0 LXI Security Extended Function

Categories: LXI Security

22.8 LXI Security Web Interface

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Security Web Interface

Explanation: Devices implementing the LXI Security Extended Function shall include 'LXI Security' in the 'LXI Extended Functions' display item of the welcome web page.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: 1.4.6

22.8.1 LXI Security Web Page unsecure Mode Indication

Category: LXI Security

Test Type: Kerberos Test, manual

Rule: LXI Security Web Page unsecure Mode Indication

Explanation: LXI Secure devices shall provide an indication on the LXI welcome web page if they are currently operating in the unsecure Mode.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

Loop next 6 Steps for unsecure mode indication

Loop over the next 6 Steps for unsecure mode indication of several attributes. Currently following list is taken into account, but may be extended in the furture:
Http::operation
IPv6::privacyModeEnabled
Hislip::mustStartEncrypted
Hislip::encryptionMandatory
Telnet::tlsRequired
VXI11::enabled
ScpiRaw::enabled.

Set unsecure Mode for specific Interface attribute

Enable each attribute, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

Set Non-unsecure Mode for specific Interface attribute

Set back the Interface attribute value to Non-unsecure.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

22.9 LXI Security XML Identification Document

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Security XML Identification Document
Explanation	LXI devices implementing LXI Security extended function shall include Function elements for the LXI Security Extended Function. The Function element are contained in the XML Device element. With the FunctionName attribute of “LXI Security” and a Version attribute containing the version number of this document.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Get identification file

Get the identification file from the device under test

Test Procedure

Get 'ExtendedFunctions'

Get all Extended Functions given by the LXI identification file.

Evaluate Security Extended Function

Evaluate the Security extended function tag from the XML identification file.

22.10.1 unsecure Mode

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: unsecure Mode

Explanation: An LXI Secure device is considered unsecure if its configuration enables protocols or behaviours that are known to be unsecure. If any part of a device configuration is known to explicitly enable unsecure operation, the device operates in unsecure mode.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

23.10.8	23.10.9	23.10.10
23.10.11	23.10.12	23.10.13
23.10.14	23.10.15	23.10.16
23.10.17	23.10.18	

22.10.1.1 Vendors Shall Indicate unsecure for non-LXI device Settings

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Vendors Shall Indicate unsecure for non-LXI device Settings

Explanation: Devices shall also indicate they are operating in an unsecure Mode if settings beyond the scope of LXI Security are considered by the device manufacturer to be unsecure.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure indicator state

Verify the unsecure indicator state through Common Configuration. It can be true/false as per expected result. If the MustStartEncrypted is set to true and EncryptionMandatory is set to false, the unsecure flag should be true and vice versa. In the case both attributes are true,the unsecure flag should be false

Test Procedure

Verify each vendor specific protocol that have impact on unsecure Mode

Find out and verify all the additional Interface elements that impact unsecure Mode.

Set unsecure Mode for specific Interface attribute

Enable each attribute, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is true

Check the unsecure mode of the interface is set to true in the Common Configuration.

Set Non-unsecure Mode for specific Interface attribute

Set back the Interface attribute value to Non-unsecure.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

22.10.2 Multiple LAN Interfaces supporting LXI Security

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Multiple LAN Interfaces supporting LXI Security
Explanation	If multiple LAN network interface cards (NICs) are present in an LXI Secure device, those that are LXI compliant shall support the LXI Security Extended Function.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	7.7

22.11.1 Support IPv4 Secure Configuration

Category	LXI Security
Test Type	Vendor Declaration
Rule	Support IPv4 Secure Configuration
Explanation	All LXI Devices implement IPv4. LXI Secure devices shall implement the secure requirements for IPv4 in this section and the LXI API Extended Function specification.

22.11.2 Support IPv6 Secure Configuration

Category	LXI Security
Test Type	Vendor Declaration
Rule	Support IPv6 Secure Configuration
Explanation	Devices that implement IPv6 capability and LXI Security shall implement the secure requirements for IPv6 in this section and the LXI API Extended Function specification. This requirement shall be followed regardless of if a device complies with the LXI IPv6 extended function.

22.11.3 Ignore mDNS Unicast Queries From Outside the Local Link

Category	LXI Security
Test Type	Vendor Declaration
Rule	Ignore mDNS Unicast Queries From Outside the Local Link
Explanation	Since it is possible for an mDNS unicast query to be received from a machine outside the local link, LXI Secure devices shall check that the source address in the mDNS query packet matches the local subnet for that link (or, in the case of IPv6, the source address has an on-link prefix) and silently ignore the packet if not. This behaviour is as recommended in RFC6762

22.12.1 IEEE 802.1AR Compliance

Category	LXI Security
Test Type	Vendor Declaration
Rule	IEEE 802.1AR Compliance
Explanation	LXI Security compliant devices shall comply with the device requirements stated in IEEE 802.1AR with the following caveats: 1. IEEE 802.1AR has a detailed description of the DevID module. In general, LXI Secure device software has no such module externally visible, thus those requirements do not directly bear on an LXI device although the device implementation is expected to substantially follow those requirements. This may be ideally accomplished through either a physical or firmware HSM in conjunction with the LXI Security API. LXI Security does require an API that includes several certificate management features similar to the DevID Module requirements, see the LXI API Extended Function. 2. IEEE 802.1AR 6.4 implies that DevID certificates can be validated using a CA root certificate as the trust anchor. Although not clearly in conflict with IEEE 802.1AR, LXI Security explicitly permits devices to use self-signed certificates in their DevID, thus making the self-signed certificate itself the trust anchor. 3. IEEE 802.1AR section 5.5, Supplier Requirements, places several requirements on the supplier which are beyond the scope of LXI and are not placed on the device vendor by LXI.

22.12.2 Use the Most Recently Provisioned DevID

Category	LXI Security
Test Type	Kerberos Test, automated

Rule	Use the Most Recently Provisioned DevID
Explanation	If any LDevID has been provisioned to the device, the IDevID shall not be used, regardless of the cryptographic suite of the LDevID. Unless explicitly configured otherwise, devices shall use the most recently provisioned valid certificate for each cryptographic suite that the device supports to authenticate itself regardless of the protocol being used.
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Remove all Certificates Delete all certificates on the dut via the delete-certificate API. Get the IDevId Certificate Get the IDevId Certificate from the DUT by requesting a list of certificates via the API.
Test Procedure	Verify device is using IDevID Get the IDevId certificate and check its the used one. Create self-signed certificate with unsupported signature algorithm Use create-certificate api to send an api request with an unsupported signature algorithm. Expect a Bad Request as response, with a list of all supported ones. Read LxiProblemDetails for supported signature algorithms Read out the list of supported signature algorithms from the LxiProblemDetails Create self-signed certificate for each supported signature algorithm Create a self-signed certificate for each signature algorithm via the create-certificate API Check latest certificate is used Check that the latest certificate is always used when creating a new certificate. Get each new certificate via API Get each of the new certificates via the API and the GUID. Verify certificate has correct crypto hash Check that every certificate was created with the correct crypto hash. Get active certificate Get the currently used certificate (LDevID) for MTLS authentication and for the webpage. Disable active certificate Disable currently used certificate via /lxi/api/certificates/<GUID>/enabled using API-Key Verify active certificate Verify that the device is using the correct certificate and check its the used one. Delete active certificate Delete the currently used certificate via API. Verify active certificate Verify that the device is using the correct certificate and check its the used one.

22.12.3.1 Distinguished Name

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Distinguished Name
Explanation	Subject Distinguished Name (DN) – field shall have the attributes as explained in the documentation
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
Test Procedure	Get IDevID Certificate from the device Get the IDevID Certificate from the device via API. Use the identified GUID from the certificate list to receive the correct certificate. Check certificate for attributes Check whether the certificate attributes CommonName, Organization, OrganizationUnit and SerialNumber have been set. Create self-signed certificate with attributes Create a self-signed certificate via API, with the CommonName, Organization, OrganizationUnit, and SerialNumber attributes set. GET Certificate for GUID GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID. Check certificate for attributes Check whether the certificate attributes CommonName, Organization, OrganizationUnit and SerialNumber have been set.

22.12.3.2 Subject Alternate Name

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Subject Alternate Name
Explanation	Devices that have a hardware or firmware HSM shall have a SAN field, see documentation
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Vendor declared HSM availability Check if a HSM is available by checking the test configuation. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check HSM value Check the vendor declaration whether a Hardware Security Module (HSM) is required. Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Test Procedure	Get IDevID Certificate from the device
	Get the IDevID Certificate from the device via API. Use the identified GUID from the certificate list to receive the correct certificate.
	Get 'HW Module Name' from certificate
	Retrieve the Certificate Subject Alternative Names and look for the value 'HW Module Name', if the vendor declaration is set to require a Hardware Module name.
	Create self-signed certificate with attributes
	Create a self-signed certificate via API, with the CommonName, Organization, OrganizationUnit, and SerialNumber attributes set.
	GET Certificate for GUID
	GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID.
	Get 'HW Module Name' from certificate
	Retrieve the Certificate Subject Alternative Names and look for the value 'HW Module Name', if the vendor declaration is set to require a Hardware Module name.

22.13.1 Secure Command-and-Control Interface

Category	LXI Security
Test Type	Vendor Declaration
Rule	Secure Command-and-Control Interface
Explanation	LXI Secure devices shall provide at least one secure Command-and-Control interface. That is, a protocol that provides encryption and server authentication (e.g., IVI HiSLIP rev2.0, HTTPS, etc.).

22.13.2 Client Authentication Configuration

Category	LXI Security
Test Type	Vendor Declaration
Rule	Client Authentication Configuration
Explanation	At least one Command-and-Control protocol shall provide a configuration that requires client authentication.

22.13.3 unsecure Command-and-Control Interfaces

Category	LXI Security
Test Type	Vendor Declaration
Rule	unsecure Command-and-Control Interfaces
Explanation	LXI Secure devices implementing unsecure Command-and-Control interfaces shall provide settings to control which of these protocols are enabled.

22.13.4 HiSLIP Devices Supported SASL Mechanisms

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HiSLIP Devices Supported SASL Mechanisms
Explanation	LXI Secure devices that implement the HiSLIP extended function shall support client authentication using the SASL mechanisms of ANONYMOUS, PLAIN, and SCRAM.

Test Procedure	Computed by other tests

This test is computed by the result of other tests.

Dependencies			
	23.12.13.1-1	23.12.13.1-2	23.12.13.1-5
	23.12.13.1-7		

22.13.5 Devices Shall Support IVI 6.5, SASL Mechanism Specification

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Devices Shall Support IVI 6.5, SASL Mechanism Specification
Explanation	LXI Secure devices that implement the HiSLIP extended function shall support client authentication using the SASL mechanisms of ANONYMOUS, PLAIN, and SCRAM.
Test Procedure	Computed by other tests

This test is computed by the result of other tests.

Dependencies		
	23.12.13.1-6	23.12.17.1-2

22.14 LXI API Security Methods

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI API Security Methods
Explanation	Devices shall provide the APIs defined in the LXI API Extended Function.
Test Procedure	Computed by other tests

This test is computed by the result of other tests.

Dependencies	
	LXI Security

23.0 LXI API Extended Function

Categories: LXI Api

23.5.1 Devices Comply with Current Schemas

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Devices Comply with Current Schemas

Explanation: The LXI schema's may be updated from time to time. The LXI Conformance Policy indicates the minimum versions devices are required to conform to as part of conformance to a device specification version. Devices shall support schemas that are current at the time of their development, which may be minor revisions more recent than the minimum requirement of the conformance policy. Devices shall clearly indicate versions of the schema they support. Devices may also support older schema versions.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

23.10.8	23.10.9	23.10.10
23.10.11	23.10.12	23.10.13
23.10.14	23.10.15	23.10.16
23.10.17	23.10.18	

23.6 'LXI API" is not included on the Welcome Web Page

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: 'LXI API" is not included on the Welcome Web Page

Explanation: Devices implementing the 'LXI API' Extended Function do not include a reference to the 'LXI API' Extended Function in the display item of the welcome web page.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

1.4.6

23.7 LXI API Extended Function is not included in the LXI Identification

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI API Extended Function is not included in the LXI Identification

Explanation: Devices implementing LXI API Extended Function shall not include a element in the XML element with the FunctionName attribute of "LXI API" and a Version attribute containing the version number of this document.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Get identification file

Get the identification file from the device under test

Test Procedure	Get 'ExtendedFunctions'
	Get all Extended Functions given by the LXI identification file.
	Evaluate API Extended Function
	Evaluate the API extended function tag is not available in the XML identification file.

23.10.1 API Client Authentication and Authorization

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	API Client Authentication and Authorization
Explanation	API clients shall be able to authenticate themselves by providing an HTTP request header that supplies an authentication key. The authentication key may be generated by the device, or by the device working in concert with external applications. The authentication key is not generated by the client. When using API key authentication, the HTTP header X-API-Key shall be included with the HTTP request to provide the API key to the device. The procedure used by the customer to acquire the API key is beyond the scope of LXI. However, devices shall not provide the API key over Ethernet using an unsecure connection.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Send an api request for each Lxi-Api without an authorization tag
	For each Lxi-Api (Common Configuration, Device Specific Configuration, all-certificates, specific-certificate, create-certificate, enable-certificate and csr-certificate) send a API request without authorization tag. Expect a '401 Unauthorized client' response, because its not allowed to get access to the Lxi-Api without authentication and authorization.
	Expect '401 Unauthorized client' response
	Expect a '401 Unauthorized client' response, because its not allowed to get access to the Lxi-Api without authentication and authorization.
	Send API request for each Lxi-Api without '/api/'
	For each Lxi-Api (Common Configuration, Device Specific Configuration and identification) send an API request without /api/ in the URL and no authorization tag. Expect a '200 OK' response, because none Lxi-Api's doesn't need an authorization tag
	Expect '200 OK' response
	Expect a '200 OK' response, because the request was valid.

23.10.1.1 API Key Authentication

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	API Key Authentication

Explanation	API clients shall be able to authenticate themselves by providing an HTTP request header that supplies an authentication key. The authentication key may be generated by the device, or by the device working in concert with external applications. The authentication key is not generated by the client. When using API key authentication, the HTTP header X-API-Key shall be included with the HTTP request to provide the API key to the device. The procedure used by the customer to acquire the API key is beyond the scope of LXI. However, devices shall not provide the API key over Ethernet using an unsecure connection.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Send API request for each Lxi-Api with an authorization tag For each Lxi-Api (Common Configuration, Device Specific Configuration, all-certificates, specific-certificate, create-certificate, enable-certificate and csr-certificate) send a API request with authorization tag. Expect Other response than 401 Unauthorized client response Expect other response than '401 Unauthorized client response' Expect other response than 401 Unauthorized client response, because the authentication is valid.

23.10.1.2 HTTPS Basic and Digest Authentication

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HTTPS Basic and Digest Authentication
Explanation	API clients shall be able to authenticate themselves by providing HTTP Basic or Digest authentication per RFC7616/RFC7617 or whatever successors are current when the device is designed. The realm for the LXI API shall be “LXI-API”. Per section 23.10.1.3, RULE – API Requires Authorization, authenticated users must also be authorized to use the full API. The users list in the ClientCredential element permits users to be designated as authorized.
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Configure Username and password on the device PUT the Common Configuration with a username and password pair with api access to the device. Enable https 'API-LXISecurity' service with basic authentication Enable https 'API-LXISecurity' service with basic authentication via common configuation PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure	Send api request for each api with basic authentication For each Lxi-Api (Common Configuration, Device Specific Configuration, all-certificates, specific-certificate, create-certificate, enable-certificate and csr-certificate), send a api request with basic authentication. Expect valid responses, unless otherwise stated in the next test step.

23.10.1.3 API Requires Authorization

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	API Requires Authorization
Explanation	The authority of authenticated users shall be verified before they are permitted to change the LXI Security Settings via any Ethernet protocol or interface. This specification requires two mechanisms by which users may be authorized: Authorized users may be specified to the device using the API defined in section 17, RULE – LXI Common Configuration PUT API. The user list in the ClientCredential element can be used to designated users as authorized using the APIAccess attribute. Thus, users presenting the name and password indicated in the ClientCredential are permitted to perform privileged operations. Users presenting a valid API Key are authorized. Other authorization determinations beyond the scope of LXI may be used as well. Such mechanisms must be used to initially authorize a user to use the API.
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Configure Username and password on the device without API access PUT the Common Configuration with a username and password pair with no api access to the device. Enable https 'API-LXISecurity' service with basic authentication Enable https 'API-LXISecurity' service with basic authentication via common configuation Enable clientAuthenticationRequired Set the clientAuthenticationRequired attribute value to true. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Send api request for each api with basic authentication For each Lxi-Api (Common Configuration, Device Specific Configuration, all-certificates, specific-certificate, create-certificate, enable-certificate and csr-certificate), send a api request with basic authentication. Expect valid responses, unless otherwise stated in the next test step. Expect '401 Unauthorized client' response Expect a '401 Unauthorized client' response, because its not allowed to get access to the Lxi-Api without authentication and authorization. Send API request with incorrect API key Send an API request (e.g. Common Configuration) with an invalid API-Key and expect an 401 Unauthorized client response.

Expect '401 Unauthorized client' response

Expect a '401 Unauthorized client' response, because its not allowed to get access to the Lxi-Api without authentication and authorization.

23.10.2 Additional Means of Authorization

Category: LXI Security

Test Type: Vendor Declaration

Rule: Additional Means of Authorization

Explanation: LXI devices are permitted to implement additional means beyond the scope of this specification to authorize the API, however such means shall ensure that clients are fully authenticated and authorized.

23.10.3 LXI Certificate and CSR GUIDs

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Certificate and CSR GUIDs

Explanation: Several of the LXI APIs reference either certificates, certificate chains or CSRs using a GUID. The GUID is created and managed by the device and shall be made up of an arbitrary string of alpha-numerics and hyphens. CSRs may be deleted by the user or, from time-to-time, expire on the device. See section 23.10.16.1, RULE – Minimum CSR Retention, for LXI requirements. The device shall ensure that GUIDs do not replicate under foreseeable circumstances including malicious client actions. When a certificate is posted to the device it shall receive a new GUID, and the GUID for the corresponding CSR shall not be used again.

Pre Condition:

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure:

Create self-signed certificate with attributes

Create a self-signed certificate via API, with the CommonName, Organization, OrganizationUnit, and SerialNumber attributes set.

Get CSR

Get CSR certificate via the /lxi/api/get-csr API.

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Check GUIDs are alpha-numeric strings

Check the GUID only contains alpha-numeric characters.

Check GUIDS are unique

Check the given GUIDS are unique within a certificates list recevied from the DUT.

23.10.4.1 XML Payloads Comply with LXI Schemas

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: XML Payloads Comply with LXI Schemas

Explanation: LXI provides XSD schemas for each of the LXI APIs that uses an XML payload. Devices shall produce schema-valid XML and accept and properly act on any schema-valid XML. Numerous requirements regarding the use and interpretation of the schema are included in the following sections regarding the schemas and shall be followed by devices.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.10.8	23.10.9	23.10.10
23.10.11	23.10.12	23.10.13
23.10.14	23.10.15	23.10.16
23.10.17	23.10.18	

23.10.4.2 Response and Request headers

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Response and Request headers

Explanation: Devices shall return the specified response headers. Devices shall observe the request headers and ensure that a client presenting request payloads based on the LXI-specified payloads and syntaxes are accepted.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.10.8	23.10.9	23.10.10
23.10.11	23.10.12	23.10.13
23.10.14	23.10.15	23.10.16
23.10.17	23.10.18	

23.10.4.3 HTTP Return Codes

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: HTTP Return Codes

Explanation: If an operation fails, the device shall return the appropriate HTTP status code.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.10.8	23.10.9	23.10.10
23.10.11	23.10.12	23.10.13
23.10.14	23.10.15	23.10.16
23.10.17	23.10.18	

23.10.4.4 LXI Problem Details

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Problem Details

Explanation: When returning errors, devices shall return information regarding the failure using the LXIProblemDetails XML. The HTTP Response Header returned with LXI Problem Details shall be 'Content-Type:application/xml'.

Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Send a bad request Send a api request with an error like a syntax error to the device, using the API-Key. Check response for Problem Details xml Check the response from the previous API call for a Problems Details xml. Check xml against xsd Validate the xml against the corresponding xsd schema.

23.10.4.5 Operation Pending Response Handling

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Operation Pending Response Handling
Explanation	If an LXI API returns status 202, that is request pending, it shall return the LXIPendingDetails XML. The pending details permits the client to determine details about pending actions and determine when they are complete. Devices shall include a response header of: Content-Type: application/xml The LXIPendingDetails XML includes a URL at which the client can perform an HTTP GET to determine the status of the pending operation. The response from that URL shall either be status 200, OK, or a status of 202, accepted with a new LXIPendingDetails XML.
Test Procedure	Send vendor given API Send the API given by tet configuration. Call URL given by Pending details Call the URL given by the Pending details API response. Evaluate if user action needed and time to wait Evaluate if user action is requried and/or time to wait is set.

23.10.4.5.1 Operations That Require User Action Return Operation Pending

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Operations That Require User Action Return Operation Pending
Explanation	If an LXI API requires user action, it shall return a status of 202, with the LXIPendingDetails XML without waiting for user intervention.
Test Procedure	Send vendor given API Send the API given by tet configuration. Call URL given by Pending details Call the URL given by the Pending details API response. Evaluate if user action needed and time to wait Evaluate if user action is requried and/or time to wait is set.

23.10.4.5.2 Accepted Response URL Expiration

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Accepted Response URL Expiration
Explanation	As long as the operation remains pending each response shall return a status of 202 and an LXIPendingDetails XML. The subsequent responses are permitted to use a different URL, therefore the client must base subsequent GETs on the updated URL. The client performs a GET on the URL (which may return a fresh LXIPending response) or, The client executes another HTTP method that returns a pending status or, 1 hour has elapsed or, The device is rebooted. If the pending operation requires a reboot to complete, the URL may be invalid after the reboot, however, the device should attempt to provide a URL that will remain valid.
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies	
23.10.4.5	23.10.4.5.1

23.10.6.3 Schema location on the device

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Schema location on the device
Explanation	Devices shall provide schemas for each payload produced or consumed by the device. The schemas, on a device, shall be located at the device URL from the HTTP(S) server ports that serve the specific API, in the directory lxi. Thus, the URL for the 1.0 release of the LXI Common Configuration schema shall be:http(s):///lxi/schemas/LXICommonConfiguration/1.0The schemas are also available on the LXI website in the directory schemas. Thus, the URL for the 1.0 release of the LXI Common Configuration schema is: http(s)://lxistandard.org/lxi/schemas/LXICommonConfiguration/1.0
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Validate schema location for GET APIs Validate schema location for every GET API Url. Validate schema location for APIs with Xml payload Validate schema location for every API Url, except GET, which has an Xml as payload.

23.10.7 XML Identification Document

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	XML Identification Document
Explanation	All LXI Devices shall provide an XML identification document that can be queried via a GET at “http://:80/lxi/identification” that conforms to the LXI XSD Schema (available at http://www.lxistandard.org/InstrumentIdentification/1.0) and the W3C XML Schema Standards (http://www.w3.org/XML/Schema).

Pre Condition	Connect DUT
	Connect the DUT to the test network
Test Procedure	Get identification file
	Get the identification file from the device under test
	Validate identification file
	Validate the identification file from the device under test

23.10.7.1 Content Type Header

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	Content Type Header
Explanation	The response to the GET request on the URL defined in 10.2 or to the URL that actually returns the XML document after possible redirection(s) shall include the “Content-Type” header with “text/xml” as the value.
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get identification file
	Get the identification file from the device under test
Test Procedure	Validate Content header
	Validate the identification files content header for type : "text/xml"

23.10.7.2 Schema Location Attribute

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	Schema Location Attribute
Explanation	The xsi:schemaLocation attribute of the root element of the identification document shall contain an entry for the LXI XSD namespace with an accompanying absolute URI on the instrument that shall return the actual XSD schema document from the instrument (https://www.w3.org/standards/xml/schema). The W3C XSD Schema itself does not need to be available via a URI on the instrument. Example: LXIDevice xmlns="http://www.lxistandard.org/InstrumentIdentification/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.lxistandard.org/InstrumentIdentification/1.0 http://1.2.3.4/identification.xsd">
Pre Condition	Connect DUT
	Connect the DUT to the test network
	Get identification file
	Get the identification file from the device under test
Test Procedure	Validate Schema Location
	Validate the identification files Schema Location

23.10.8 LXI Common Configuration GET API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Common Configuration GET API

Explanation	The LXI Common Configuration GET API returns the overall device LXI configuration. The configuration returned in the XML payload may meaningfully be applied to all devices in a system.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check response header content-type for xml Check the previous API calls response header content-type for xml. Validate Xml against local schema Validate the response Xml against the appropriate local schema. GET Common Configuration without authentication GET the CommonConfiguration from the device without authentication. Expect the call to fail as no authentication was given. '401 Unauthorized' error expected. Validate Xml against the schema on the device Validate the response Xml against the appropriate schema on the device.

23.10.8.1 The lxi/common-configuration Endpoint Elides User Lists

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	The lxi/common-configuration Endpoint Elides User Lists
Explanation	The lxi/common-configuration endpoint does not require client authentication, therefore, this response shall elide the user lists used for client authentication and authorization.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.1.2-4

23.10.9 LXI Common Configuration PUT API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Common Configuration PUT API
Explanation	The LXI Common Configuration PUT API configures the common device LXI configuration. The configuration represented by the XML payload may meaningfully be applied to all devices in a system.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

PUT Common Configuration without authorization

PUT the Common Configuration with the URL /lxi/api/common-configuration without any authorization. Expect it to fail because of missing authorization. The failure should be '401 Unauthorized client'.

PUT Common Configuration missing '/api/' in URL

PUT Common Configuration using the URL /lxi/common-configuration. Expect failure as the endpoint does not exist.

23.10.9.1 Ignore Read-Only Attributes On Write

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Ignore Read-Only Attributes On Write

Explanation: There are several attributes in the LXI Common Configuration Schema that are read-only, that is, they are returned by the device as part of a GET, but they are not intended for use during a PUT. If a device receives Read-only attributes on a PUT it shall ignore them, and not treat them as an error.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.12.1.1-2	23.12.2.1-3	23.12.2.1-6

23.10.10 LXI Device Specific Configuration GET API

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Device Specific Configuration GET API

Explanation: The LXI Device Specific Configuration GET API returns device-specific configuration and capabilities as specified in the LXI Device Specific Configuration schema. The settings returned by this API are either potentially unique to a particular device or automatically configured. The two endpoints return the same response.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Check response header content-type for xml

Check the previous API calls response header content-type for xml.

Validate Xml against local schema

Validate the response Xml against the appropriate local schema.

Validate Xml against the schema on the device

Validate the response Xml against the appropriate schema on the device.

GET Device Specific Configuration without authentication

GET the Device Specific Configuration from the device without authentication. Expect the call to fail as no authentication was given. '401 Unauthorized' error expected.

23.10.11 LXI Device Specific Configuration PUT API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Device Specific Configuration PUT API
Explanation	The LXI Device Specific Configuration PUT API configures network settings that are device-specific or potentially automatically configured. Devices retain the LXI Device Specific configuration and only utilize it when automatic configuration is disabled. Thus, writing the LXI Device Specific configuration while automatic configuration is active then subsequently disabling automatic configuration will result in the device using the configuration specified in the LXI Device Specific configuration.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Device Specific Configuration GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.
Test Procedure	PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response. PUT Device Specific Configuration without authorization tag PUT the valid Device Specific Configuration to the device via device-specific-configuration API without an authorization tag. Expect an Error because of the missing authorization. PUT Device Specific Configuration missing '/api/' in URL PUT the Device Specific Configuration to the device via the API leaving away the '/api/' in the URL. Expect it to fail due to invalid endpoint.

23.10.12 LXI Certificates GET API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Certificates GET API

Explanation	The LXI Certificates GET API returns a listing of certificates, certificate chains, and outstanding CSRs on the device. This listing includes information specified in the LXICertificateList schema including GUIDs that identify each entity. These GUIDs may be used, for instance, to designate the LXI Certificate to the DEL method. CSRs may be deleted by the user or, from time-to-time, expire on the device. See section 23.10.16.1, RULE – Minimum CSR Retention, for LXI requirements.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Check response header content-type for xml Check the previous API calls response header content-type for xml. Validate Xml against local schema Validate the response Xml against the appropriate local schema. Get certificates via API /lxi/certificates Try to GET the certificates list via API /lxi/certificates, expect error due to invalid endpoint.

23.10.13 LXI Certificates POST API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Certificates POST API
Explanation	The LXI Certificates POST API provisions a certificate or certificate chain to the device to be used by the device to identify itself
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
Test Procedure	Get CSR Get CSR certificate via the /lxi/api/get-csr API. Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Create certificate from CSR Create a self-signed certificate out of the Certificate Signing Request.

POST certificate

POST the certificate to the device via /lxi/api/certificates using the API-Key.

Check response header content-type for xml

Check the previous API calls response header content-type for xml.

Validate Xml against local schema

Validate the response Xml against the appropriate local schema.

GET Certificate for GUID

GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID.

Match returned certificate to created certificate

Compare the values from the certificate with the values in the created one for a match.

Get certificates, check for CSR GUID

Get the certificates list from device and check for CSR GUID within the list.

POST certificate, expect failure missing CSR

Repost the certificate to the device and expect a failure as the CSR has been deleted inbetween.

Get CSR

Get CSR certificate via the /lxi/api/get-csr API.

Create certificate from CSR

Create a self-signed certificate out of the Certificate Signing Request.

POST certificate, expect failure

POST certificate via /lxi/certificate and expect an error due to endpoint not available.

Get certificates, expect new GUID in list

Get the certificates list from the device and expect the new GUID to be returned in the list additionally to the original list retrieved previously.

POST certificate created without CSR from the device

POST a self-signed certificate to the device which was not created from a CSR retrieved from the device. Expect this POST to fail, as a posted certificate shall match a CSR on the device.

23.10.14 LXI Certificate GET API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Certificate GET API
Explanation	The LXI Certificates/<GUID> GET API returns the certificate, certificate chain, or CSR identified by the <GUID> incorporated into the URL. Note that the type of the response is dependent on the GUID.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Ensure at least two LDevID's are available

Ensure at least two LDevIDs are available in the certificate list. If not create self-signed certificates on the device via the create-certificate API.

Ensure at least two CSR's are available

Ensure at least two CSR's are available in the certificate list. If not create them on the device via the get-csr API.

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Test Procedure

For each GUID in the GUID list:

GET Certificate for GUID

GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID.

Check response header content-type

Check the response header content-type. If the response is a certificate, then the content-type shall be cms. If it is a csr, the content-type hsall be pkcs10.

Check response header transfer-encoding for base64

If the response is a pkcs10, check the header transfer-encoding for base64.

GET Certificate for GUID

GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID.

23.10.15 LXI Certificate DELETE API

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Certificate DELETE API

Explanation: The LXI Certificates/<GUID> DELETE API deletes the certificate, certificate chain, or CSR identified by the <GUID> incorporated into the URL.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Ensure at least two LDevID's are available

Ensure at least two LDevIDs are available in the certificate list. If not create self-signed certificates on the device via the create-certificate API.

Ensure at least two CSR's are available

Ensure at least two CSR's are available in the certificate list. If not create them on the device via the get-csr API.

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Test Procedure

DELETE certificate via the GUID

DELETE certificate via /lxi/api/certificates/<GUID> using API-Key.

Expect Error

Expect Error. This can have several reasons. For an API this may be an invalid endpoint, wrong data (such as invalid GUID). Check previous test step for indication of expected error.

Check no GUID was removed

Get certificates from device and ensure no GUID was removed.

For each certificate which is not an IDevID:

For each certificate which is not an IDevID, do the next steps.

Delete certificate, expect failure

Delete the certificate using the API /lxi/certificate/<GUID> and expect an error due to endpoint not available.

DELETE certificate via the GUID

DELETE certificate via /lxi/api/certificates/<GUID> using API-Key.

Get certificates and check guid was deleted

Get certificates from device and ensure the GUID is no more listed.

GET certificate for GUID, expect failure

GET certificate for a specific GUID and expect an error as the GUID is not available.

For each CSR:

Do the next steps for each CSR

DELETE CSR via the GUID

DELETE CSR via /lxi/api/certificates/<GUID> using API-Key.

Get CSR, expect failure

Get CSR via /lxi/api/certificates/<GUID> using API-Key and expect an error. No CSR with the given GUID available.

23.10.16 LXI CSR GET API

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI CSR GET API

Explanation: The LXI CSR GET API acquires a PKCS#10 CSR from the device. The CSR is created based on the data in the LXICertificateRequest XML which includes the subject and other fields the client specifies for the CSR.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

	Get IP from mdns	
		Search via mdns for a single lxi service and retrieve its IP address
	Create certificate request	
		Create a certificate request XML with values to use for an API call.
Test Procedure	Get CSR	
		Get CSR certificate via the /lxi/api/get-csr API.
	Check response header content-type for pkcs10	
		Check response header content-type for pkcs10. Pkcs10 is the format of a CSR.
	Check response header transfer encoding for Base64	
		Check the response header transfer encoding is Base64.
	Verify PEM file response	
		Check the format of the certificate signing request.
	Ensure request parameters are within the PEM file	
		Check the parameters from the Certificate Request xml are within the retrieved certificate signing request.
	Get CSR missing '/api/' in URL	
		Get CSR certificate via the /lxi/get-csr API and expect an error due to invalid endpoint.

23.10.16.1 Minimum CSR Retention

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Minimum CSR Retention
Explanation	Devices shall at least retain the most recently generated CSR for any given cryptography suite at least until a power cycle. Devices should retain CSRs longer than this to support other customer use models, especially those that require operator intervention.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	Get certificates
	Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
	Get CSR
	Get CSR certificate via the /lxi/api/get-csr API.
	Get certificates
	Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
Test Procedure	Validate CSR lifetime
	Identify the CSR GUID in the GUID list every 10 seconds. Ensure it stays available for a while.

23.10.17 LXI Create Certificate API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Create Certificate API
Explanation	In response to this call, the device shall create a new certificate (that is, an LDevID) to use to authenticate itself. This self-signed certificate shall be managed and presented to clients consistent with the requirements in the LXI Security Extended Function. If the device is unable to respect any of the fields specified in the LXICertificateRequest, the device shall return an error.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Create simple certificate request and values Create simple certificate request and values to send to the DUT.
Test Procedure	Create certificate Create a certificate via PUT /lxi/api/create-certificate using API-Key. Check response header content-type for xml Check the previous API calls response header content-type for xml. Validate Xml against local schema Validate the response Xml against the appropriate local schema. GET Certificate for GUID GET certificate via the API /lxi/certificates/<GUID> using the appropriate GUID. Check fields in certificate Validate all fields from the certificate request are used for the certificate. Create certificate with an invalid xml Try to create a certificate with a faulty certificate request xml. Expect an error due to invalid certificate request xml. Create certificate via PUT /lxi/create-certificate Try to create a certificate via the endpoint /lxi/create-certificate. Expect an Error as endpoint shall not be available.

23.10.18 LXI Certificate ENABLED API

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXI Certificate ENABLED API
Explanation	The LXI Certificates/<GUID>/enabled PUT API enables or disables the designated certificate or certificate chain identified by the <GUID> incorporated into the URL.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	Get certificates
	Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
	Ensure at least two certificates are available
	Ensure at least two certificates are available, if not create them.
Test Procedure	Identify active certificate
	Identify currently used certificate. This can be done via HTTPS or HiSLIP.
	Disable active certificate
	Disable currently used certificate via /lxi/api/certificates/<GUID>/enabled using API-Key
	Verify device has stopped using the certificate
	Verify the device has stopped using the certificate.
	Get certificate enabled value
	Read back value via /lxi/api/certificates/<GUID>/enabled using API-Key and check for enabled value.
	Enable certificate
	Enable the certificate via the API /lxi/api/certificates/<GUID>/enabled and the apropriate GUID and the boolean value true.
	Verify the device is using the certificate
	Verify the device is using the certificate again. This can be verified via HiSLIP or HTTPS webpages.
	Get certificate enabled value
	Read back value via /lxi/api/certificates/<GUID>/enabled using API-Key and check for enabled value.
	Disable certificate missing '/api/' in URL
	Disable the certificate via the URL /lxi/certificates/<GUID>/enabled using the apropriate GUID.

23.10.18.1 LXILiterals Parameter to Enabled is Boolean

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXILiterals Parameter to Enabled is Boolean
Explanation	The LXILiterals schema permits arbitrarily typed attributes. The request LXILiterals parameter to enabled shall be an attribute of name value and of type xs:boolean. The value of the Boolean attribute indicates if the certificate or certificate chain identified by the <GUID> is enabled.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.10.18

23.10.18.2 LXILiterals Response to Enabled is Boolean

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXILiterals Response to Enabled is Boolean

Explanation	The LXILiterals schema permits arbitrarily typed attributes. The response LXILiterals parameter to enabled shall be an attribute of name value and of type xs:boolean. The value of the Boolean attribute indicates if the certificate or certificate chain identified by the <GUID> is enabled.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.10.18

23.11.2-1 Connected Device URLs

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	Connected Device URLs
Explanation	Devices that support connected devices (e.g., bridges) shall provide base URLs for all connected devices in the ConnectedDevices element of the identification document. A base URL is defined as a URL with a “url-path” that clearly identifies the connected device and one onto which a suffix path may be added to access properties of that connected device. The base URL allows clients to enumerate devices connected to the bridge device. For example, the base URL for a connected device might be “http://hostname/device0” while another connected device might have a base URL of “http://hostname/device5”. The format and path naming conventions for these connected device base URLs are left up to the vendor. The following is an example snippet from an identification document with connected device DeviceURI elements: http://10.1.2.60/devices/LogicalAddress/0/ http://10.1.2.60/devices/LogicalAddress/1/
Pre Condition	Connect DUT Connect the DUT to the test network Get identification file Get the identification file from the device under test
Test Procedure	Get Connected Devices Get the connected devices from the identification file of the device under test Get identification files for Connected Devices Get the connected devices identification files of the device under test

23.11.2.1-1 Connected Device XML Identification Document URLs

Category	Identification, Device Specification
Test Type	Kerberos Test, automated
Rule	Connected Device XML Identification Document URLs
Explanation	Devices that support connected devices shall provide identification documents that can be queried via a GET on /lxi/identification that conform to the LXI XSD Schema or one derived from that Schema according to the rules of XSD inheritance. The values may be found in DeviceURI elements of the ConnectedDevice element of the root element of the identification document of Rule 10.2. This rule coupled with Rule 10.2.4 allows clients to enumerate (discover) and identify all connected devices.
Pre Condition	Connect DUT Connect the DUT to the test network Get identification file Get the identification file from the device under test

Get Connected Devices

Get the connected devices from the identification file of the device under test

Test Procedure: Validate identification files for Connected Devices

Get the connected devices identification files of the device under test

23.11.2.1-2 Connected Device XML Identification Document Schema Location Attribute

Category: Identification, Device Specification

Test Type: Kerberos Test, automated

Rule: Connected Device XML Identification Document Schema Location Attribute

Explanation: The xsi:schemaLocation attribute of the root element of the identification document shall contain an entry for the LXI XSD namespace with an accompanying absolute URI on the instrument that shall return the actual XSD schema document from the instrument (https://www.w3.org/standards/xml/schema)). The W3C XSD Schema itself does not need to be available via a URI on the instrument.

Pre Condition: Connect DUT

Connect the DUT to the test network

Get identification file

Get the identification file from the device under test

Get Connected Devices

Get the connected devices from the identification file of the device under test

Test Procedure: Validate schema location for Connected Devices

Validate the schema locations of the connected devices given by their identification files

23.12-1 LXICommonConfigurationSchema HTTP PUT

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXICommonConfigurationSchema HTTP PUT

Explanation: On an HTTP PUT the device shall go to the state specified in the XML.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies:

23.12.6-1	23.12.6-2	23.12.6.1-1
23.12.6.1-2	23.12.6.1-3	23.12.6.2-1

23.12.1.1-1 Attribute LXICommonConfiguration Strict Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute LXICommonConfiguration Strict Required

Explanation: Attribute strict shall be implemented. Attribute strict indicates that designated portions of this XML document may not be ignored by the device. This requirement does not bear on attributes and elements that are explicitly documented to be ignored, for instance, extension attributes.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Ensure Common Configuration does not return strict attribute

Ensure Common Configuration does not return strict attribute.It is a write only attribute.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Verify all interface elements and create missing elements

Verify all of the interface elements and create each missing element as per LXI Common Configuration.

PUT Common Configuration, expect failure, depending on strict handling

Expect failure notice due to strict handling. If device implements all elements, then strict mode does not change the behaviour of the device and gets success response

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.1.1-2 Attribute LXICommonConfiguration HSMPresent

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute LXICommonConfiguration HSMPresent

Explanation: HSMPresent is a read-only attribute that is true if and only if the device uses a HSM to protect the private keys used for LXI communication.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure	Ensure availability of HSMPresent attribute Read the HSMPresent value from the LXI CommonConfiguration. Compare the HSMPresent value against test configuration Compare the HSMPresent value against the test configuration value. Modify the HSMPresent value Modify the HSMPresent value via the Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Read the HSMPresent Value and ensure modified value was ignored Read the HSMPresent Value from the LXI Common Configuration XML and ensure the modified value was ignored.

23.12.1.1-3 Attribute LXICommonConfiguration HSMPresent Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute LXICommonConfiguration HSMPresent Required
Explanation	Attribute HSMPresent shall be implemented. HSMPresent indicates if the device has a hardware security module.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Ensure availability of HSMPresent attribute Read the HSMPresent value from the LXI CommonConfiguration.

23.12.1.2-1 LXICommonConfiguration Interface Configuration

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXICommonConfiguration Interface Configuration
Explanation	Devices shall accept configuration based on an Interface element for any LXI conformant interface.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4

	Connect DUT	
		Connect the DUT to the test network
	Get IP from mdns	
		Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration	
		GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Modify interface element	
		Modify the interface element value.
	PUT Common Configuration	
		PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.1.2-2 Return of Interfaces by Devices

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Return of Interfaces by Devices
Explanation	Devices shall return an Interface element for each interface.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Compare number of interface elements against test configuration
	The total number of interfaces in the LXI Common Configuration should match the number specified in the test configuration.
	Compare amount of LXI compliant interfaces against test configuration
	The total number of LXI compliant interfaces in the LXI Common Configuration should match the number specified in the test configuration.

23.12.1.2-3 ClientAuthentication PUT

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthentication PUT
Explanation	ClientAuthentication shall be optionally accepted for PUT.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check availability of ClientAuthentication element

Check the availability of ClientAuthentication element in the Common Configuration XML retrieved from the DUT.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Verify Common Configuration is unchanged

Ensure that the LXI Common Configuratiuon has no change and ClientAuthentication element is in the Common Configuration.

Remove ClientAuthentication element

Remove the ClientAuthentication element from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Verify Common Configuration is unchanged

Ensure that the LXI Common Configuratiuon has no change and ClientAuthentication element is in the Common Configuration.

23.12.1.2-4 ClientAuthentication Attributes

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: ClientAuthentication Attributes

Explanation: ClientAuthentication without the @passwords or @APIAccess attributes shall be returned for GET over secure connections and elided for unsecure connections.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Availability of HTTP

Ensure that the HTTP element is available in the Common Configuration.

Enable HTTP operation attribute

Enable the HTTP operation attribute via Common Configuration

Enable HTTP API-LXISecurity service

Enable the HTTP API-LXISecurity service via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Validate availability of ClientAuthentication

Verify that the ClientAuthentication element is in the Common Configuration but without passwords and APIAccess attributes.

GET Common Configuration missing '/api/' in URL

GET Common Configuration over secure connection (HTTPS) via /lxi/api/common-configuration and expect success response.

Validate the absence of ClientAuthentication

Verify that the ClientAuthentication element is absence in the Common Configuration.

GET Common Configuration via HTTP

GET Common Configuration over unsecure connection (HTTP) and expect failure response.

GET Common Configuration missing '/api/' in URL via HTTP

GET Common Configuration over unsecure connection (HTTP) and expect success response.

Validate the absence of ClientAuthentication

Verify that the ClientAuthentication element is absence in the Common Configuration.

23.12-2 LXICommonConfigurationSchema GET Response

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXICommonConfigurationSchema GET Response

Explanation: The device GET response shall indicate the current state and capabilities of the device.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.12-1	23.10.6.3

23.12.2-1 **Interface Disable**

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Disable
Explanation	Non-LXI interfaces can be disabled using the Interface/@enabled attribute
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Get Interface elements which are not LXI compliant Get the Non-LXI compliant interface elements from the Common Configuration. Check for enabled attribute for all Non-LXI compliant interfaces Validate the Non-LXI compliant interfaces should have enabled attribute.

23.12.2.1-1 **Interface Default Name**

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Default Name
Explanation	Devices with a single interface shall treat the Interface element with the name LXI (the default name) to configure the single interface. Devices with multiple interfaces shall assign one of them the name LXI (the default name).
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Modify Network parameters Modify the Network parameters of the Common Configuration. Rename interface to 'LXI' If there is a single interface, rename the interface to 'LXI'.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Verify settings

Verify that the network parameters and interface name are same as set before.

Ensure single interface named 'LXI'

If multiple interfaces are available, remove all of the interface elements except the interface named 'LXI'.

Modify Network parameters

Modify the Network parameters of the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Verify 'LXI' interface has assigned values

Verify that the single enabled interface is named LXI and the assigned values are same as set before in the interface.

Remove interface name attribute named LXI

Remove the name attribute in the interface, which is named LXI from the Common Confgiuration.

Modify Network parameters

Modify the Network parameters of the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Ensure default interface name is named LXI

Ensure the device shall have the default interface name set to LXI.

23.12.2.1-2 Attribute Interface Name Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Interface Name Required

Explanation	Attribute name shall be implemented. name identifies this physical network interface within the device. It differentiates the interfaces in devices that have multiple interfaces.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check for 'name' attribute for each interface For each interface check for the 'name' attribute in the Common Configuratrion. Check for single interface named LXI Go through each interface in the Common Configuration and ensure only one is named LXI. Modify the Interface name Modify the Interface name attribute and set a value other than LXI. This shall cause a Common Configuration PUT action to fail. PUT Common Configuration, expect failure PUT the Common Configuration to the device and expect failure response. Check previous step for better understanding. This may be due to incorrect data, no authentication or any other reason for the API call to fail.

23.12.2.1-3 Attribute Interface LXIConformant Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Interface LXIConformant Required
Explanation	Attribute LXIConformant shall be implemented. LXIConformant is a read-only attribute that indicates the LXI specifications this device complies with. If this interface does not comply with the LXI Device specification, an empty string is used.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Get identification file Get the identification file from the device under test

Test Procedure	Check all interface elements for LXIConformant attribute
	Check all of the interface elements for LXIConformant attribute
	Match test interface values against Identification file values
	Match the test interface LXIConformant values against Identification file values
	Modify LXIConformant attribute's value
	Modify the LXIConformant attribute's value in the Common Configuration
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
	Verify that the LXI-Conformant read only attribute ignored the modified value
	Verify that the LXI-Conformant read only attribute ignored the modified value
	Match test interface values against Identification file values
	Match the test interface LXIConformant values against Identification file values

23.12.2.1-4 LXI conformant Interfaces Enabled

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	LXI conformant Interfaces Enabled
Explanation	LXI conformant interfaces shall be enabled, others may be enabled.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Disable all LXI Conformant interfaces
	Disable all of the LXI Conformant interfaces in the Common Configuration.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get Common Configuration, expect failure

GET Common Configuration via API and expect failure response due to disabled interface.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Ensure interfaces are enabled

Go through each interface in the Common Configuration and ensure the LXIConformant interfaces are enabled.

23.12.2.1-5 Attribute Interface Enabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Interface Enabled Required
Explanation	Attribute enabled shall be implemented. enabled indicates if this physical network interface is enabled.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of Enabled attribute on all interfaces

Check the availability of Enabled attribute on all interfaces in the Common Configuration

23.12.2.1-6 Attribute Interface unsecureMode Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Interface unsecureMode Required
Explanation	Attribute unsecureMode shall be implemented. unsecureMode is a read-only attribute that indicates that one or more configurations in this XML do not meet the LXI minimum requirements for secure device operation.
Test Procedure	Computed by other tests

This test is computed by the result of other tests.

Dependencies	23.12.2-3

23.12.2.1-7 Interface LXI Secure Devices Protocol

Category	LXI Security
Test Type	Vendor Declaration

Rule	Interface LXI Secure Devices Protocol
Explanation	LXI Secure devices shall document the protocols that are controlled by this attribute.

23.12.2.1-8 Interface unsecure Protocols

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface unsecure Protocols
Explanation	If the device does not implement any other unsecure protocols, then on a GET, otherUnsecureProtocolsEnabled shall return false. However, if written true, such a device shall either fail the PUT or indicate unsecure mode is True.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check otherUnsecureProtocolsEnabled value for each interface Check the otherUnsecureProtocolsEnabled value for each interface. If the value is true, the test passes, otherwise it continues to the further steps. Enable otherUnsecureProtocolsEnabled attribute Modify the value of otherUnsecureProtocolsEnabled to true for each interface. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check otherUnsecureProtocolsEnabled for true Read otherUnsecureProtocolsEnabled of the interface and expect value to be true. Check unsecure mode for unsecure Check the unsecure mode state is usnecure, therefore expect the value to be true.

23.12.2.1-9 Attribute Interface otherUnsecureProtocolsEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Interface otherUnsecureProtocolsEnabled Required

Explanation	Attribute otherUnsecureProtocolsEnabled shall be implemented. otherUnsecureProtocolsEnabled represents the state of various device-specific protocols that are beyond the scope of LXI
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.2-3

23.12.2.1-10 Interface Ethernet communication

Category	LXI Security
Test Type	Vendor Declaration
Rule	Interface Ethernet communication
Explanation	Those settings are necessary to re-establish Ethernet communication with the instrument shall be enabled.

23.12.2.1-11 Interface Indicate unsecure Mode

Category	LXI Security
Test Type	Vendor Declaration
Rule	Interface Indicate unsecure Mode
Explanation	The impact of these configurations on the device secure mode are determined by the device vendor. However, if unsecure protocols are enabled, the device shall indicate it is in unsecure mode.

23.12.2-2 Non Lxi Conformant Interfaces

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Non Lxi Conformant Interfaces
Explanation	Device network interfaces (including those added dynamically) over which the LXI device may be controlled that are not LXI Conformant shall at least support this element with the enabled attribute so that network interfaces that are not LXI Security capable can be disabled.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.2-1

23.12.2.2-1 Interface Network Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Network Required
Explanation	Network is required. Interfaces that are not LXI Conformant are required to implement this element, however, they are only required to implement the Network/@Enabled attribute.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of Network element on all interfaces

Check availability of Network element on all interfaces in the Common Configuration

23.12.2.2-2 Interface HTTP Element

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Interface HTTP Element

Explanation: HTTP is optional, however devices that implement HTTP are require to fully implement this element.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of HTTP element on all LXI Conformant interfaces

Check the availability of HTTP element on all LXI Conformant interfaces in the Common Configuration.

Add HTTP element

If HTTP element is not present, create a HTTP element as disabled in the Common Configuration

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-3 Interface Multiple HTTP Elements

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Interface Multiple HTTP Elements

Explanation: If multiple HTTP elements are present, each shall have a different port. Additional instances of this element may be used to provide independent control of multiple servers (although each must be on a different port). This may be useful, for instance, if separate servers are setup for the API and the human interface

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check for multiple HTTP elements

Check for multiple HTTP elements. If single HTTP element is found in the interface, test is pass.

Ensure the HTTP ports are all different

Ensure all of the HTTP ports of various HTTP elements are different.

23.12.2.2-4 Interface HTTPS Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Interface HTTPS Required

Explanation: HTTPS is required.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check availability of HTTPS element on all LXI Conformant interfaces

Check the availability of HTTPS element on all interfaces in the Common Configuration.

Add HTTPS element

If HTTPS element is not present, create a HTTPS element as disabled in the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-5 Multiple HTTPS Elements

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Multiple HTTPS Elements

Explanation: If multiple HTTPS elements are present, each shall have a different port. Additional instances of this element may be used to provide independent control of multiple servers (although each must be on a different port). This may be useful, for instance, if separate servers are setup for the API and the human interface.

Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check for multiple HTTPS elements
	Check for multiple HTTPS elements. If single HTTPS element is found in the interface, test is pass.
	Ensure the HTTPS ports are all different
	Ensure all of the HTTPS ports of various HTTPS elements are different.

23.12.2.2-6 Interface SCPIRaw Element

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface SCPIRaw Element
Explanation	At least one instance of SCPIRaw shall be accepted by devices that implement a SCPIRaw Command and Control connection. A separate instance of SCPIRaw is used for each port at which a SCPIRaw server is running.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check availability of SCPIRaw
	Check the availability of SCPIRaw element on tested interface as per test configuration. If present, disable it otherwise create the SCPIRaw element as disabled.
	Disable Strict Mode
	Deactivate the Strict Mode in the LXI Common Configuration XML.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	Enable Strict Mode
	Activate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-7 Interface Telnet Element

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Telnet Element
Explanation	At least one instance of Telnet shall be accepted by devices that implement the Telnet Command and Control connection. A separate instance of Telnet is used for each port at which a Telnet server is running.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of Telnet

Check the availability of Telnet element on tested interface as per test configuration. If present, disable it otherwise create the Telnet element as disabled.

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

Enable Telnet

Enable Telnet via Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and Telnet not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

Enable Telnet

Enable Telnet via Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and Telnet not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-8 Interface SCPITLS Element

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface SCPITLS Element
Explanation	At least one instance of SCPITLS shall be accepted by devices that implement a SCPITLS Command and Control connection. A separate instance of SCPITLS is provided for each port at which a SCPITLS server is running.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check availability of SCPITLS

Check the availability of SCPITLS element on tested interface as per test configuration. If present, disable it otherwise create the SCPITLS element as disabled.

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable Strict Mode

Activate the Strict Mode in the LXI Common Configuration XML.

Enable SCPITLS

Enable SCPITLS on the device by setting the Enabled attribute of the SCPITLS element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPITLS not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Disable Strict Mode

Deactivate the Strict Mode in the LXI Common Configuration XML.

Enable SCPITLS

Enable SCPITLS on the device by setting the Enabled attribute of the SCPITLS element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPITLS not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-9 Interface HiSLIP Element

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Interface HiSLIP Element

Explanation	HiSLIP shall be accepted by devices that implement the LXI HiSLIP extended function. Only a single instance of HiSLIP is permitted because a single instance of the protocol supports an arbitrary number of instances of servers at an arbitrary number of sub addresses.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check availability of HiSLIP Check the availability of HiSLIP element on tested interface as per test configuration. If present, disable it otherwise create the HiSLIP element as disabled. Disable Strict Mode Deactivate the Strict Mode in the LXI Common Configuration XML. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Enable Strict Mode Activate the Strict Mode in the LXI Common Configuration XML. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Enable Strict Mode Activate the Strict Mode in the LXI Common Configuration XML. Enable HiSLIP Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Disable Strict Mode Deactivate the Strict Mode in the LXI Common Configuration XML. Enable HiSLIP Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-10 Interface VXI11 Element

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface VXI11 Element
Explanation	VXI11 shall be accepted by devices that implement a VXI-11 Command and Control connection. Only a single instance of the VXI-11 protocol can be created on an interface.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check availability of VXI-11 Check the availability of VXI11 element on tested interface as per test configuration. If present, disable it otherwise create the VXI-11 element as disabled. Disable Strict Mode Deactivate the Strict Mode in the LXI Common Configuration XML. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Enable Strict Mode Activate the Strict Mode in the LXI Common Configuration XML. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Enable Strict Mode Activate the Strict Mode in the LXI Common Configuration XML. Enable VXI-11 Set VXI11 'enabled' attribute to true via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Disable Strict Mode Deactivate the Strict Mode in the LXI Common Configuration XML.

Enable VXI-11

Set VXI11 'enabled' attribute to true via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-11 Interface Unrecognized Extensions

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Unrecognized Extensions
Explanation	If a device receives a well-formed extension element it does not recognize, it shall ignore it.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Add unknown extension element

Create an unknown and well formed element in the interface, which is unknown by device.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-12 Interface Get Configuration

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Get Configuration
Explanation	On a GET, devices are permitted to express arbitrary configuration with extension elements, however such a device shall accept configuration using those elements.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure	Check for Any Element Check for Any Element for all interfaces. If none found, test passes, otherwise it continues to the further steps. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.2.2-13 Interface unsecure Mode Attribute unsecureEnabled

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	Interface unsecure Mode Attribute unsecureEnabled
Explanation	Any element that controls a protocol that impacts the unsecure mode shall include an unsecureEnabled attribute. Setting this false shall disable the protocol or disable the unsecure behaviour. The device shall report unsecureMode true, when any protocol has unsecureEnabled true.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Set the DUT to Non-Unsecure Mode Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.
Test Procedure	Check all any elements for unsecureEnabled flag Check all any elements of the interface element for unsecureEnabled flag. Enable unsecureEnabled attribute Set the unsecureEnabled attribute of the interface element value to true, if available. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Query unsecure mode indicator Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator. Disable unsecureEnabled attribute Set the unsecureEnabled attribute of the interface element value to false, if available.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

23.12.2-3 unsecure Interface

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	unsecure Interface
Explanation	If any unsecure interface is enabled, then the device shall report that it is unsecure mode.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

Check otherUnsecureProtocolsEnabled for false

Check the otherUnsecureProtocolsEnabled flag in the Common Configuration is set to false.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure indicator for false

Check the unsecure indicator state through the Common Configuration and expect it to be false.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

Check protocols and enable unsecure ones

For each interface,check protocols and enable unsecure protocols.

Check otherUnsecureProtocolsEnabled for true

Read otherUnsecureProtocolsEnabled of the interface and expect value to be true.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the unsecure indicator state, expect true

Check the unsecure indicator state and expect the value to be true. This means the device is in an unsecure state.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

Disable interface

Disable each interface in the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Query unsecure mode indicator

Open the LXI welcome page and visually check the welcome page that the DUT has an unsecure mode indicator.

23.12.2-4 Interface Optional Elements

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Optional Elements

Explanation	Absence of optional elements disables them
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Get interface elements from the Common Configuration Get all of the interface elements from the Common Configuration. This includes non LXI interfaces. Enable each available ELEMENT Enable each available element, which has enabled attribute. Depending on the iteration this may be either SCPIRaw, SCPITLS, Telnet, HiSLIP, VXI-11 or even an AnyElement. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Remove each element from the Common Configuration Remove each available element from the Common Configuration. Depending on the iteration this may be either SCPIRaw, SCPITLS, Telnet, HiSLIP, VXI-11 or even an AnyElement. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check each element is disabled Check that each elements enabled attribute is false. This may be either SCPIRaw, SCPITLS, Telnet, HiSLIP, VXI-11 or even an AnyElement.

23.12.2-5 Interface Optional Elements Response

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Interface Optional Elements Response
Explanation	If a device does not implement a capability configured by an XML element within Interface, it shall omit that optional XML element from its response. If the device does implement the capability, it shall include the element in the response and indicate the current configuration. See the details regarding the implementation of LXICommonConfiguration/@strict attribute regarding how certain protocol configurations are handled.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get interface elements from the Common Configuration

Get all of the interface elements from the Common Configuration. This includes non LXI interfaces.

Test Procedure

Ensure correct number of elements

Ensure the correct number of elements are present in the Common Configuration as per test configuration. Depending on the iteration this may be either SCPIRaw, SCPITLS, Telnet, HiSLIP, VXI-11 or even an AnyElement.

Compare capability attribute value against test configuration

Compare the capability attribute value with test configuration value. These must match.

23.12-3 LXICommonConfigurationSchema Capability Attributes

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXICommonConfigurationSchema Capability Attributes

Explanation: Devices shall indicate capabilities not apparent from the queried settings using the capability attribute.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.12.9-1	23.12.9.1-1	23.12.9.1-2
23.12.9.1-3	23.12.10-1	23.12.10-2
23.12.10-3	23.12.10.1-1	23.12.10.1-2
23.12.10.1-3	23.12.11.1-3	23.12.11.1-6
23.12.11.1-7		

23.12.3.1-1 Network Element Ipv4 Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Network Element Ipv4 Required

Explanation: IPv4 is required.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check for IPv4 Element in each LXI conformant interface element

Check the availability of IPv4 Element in each LXI conformant interface element.

23.12.3.1-2 Network Element Ipv6 Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Network Element Ipv6 Required

Explanation: IPv6 is required by devices that implement the IPv6 Extended Function.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check IPv6 Element for each LXI Conformant interface

Check the IPv6 Element for each LXI Conformant interface is available.

Check for 'LXI IPv6' in the LXIConformant attribute

Check that 'LXI IPv6' extended function is available in the LXIConformant attribute.

23.12.4.1-1 Attribute IPv4 Enabled Required

Category: LXI Security

Test Type: Kerberos Test, manual

Rule: Attribute IPv4 Enabled Required

Explanation: Attribute enabled shall be implemented. Enabled generally enables or disables IPv4 operation.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv4 and IPv6 'PingEnabled' attribute

Set IPv4 and IPv6 'PingEnabled' attribute to true via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Check availability of enabled attribute in all IPv4 elements

Check the availability of enabled attribute in all IPv4 elements in the Common Configuration.

Disable IPv4 'enabled' attribute

Set IPv4 'enabled' attribute to false.

Enable IPv4 and IPv6 'PingEnabled' attribute

Set IPv4 and IPv6 'PingEnabled' attribute to true via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Ping the DUT for failure

Ping the DUT via IPv4 which is expected to fail.

Get Common Configuration via IPv4, expect failure

GET Common Configuration via IPv4 and expect the call to fail.

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Enable IPv4 via Common Configuration

Set the IPv4 enabled attribute to true via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

Ping the DUT for success

Ping the DUT via IPv4 which is expected to succeed

23.12.4.1-2 IPv4 State Without AutoIPEnabled

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 State Without AutoIPEnabled
Explanation	If omitted, and DHCPEnabled is present, the device uses the same state as DHCPEnabled.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. GET Device Specific Configuration GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key. Set static IP Set the static IP in the Device Specific Configuration xml. PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.
Test Procedure	Remove AutoIPEnabled attribute Remove the AutoIPEnabled attribute from the IPv4 element. Enable IPv4 DHCPEnabled Set DHCPEnabled to true in the IPv4 element. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check AutoIPEnabled is true Check AutoIPEnabled attribute value is true. Remove AutoIPEnabled attribute Remove the AutoIPEnabled attribute from the IPv4 element. Disable IPv4 DHCPEnabled Set DHCPEnabled to false in the IPv4 element. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Validate IP address

Validate IP address and confirm that device is using the static IP address.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check DHCPEnabled is false

Check DHCPEnabled attribute value is false.

Check AutoIPEnabled is false

Check AutoIPEnabled attribute value is false.

23.12.4.1-3 Attribute IPv4 AutoIPEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4 AutoIPEnabled Required
Explanation	Attribute autoIPEnabled shall be implemented. AutoIPEnabled represents the state of the Link Local Addressing capability in the device. If enabled, the device may acquire an address using Link Local Address. Link Local addresses supersede static values configured in the LXI Device Specific Configuration.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Set static IP

Set the static IP in the Device Specific Configuration xml.

PUT Device Specific Configuration

PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

Test Procedure

Check the availability of AutoIPEnabled attribute

Check the availability of AutoIPEnabled attribute in the IPv4 elements of the Common Configuration.

Disable AutoIPEnabled and DHCPEnabled attributes

Disable the AutoIPEnabled and DHCPEnabled attributes of the IPv4 element of the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Check DUT has static IP address

Check the device has the previously configured static IP address.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable AutoIPEnabled attribute

Enable the AutoIPEnabled attribute of the IPv4 element of the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable AutoIPEnabled attribute

Enable the AutoIPEnabled attribute of the IPv4 element of the Common Configuration.

Enable DHCPEnabled attribute

Enable the DHCPEnabled attribute of the IPv4 element in the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Stop IPv4 DHCP router

Stop the IPv4 DHCP router, so that no IPv4 DHCP addresses given for lease

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable DHCPEnabled attribute

Enable the DHCPEnabled attribute of the IPv4 element in the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

23.12.4.1-4 IPv4 State Without DHCPEnabled

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 State Without DHCPEnabled
Explanation	If omitted, and autoIPEnabled is present, the device uses the same state as autoIPEnabled.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. GET Device Specific Configuration GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key. Set static IP Set the static IP in the Device Specific Configuration xml. PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.
Test Procedure	Remove DHCPEnabled attribute Remove the DHCPEnabled attribute from the IPv4 element. Enable AutoIPEnabled attribute Enable the AutoIPEnabled attribute of the IPv4 element of the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check DHCPEnabled is enabled

Check DHCPEnabled attribute value is set to true which means DHCP is enabled.

Remove DHCPEnabled attribute

Remove the DHCPEnabled attribute from the IPv4 element.

Disable AutoIPEnabled attribute

Set AutoIPEnabled attribute to false in the IPv4 element.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Validate IP address

Validate IP address and confirm that device is using the static IP address.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check DHCPEnabled is false

Check DHCPEnabled attribute value is false.

23.12.4.1-5 Attribute IPv4 DHCPEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4 DHCPEnabled Required
Explanation	Attribute DHCPEnabled shall be implemented. DHCPEnabled represents the state of the device DHCP protocol.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.4.1-3

23.12.4.1-6 Attribute IPv4 mDNSEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4 mDNSEnabled Required
Explanation	Attribute mDNSEnabled shall be implemented. mDNSEnabled represents the state of the multicast DNS responder in the device.

Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration.
Test Procedure	Check the availability of mDNSEnabled attribute Check the availability of mDNSEnabled attribute in IPv4 and/or IPv6 element of the Common Configuration. Loop next 5 Steps for mDNSEnabled value Loop over the next 5 Steps to set all combinations of the mDNSEnabled value for IPv4 and IPv6. IPv4: true; IPv6: true IPv4: false; IPv6: true IPv4: true; IPv6: false IPv4: false; IPv6: false Set IPv4 mDNSEnabled attribute Set the IPv4 mDNSEnabled attribute to true/false via the Common Configuration. Set IPv6 mDNSEnabled attribute If IPv6 is supported, set the IPv6 mDNSEnabled attribute to true/false via the Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Verify mDNS behaviour IPv4 Verify the mDNS behaviour for IPv4 as per mDNSEnabled attribute value. If mDNSEnabled attribute value is true then device can get the IP from the mdns otherwise not. Verify mDNS behaviour IPv6 Verify the mDNS behaviour for IPv6 as per mDNSEnabled attribute value. If mDNSEnabled attribute value is true then device can get the IP from the mdns otherwise not. If Ipv6 is not supported, this step is skipped.

23.12.4.1-7 IPv4 Dynamic DNS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 Dynamic DNS
Explanation	Dynamic DNS is optional for LXI devices. Therefore, if not implemented, the device shall ignore this attribute on a PUT.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the availability of dynamicDNSEnabled attribute Check the availability of dynamicDNSEnabled attribute. If attribute is available and configured, test passes. Otherwise,if attribute is not available and not configured, test continues to further steps. Enable IPv4 dynamicDNSEnabled attribute Enable IPv4 dynamicDNSEnabled attribute by setting or adding dynamicDNSEnabled attribute with value true in IPv4 element, if not available. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Disable IPv4 dynamicDNSEnabled attribute Disable IPv4 dynamicDNSEnabled attribute by setting or adding dynamicDNSEnabled attribute with value false in IPv4 element, if not available. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.4.1-8 IPv4 Devices Without dynamic DNS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 Devices Without dynamic DNS
Explanation	Devices that do not implement dynamic DNS shall omit this attribute on a GET.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.4.1-7

23.12.4.1-9 IPv4 dynamicDNSEnabled With IPv6 dynamic DNS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 dynamicDNSEnabled With IPv6 dynamic DNS
Explanation	The dynamicDNSEnabled attribute shall be implemented irrespective of if IPv6 dynamic DNS is implemented.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.4.1-7

23.12.4.1-10 Attribute IPv4 dynamicDNSEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4 dynamicDNSEnabled Required
Explanation	Attribute dynamicDNSEnabled shall be implemented. DynamicDNSEnabled represents the state of the dynamic DNS capability. Dynamic DNS is used to publish the hostname of the device to DNS.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the availability of dynamicDNSEnabled attribute Check the availability of dynamicDNSEnabled attribute. If attribute is available and configured, test passes. Otherwise,if attribute is not available and not configured, test continues to further steps. Enable dynamicDNSEnabled for IPv4 Set dynamicDNSEnabled attribute of the Common Configuration to true for IPv4 Enable dynamicDNSEnabled for IPv6 Set dynamicDNSEnabled attribute of the Common Configuration to true for IPv6, if this feature is supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Verify DynamicDNS behaviour for IPv4 through capture and analysis of Dynamic Update Packets Verify the behaviour of Dynamic DNS for IPv4 by capturing the network packets and analysing them for Dynamic Update Packets.

Disable dynamicDNSEnabled for IPv4

Set dynamicDNSEnabled attribute of the Common Configuration to false for IPv4

Disable dynamicDNSEnabled for IPv6

Set dynamicDNSEnabled attribute of the Common Configuration to false for IPv6, if this feature is supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Verify DynamicDNS behaviour for IPv4 through capture and analysis of Dynamic Update Packets

Verify the behaviour of Dynamic DNS for IPv4 by capturing the network packets and analysing them for Dynamic Update Packets.

Disable dynamicDNSEnabled for IPv4 and enable for IPv6

If IPv6 is supported, set the dynamicDNSEnabled attribute to false for IPv4 and true for IPv6.

PUT Common Configuration, expect failure

PUT the Common Configuration to the device and expect failure response. Check previous step for better understanding. This may be due to incorrect data, no authentication or any other reason for the API call to fail.

Verify DynamicDNS behaviour for IPv4 through capture and analysis of Dynamic Update Packets

Verify the behaviour of Dynamic DNS for IPv4 by capturing the network packets and analysing them for Dynamic Update Packets.

Enable dynamicDNSEnabled for IPv4 and disable for IPv6

If IPv6 is supported, set the dynamicDNSEnabled attribute of the Common Confgiuration to true for IPv4 and false for IPv6.

PUT Common Configuration, expect failure

PUT the Common Configuration to the device and expect failure response. Check previous step for better understanding. This may be due to incorrect data, no authentication or any other reason for the API call to fail.

Verify DynamicDNS behaviour for IPv4 through capture and analysis of Dynamic Update Packets

Verify the behaviour of Dynamic DNS for IPv4 by capturing the network packets and analysing them for Dynamic Update Packets.

23.12.4.1-11 Attribute IPv4 pingEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4 pingEnabled Required
Explanation	Attribute pingEnabled shall be implemented. Attribute pingEnabled represents the state of the IPv4 ICMP ping responder. shall be implemented.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

	Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration.
Test Procedure	Check the availability of pingEnabled attribute Check the availability of pingEnabled attribute in the Common Configuration. Loop next 5 Steps for pingEnabled value Loop over the next 5 Steps to set all combinations of the pingEnabled value for IPv4 and IPv6. IPv4: true; IPv6: true IPv4: false; IPv6: true IPv4: true; IPv6: false IPv4: false; IPv6: false Set IPv4 pingEnabled to true/false Set IPv4 pingEnabled to true/false via Common Configuration. Set IPv6 pingEnabled to true/false Set IPv6 pingEnabled to true/false via Common Configuration, if supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Ping the DUT for success Ping the DUT via IPv4 which is expected to succeed Ping the DUT via IPv6 for success Ping the DUT via IPv6 for success using the global IPv6 address.

23.12.4.1-12 IPv4 Unrecognized Extensions

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4 Unrecognized Extensions
Explanation	LXI devices shall ignore extension attributes they do not recognize.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Add additional attribute to IPv4 element

Add an additional attribute to IPv4 element.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.5-1 IPv6 Required

Category

LXI Security

Test Type

Kerberos Test, automated

Rule

IPv6 Required

Explanation

Since IPv6 is required in devices that implement the LXI IP Version 6 Extended Function, the required attributes are only required in implementations that implement IPv6.

Pre Condition

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check test configuration for LXI IPv6

Check test configuration for LXI IPv6. If configured, test results depending on attribute testing. If IPv6 not supported, it is an automatic pass.

Dependencies

23.12.5.1-1	23.12.5.1-2	23.12.5.1-3
23.12.5.1-4	23.12.5.1-5	23.12.5.1-6
23.12.5.1-7	23.12.5.1-8	23.12.5.1-9
23.12.5.1-10	23.12.5.1-11	

23.12.5.1-1 IPv6 Attribute Enabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Attribute Enabled Required
Explanation	Attribute enabled shall be implemented. Enabled generally enables or disables IPv6 capability.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 DHCP router Enable IPv6 DHCP address assignment on the router. Ensure the DUT has no RA address any more. Ensure the DUT has a DHCP address. Get DHCP IPv6 from mdns Get the DHCP address only via mDNS. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Enable IPv6 'PingEnabled' attribute Set IPv6 'PingEnabled' attribute value to true. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Check availability of enabled attribute in all IPv6 elements Check the availability of enabled attribute in all IPv6 elements in the Common Configuration. Disable IPv6 'enabled' attribute Set IPv6 'enabled' attribute value to false.

Enable IPv6 'PingEnabled' attribute

Set IPv6 'PingEnabled' attribute value to true.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Ping the DUT via IPv6 for failure

Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail.

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Ping the DUT via IPv6 for success

Ping the DUT via IPv6 for success using the global IPv6 address.

23.12.5.1-2 IPv6 Attribute DHCPEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Attribute DHCPEnabled Required
Explanation	Attribute DHCPEnabled shall be implemented. DHCPEnabled represents the state of the device IPv6 DHCP protocol. If True, configuration is accepted via the DHCP protocol.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 DHCP router Enable IPv6 DHCP address assignment on the router. Ensure the DUT has no RA address any more. Ensure the DUT has a DHCP address. Get DHCP IPv6 from mdns Get the DHCP address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check availability of DHCPEnabled in all IPv6 elements

Check the availability of DHCPEnabled attribute in all IPv6 elements.

Disable IPv6 DHCPEnabled attribute

Disable IPv6 DHCPEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check mdns advertisement of DHCPv6 address has stopped

Check mdns advertisement of DHCPv6 address has stopped.

Ping IPv6 DHCP address for failure

Ping the device via DHCPv6 address for failure.

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

Ping IPv6 DHCP address for success

Ping the device via DHCPv6 address for success.

23.12.5.1-3 IPv6 Attribute RAEnabled Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: IPv6 Attribute RAEnabled Required

Explanation: Attribute RAEnabled shall be implemented. RAEnabled represents the state of address generation based on the router advertisement.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 RA router

Enable IPv6 RA address assignment on the router.
Ensure the DUT has no DHCP address any more.
Ensure the DUT has a RA address.

Connect DUT

Connect the DUT to the test network

Get RA IPv6 from mdns

Get the RA address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable IPv6 PrivacyModeEnabled attribute for RA

Enable IPv6 PrivacyModeEnabled attribute for RA via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Check availability of RAEnabled in IPv6 element

Check the availability of RAEnabled attribute in IPv6 elements.

Disable IPv6 RAEnabled attribute

Disable IPv6 RAEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check the mdns advertisement of RA address has stopped

Check the mdns advertisement of RA address has stopped

Ping IPv6 RA address for failure

Ping device via RA address for failure

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get RA IPv6 from mdns

Get the RA address only via mDNS.

Ping IPv6 RA address for success

Ping the IPv6 RA address for success.

23.12.5.1-4 IPv6 Attribute staticAddressEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Attribute staticAddressEnabled Required
Explanation	Attribute staticAddressEnabled shall be implemented. staticAddressEnabled indicates if the device uses the static address configured with LXIDeviceSpecificConfiguration/IPv6/StaticAddress.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

Enable IPv6 DHCP router

Enable IPv6 DHCP address assignment on the router.
Ensure the DUT has no RA address any more.
Ensure the DUT has a DHCP address.

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get identification file

Get the identification file from the device under test

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Set static IP

Set the static IP in the Device Specific Configuration xml.

PUT Device Specific Configuration

PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

Enable IPv6 staticAddressEnabled attribute via Common Configuration

Use the Common Configuration from the DUT and set the IPv6 attribute staticAddressEnabled to enabled.

Disable IPv6 DHCPEnabled and RAEnabled attributes via Common Configuration

Use the Common Configuration from the DUT and disable the IPv6 attributes DHCPEnabled and RAEnabled.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Disable IPv6 RA and DHCP routers

Disable IPv6 RA and IPv6 DHCP on the networks router. This forces the device to loses its IPv6 RA and DHCPv6 address once the lease time has expired.

Disconnect DUT

Disconnect the DUT from the test network

Connect DUT

Connect the DUT to the test network

Get IPv6 static address from mdns

Get IPv6 static address from mdns. Look for single _lxi._tcp service via mdns, get the IPv6 addresses from the service and filter for IPv6 static IP address.

Test Procedure

Check the availability of staticAddressEnabled attribute in IPv6 element

Check the availability of staticAddressEnabled attribute in IPv6 element.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check advertisement of IPv6 static address via mDNS stopped

Check the advertisement of the IPv6 static address via mDNS has stopped.

Ping IPv6 static address for failure

Ping the DUT via IPv6 static address and expect it to fail.

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 staticAddressEnabled attribute via Common Configuration

Use the Common Configuration from the DUT and set the IPv6 attribute staticAddressEnabled to enabled.

Disable IPv6 DHCPEnabled and RAEnabled attributes via Common Configuration

Use the Common Configuration from the DUT and disable the IPv6 attributes DHCPEnabled and RAEnabled.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check advertisement of IPv6 static address via mDNS

Ensure the IPv6 static address is being advertised via mDNS. Look for single lxi service, get the IPv6 address from the service and ensure it is the expected static IPv6 address.

Ping IPv6 static address for success

Ping the DUT's IPv6 static address and expect a successful ping.

23.12.5.1-5 IPv6 Attribute privacyModeEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Attribute privacyModeEnabled Required
Explanation	Attribute privacyModeEnabled shall be implemented. When privacyModeEnabled is enabled, neither the link local address, unique local address nor the RA-generated addresses include the device MAC address.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Get RA IPv6 from mdns Get the RA address only via mDNS.

	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
	Get identification file
	Get the identification file from the device under test
Test Procedure	Check availability of PrivacyModeEnabled in IPv6 elements
	Check the availability of PrivacyModeEnabled attribute in IPv6 elements.
	Disable PrivacyModeEnabled attribute
	Disable the PrivacyModeEnabled attribute in the Common Configuration.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	Get MACAddress from Identification file
	Get the MACAddress from the XML Identification file for further usage.
	Get RA IPv6 from mdns
	Get the RA address only via mDNS.
	Verify Privacy Setting is disabled
	Verify Privacy Setting is disabled by investigating the RA IPv6 address.
	Enable PrivacyModeEnabled attribute
	Enable the PrivacyModeEnabled attribute in the Common Configuration.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	Get RA IPv6 from mdns
	Get the RA address only via mDNS.
	Verify Privacy Setting is enabled
	Verify the Privacy Setting is enabled by investigating the RA IPv6 address.

23.12.5.1-6 IPv6 Attribute mDNSEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Attribute mDNSEnabled Required
Explanation	Attribute mDNSEnabled shall be implemented. mDNSEnabled represents the state of the IPv6 multicast DNS responder in the device.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.4.1-6

23.12.5.1-7 IPv6 Optional Dynamic DNS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Optional Dynamic DNS

Explanation	Dynamic DNS is optional for LXI devices. Therefore, if not implemented, the device shall ignore this attribute on a PUT.
Pre Condition	Enable IPv6 RA router Enable IPv6 RA address assignment on the router. Ensure the DUT has no DHCP address any more. Ensure the DUT has a RA address. Connect DUT Connect the DUT to the test network Get RA IPv6 from mdns Get the RA address only via mDNS. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the availability of dynamicDNSEnabled attribute Check the availability of dynamicDNSEnabled attribute. If attribute is available and configured, test passes. Otherwise,if attribute is not available and not configured, test continues to further steps. Enable IPv6 dynamicDNSEnabled attribute Enable IPv6 dynamicDNSEnabled attribute by setting or adding dynamicDNSEnabled attribute with value true in IPv6 element, if not available. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Disable IPv6 dynamicDNSEnabled attribute Disable IPv6 dynamicDNSEnabled attribute by setting or adding dynamicDNSEnabled attribute with value false in IPv6 element, if not available. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.5.1-8 IPv6 Devices Without Dynamic DNS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Devices Without Dynamic DNS
Explanation	Devices that do not implement dynamicDNS shall omit this attribute on a GET.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.5.1-7

23.12.5.1-9 Attribute IPv6 IPv6DynamicDNS Required

Category	LXI Security
Test Type	Kerberos Test, automated

Rule	Attribute IPv6 IPv6DynamicDNS Required
Explanation	Attribute IPv6DynamicDNS shall be implemented irrespective of if IPv4DynamicDNS is implemented.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.4.1-10

23.12.5.1-10 Attribute IPv6 pingEnabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv6 pingEnabled Required
Explanation	Attribute pingEnabled shall be implemented. PingEnabled represents the state of the IPv6 ICMP ping function.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.4.1-11

23.12.5.1-11 IPv6 Unrecognized Extensions

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 Unrecognized Extensions
Explanation	LXI devices shall ignore extension attributes they do not recognize.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) Enable IPv6 DHCPEnabled attribute Enable IPv6 DHCPEnabled attribute via Common Configuration. Enable IPv6 RAEnabled attribute Enable IPv6 RAEnabled attribute via Common Configuration. Disable IPv6 staticAddressEnabled Disable IPv6 staticAddressEnabled attribute via Common Configuration. Enable IPv6 DHCP router Enable IPv6 DHCP address assignment on the router. Ensure the DUT has no RA address any more. Ensure the DUT has a DHCP address. Connect DUT Connect the DUT to the test network Get DHCP IPv6 from mdns Get the DHCP address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Add an additional attribute to IPv6 element

Add an additional attribute to IPv6 element, which is unknown to the device.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.5-2 Devices Without IPv6 Implementation

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Devices Without IPv6 Implementation
Explanation	Devices shall implement IPv6/@enabled. If the device does not implement IPv6 it shall always return false. If LXICommonConfiguration/@strict attribute is false such a device ignores the IPv6 element on a PUT.
Test Procedure	Computed by other tests

This test is computed by the result of other tests.

Dependencies	23.12.5.1-1

23.12.6-1 HTTP Port Enabled

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HTTP Port Enabled
Explanation	If no services are specified the server at this port is disabled.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the availability of HTTP

Check the availability of HTTP element in the Common Configuration.

Enable HTTP

Enable HTTP via Common Configruation

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Remove all of the HTTP services

Remove all of the HTTP services from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Ensure HTTP port is not active

Ensure HTTP port is not active. Do a port scan.

23.12.6.1-1 Requirements HTTP

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Requirements HTTP

Explanation: Devices that implement the unsecure HTTP protocol shall implement at least the disable and redirectAll settings of @operation. Operation controls if the HTTP server is enabled, disabled, or if it forwards all requests to HTTPS.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable HTTP API-LXISecurity and Human-Interface services

Enable HTTP API-LXISecurity and Human-Interface services via Common Configuration.

Test Procedure

Check availability of HTTP operation attribute on all interfaces

Check the availability of HTTP operation attribute on all interfaces.

Set HTTP operation attribute value

Set the HTTP operation attribute value to enable/disable/redirectAll.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

23.12.6.1-2 HTTP Port Number

Category: LXI Security

Test Type: Kerberos Test, manual

Rule: HTTP Port Number

Explanation: The LCI HTTP port for the LXI Web interface and the LXI API services shall be 80.

Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check interfaces API-LXISecurity and Human-Interface services Check interfaces for HTTP API-LXISecurity and Human-Interface services Modify HTTP port Modify HTTP port for API-LXISecurity and Human-Interface (e.g. from port 80 to port 90). PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Get root webpage via HTTP port, expect failure response Get root webpage via HTTP port (e.g. default port 80) and expect failure response. Port has been modified. Get Common Configuration via modified HTTP port, expect success response Fetch the Common Configuration from the device via the modified HTTP port (e.g. port 90) and expect success response. Get Common Configuration via HTTP port, expect failure response Fetch the Common Configuration from the device via HTTP port (e.g. default port 80) and expect failure response. Port has moved away from default port. Do LCI The tester is prompted to do a manual LAN reset on the DUT. Get Common Configuration via HTTP port, expect success response Fetch the Common Configuration from the device via HTTP port (e.g. default port 80) and expect success response. Get root webpage via HTTP port, expect success response Get root webpage via HTTP port (e.g. default port 80) and expect success response.

23.12.6.1-3 Attribute HTTP Port Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute HTTP Port Required
Explanation	Attribute port shall be implemented. TCP port of the HTTP server.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.6.1-2

23.12.6-2 HTTP unsecure Mode

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HTTP unsecure Mode
Explanation	If any service is enabled that permits changing the device configuration over an unencrypted connection the device is in unsecure mode.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the availability of HTTP unsecure service Check the availability of HTTP unsecure service. Set the DUT to Non-Unsecure Mode Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode. Turn of all unsecure services Turn of all unsecure services. Go through the Common Configuration and disable all unsecure services. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check unsecure mode for interface is false Check the unsecure mode of the interface is set to false in the Common Configuration. Enable each HTTP unsecure service Enable each HTTP unsecure service. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is true

Check the unsecure mode of the interface is set to true in the Common Configuration.

Disable each HTTP unsecure service

Disable each HTTP unsecure service.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

23.12.6.2-1 HTTP Device Queried

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HTTP Device Queried
Explanation	When the device is queried, it shall provide a Service element for each service provided by the device, with the Service/@enable attribute indicating those that are currently enabled..
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Availability of HTTP Ensure that the HTTP element is available in the Common Configuration. Enable HTTP operation attribute Enable the HTTP operation attribute via Common Configuration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Disable HTTP Human-Interface service Disable the HTTP Human-Interface service via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get root webpage via HTTP, expect failure

Get root web Page via HTTP and expect failure response.

Enable HTTP Human-Interface service

Enable the HTTP Human-Interface service via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get root webpage via HTTP

Get root webpage via HTTP and expect success response.

Disable HTTP API-LXISecurity service

Disable the HTTP API-LXISecurity service via Common-Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get Common Configuration via HTTP port, expect failure response

Fetch the Common Configuration from the device via HTTP port (e.g. default port 80) and expect failure response. Port has moved away from default port.

Enable HTTP API-LXISecurity service

Enable the HTTP API-LXISecurity service via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

23.12.7-1 HTTPS Human Interface Content

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HTTPS Human Interface Content
Explanation	The HTTPS web human interface content served by LXI Secure devices shall be a superset of the content available via HTTP. That is, a device is not permitted to only offer a subset of the HTTP human interface over the secure HTTPS connection.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable HTTP protocol with Basic authentication

Enable HTTP protocol with Basic authentication via Common Configuration.

Enable HTTPS protocol with Basic authentication

Enable HTTPS protocol with Basic authentication via Common Configuration.

Setup User/Password with API-Access

Setup User/Password with API-Access via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Check the available Webpages in the test configuration

Check the available Webpages in the test configuration.

Call webpage via HTTP and expect success response

Call webpage via HTTP and expect success response. It may also be possible to get a failure response as a call to a protected webpage over insecure connection(HTTP) is not allowed.

Call webpage via HTTPS and expect success response

Call webpage via HTTPS and expect success response.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.7.1-1 HTTPS Default Port

Category: LXI Security

Test Type: Kerberos Test, manual

Rule: HTTPS Default Port

Explanation: The default HTTPS port shall be 443 for the Human Interface and the LXI API Service.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Modify HTTPS port for Service 'Human-Interface' and 'API-LXISecurity' Modify HTTPS port away from default port. (e.g. from 443 to 446) PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Get root webpage via HTTPS, expect failure Get root web Page via HTTPS port (e.g. default,443) and expect failure response. Either the wrong port is given or Human-Interface is disabled. Get Common Configuration via HTTPS port and expect failure response Get the Common Configuration via HTTPS port (e.g. default,443) from the device and expect failure response. Either the port is wrong, API-LXISecurity is not enabled or no authentication is given. Get Common Configuration via modified HTTPS port and expect success GET Common Configuration via the modified HTTPS port (e.g. 446) and expect a success response from the device. Do LCI The tester is prompted to do a manual LAN reset on the DUT. Get Common Configuration via HTTPS port and expect success response GET Common Configuration via HTTPS port (e.g. default,443) and expect success response. The HTTPS port is enabled, API-LXISecurity is enabled, API-Key is given. Get Common Configuration via modified HTTPS port and expect failure GET Common Configuration via the modified HTTPS port (e.g. 446) and expect a failure response from the device. Ensure HTTPS port for 'Human-Interface' and 'API-LXISecurity' have reverted Ensure HTTPS port for 'Human-Interface' and 'API-LXISecurity' have reverted to the default value(e.g. 443). Get root webpage via HTTPS, expect success Get root webpage via HTTPS port (e.g. default, 443) and expect success response. The HTTPS port is enabled, the Human-Interface is enabled and no authentication is required.

23.12.7.1-2 Element HTTPS Port Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Element HTTPS Port Required
Explanation	Element Port shall be implemented. TCP port of the HTTPS server.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.7.1-1

23.12.7.1-3 Element HTTPS ClientAuthenticationRequired Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Element HTTPS ClientAuthenticationRequired Required
Explanation	Element clientAuthenticationRequired shall be implemented. The clientAuthenticationRequired indicates if clients are required to authenticate as configured in this element.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Setup User/Password with API-Access Setup User/Password with API-Access via Common Configuration. Enable Human-Interface and API-LXISecurity with basic authentication Enable the HTTPS services Human-Interface and API-LXISecurity with basic authentication via the Common COnfiguration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Ensure clientAuthenticationRequired is available on all HTTPS elements Ensure clientAuthenticationRequired attribute is available on all HTTPS elements. Disable clientAuthenticationRequired Set the clientAuthenticationRequired attribute value to false. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration without authentication GET the CommonConfiguration from the device without authentication. Expect the call to fail as no authentication was given. '401 Unauthorized' error expected. Get root webpage via HTTPS without authentication, expect success Get root webpage via HTTPS without authentication and expect success response as client authentication is not required. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get root webpage via HTTPS with authentication and expect success response

Get the devices root webpage via HTTPS with authentication and expect success response. The HTTPS port is enabled, the Human-Interface is enabled and the correct authentication data has been given.

Enable clientAuthenticationRequired

Set the clientAuthenticationRequired attribute value to true.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration without authentication

GET the CommonConfiguration from the device without authentication. Expect the call to fail as no authentication was given. '401 Unauthorized' error expected.

Get root webpage via HTTPS without authentication and expect failure response

Get the devices root webpage via HTTPS without authentication and expect failure response as authentication should be required.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get root webpage via HTTPS with authentication and expect success response

Get the devices root webpage via HTTPS with authentication and expect success response. The HTTPS port is enabled, the Human-Interface is enabled and the correct authentication data has been given.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.7-2 HTTPS Without Service

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: HTTPS Without Service

Explanation: If no services are enabled, then the HTTPS server is disabled. In addition to the LXI-required HTTP client authentication, LXI devices should provide application-level authentication

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Disable all HTTPS services

Disable all HTTPS services.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get root webpage via HTTPS, expect failure

Get root web Page via HTTPS port (e.g. default,443) and expect failure response. Either the wrong port is given or Human-Interface is disabled.

Ensure HTTPS port is not active

Ensure HTTPS port is not active. Do a port scan on the device.

Post Condition

Enable all HTTPS services

Enable all HTTPS services. If HTTP supported, this can automated by enabling HTTPS via the Comon Coonfiguration on HTTP, otherwise a user interaction may be required to ensure the next tests can continue.

23.12.7.2-1 HTTPS Device Queried

Category

LXI Security

Test Type

Kerberos Test, manual

Rule

HTTPS Device Queried

Explanation

When the device is queried, it shall provide a Service element for each service provided by the device, with the Service/@enable attribute indicating those that are currently enabled

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Disable HTTPS Human-Interface service

Disable the HTTPS Human-Interface service via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get root webpage via HTTPS, expect failure

Get root web Page via HTTPS port (e.g. default,443) and expect failure response. Either the wrong port is given or Human-Interface is disabled.

Enable HTTPS Human-Interface service

Enable the HTTPS service Human-Interface via the Common Configuration

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get root webpage via HTTPS, expect success

Get root webpage via HTTPS port (e.g. default, 443) and expect success response. The HTTPS port is enabled, the Human-Interface is enabled and no authentication is required.

Disable HTTPS API-LXISecurity service

Disable the HTTPS API-LXISecurity service via Common Confgiuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get Common Configuration via HTTPS port and expect failure response

Get the Common Configuration via HTTPS port (e.g. default,443) from the device and expect failure response. Either the port is wrong, API-LXISecurity is not enabled or no authentication is given.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Post Condition

Enable HTTPS Human-Interface service

Enable the HTTPS service Human-Interface via the Common Configuration

Enable HTTPS API-LXISecurity service

Enable the HTTPS API-LXISecurity service via Common Confgiuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.7-3 HTTPS Application-level Client Authentication

Category: LXI Security

Test Type: Vendor Declaration

Rule: HTTPS Application-level Client Authentication

Explanation: If the device is using application-level client authentication, none of the sub elements indicating HTTP client authentication need to be enabled in the HTTPS element.

23.12.7-4 HTTPS LXI Common Configuration With Scheme

Category: LXI Security

Test Type: Kerberos Test, automated

Rule	HTTPS LXI Common Configuration With Scheme
Explanation	When returning the LXI Common Configuration, if a scheme is implemented, then the element representing that scheme shall be present. This permits clients to determine what schemes are available on the device.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the availability of declared SCHEME in the Common Configuration Check each declared SCHEME is given in the Common Configuration. A SCHEME is a declared authentication scheme such as Basic, Digest etc., these must be declared in the Test configuration. Note: As Basic is the only LXI required scheme, any configured scheme will be verified to be available in the Common Configuration, however only Basic will be tested functionally.

23.12.7-5 HTTPS LCI Security Scheme

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	HTTPS LCI Security Scheme
Explanation	After an LCI, the security scheme is not changed.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Setup User/Password with API-Access Setup User/Password with API-Access via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Modify the security scheme to require Basic Modify the security scheme to require Basic PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Call webpage via HTTPS using Basic authentication and expect success response Call webpage via HTTPS using Basic authentication and expect success response. Do LCI The tester is prompted to do a manual LAN reset on the DUT. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Ensure Basic scheme configuration is unchanged Ensure the Basic scheme configuration is unchanged in the Common Configuration. Call webpage via HTTPS using Basic authentication and expect success response Call webpage via HTTPS using Basic authentication and expect success response.
Post Condition	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Remove User/Password Remove previously created Usernames and Passwords from the Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.7-6 HTTPS LXI API services Enabled

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	HTTPS LXI API services Enabled
Explanation	On LCI the LXI Web interface and the LXI API services shall be enabled
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Disable HTTPS API-LXISecurity service

Disable the HTTPS API-LXISecurity service via Common Confgiuration.

Disable HTTPS Human-Interface service

Disable the HTTPS Human-Interface service via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get Common Configuration via HTTPS port and expect failure response

Get the Common Configuration via HTTPS port (e.g. default,443) from the device and expect failure response. Either the port is wrong, API-LXISecurity is not enabled or no authentication is given.

Get root webpage via HTTPS, expect failure

Get root web Page via HTTPS port (e.g. default,443) and expect failure response. Either the wrong port is given or Human-Interface is disabled.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get root webpage via HTTPS, expect success

Get root webpage via HTTPS port (e.g. default, 443) and expect success response. The HTTPS port is enabled, the Human-Interface is enabled and no authentication is required.

Verify HTTPS API-LXISecurity and Human-Interface are active

Verify that the HTTPS API-LXISecurity and Human-Interface services are active.

23.12.8.1-1 Service Name Rules

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Service Name Rules

Explanation: LXI Service names are case sensitive. LXI Security specifies the following services: Human-Interface, API-LXISecurity, API-Device and other

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check for availability of Service with name Human-Interface

Check the service with name Human-Interface is available.

Check for availability of Service with name API-LXISecurity

Check the service with name API-LXISecurity is available.

Check for availability of Service with name API-Device

Check the service with name API-LXISecurity is available.

23.12.8.1-2 Attribute Service Name Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute Service Name Required

Explanation: The name attribute shall be implemented. The name indicates the name of the service.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Check for 'name' attribute for each HTTPS service

Ensure each HTPS service has a 'name' attribute.

23.12.8.1-3 Attribute Service Enabled Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute Service Enabled Required

Explanation: The enabled attribute shall be implemented. Note this attribute is syntactically required.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies: 23.12.7.2-1

23.12.8.1-4 Service Devices Without additional Attributes

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Service Devices Without additional Attributes

Explanation: Devices that do not understand additional attributes shall ignore them.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

	Connect DUT	
		Connect the DUT to the test network
	Get IP from mdns	
		Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration	
		GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Add additional unknown attributes	
		Add additional unknown attributes to a service. These shall be ignored by the device if unknown.
	PUT Common Configuration	
		PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.8.2-1 Service Element Basic

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Service Element Basic
Explanation	Devices shall implement Basic. When Basic is configured, devices may not be in unsecure mode.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.7.1-3

23.12.8.2-2 Service Element Digest

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Service Element Digest
Explanation	Devices may implement Digest. When Digest is configured, devices may not be in unsecure mode.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.7.1-3

23.12.8.2-3 Service Default Value Enabled Attribute

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Service Default Value Enabled Attribute
Explanation	The default value of the enabled attribute of extension elements shall be True so that the presence of the element without a value indicates the mechanism is enabled. The element name should match the authentication scheme in the IANA HTTP Authentication Schemes Registry.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Disable all additional Extension elements

Disable all additional Extension elements, which means all except 'Basic' and 'Digest' authentication

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Remove schemes enabled attribute from HTTPS Human-Interface service

The HTTPS Human-Interface service has Authentication Mechanisms. Each of these have an enabled attribute. In this teststep the enabled attribute of these Authentication Mechanism schemes shall be removed.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Verify the removed extension is enabled

Verify the removed extension has become enabled, meaning the enabled attribute is set to true.

23.12.8.2-4 Extension HTTPS Client-authentication Scheme

Category: LXI Security

Test Type: Vendor Declaration

Rule: Extension HTTPS Client-authentication Scheme

Explanation: Any extension HTTPS client-authentication scheme is permitted with unsecure mode false.

23.12.9-1 SCPIRaw Receive LXI Common Configuration

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: SCPIRaw Receive LXI Common Configuration

Explanation: When the device receives an LXI Common Configuration, only those SCPIRaw ports indicated and enabled shall be available on the device.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Test Procedure

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get Capabilities

Get the Capabilities for this test case from the device via Common Configuration.

Fill SCPIRaw elements to size of capabilities

Depending on the test configuration, add to the Common Configuration as many SCPIRaw elements as possible.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Disable SCPIRaw

Disable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get current TCP/IP port for SCPIRaw

Get current TCP/IP port for SCPIRaw from the Common Configuration.

Create TCP/IP client connection, expect failure

Create a TCP/IP client connection, this is expected to fail.

Ensure SCPIRaw port is not active

Do a port scan to ensure SCPIRaw port is not active.

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Create TCP/IP client connection, expect success

Create TCP/IP client connection and expect success as the correct port is being used.

Validate ScpiRaw connection

Validate ScpiRaw connection by querying the SCPI *IDN command.

Modify SCPIRaw port

Modify SCPIRaw port by setting the attribute port value of the SCPIRaw element in the Commom Configuration

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Create TCP/IP client connection, expect success

Create TCP/IP client connection and expect success as the correct port is being used.

Validate ScpiRaw connection

Validate ScpiRaw connection by querying the SCPI *IDN command.

Create TCP/IP client connection through old port, expect failure

Create a TCP/IP client connection using the old port, this is expected to fail as the port has been changed.

Ensure old port is not active.

Ensure old port is not active by doing a port scan. This step depends on the test and may be for example the SCPIRaw, SCPITLS, Telnet or even HiSLIP port.

Post Condition

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

23.12.9.1-1 Attribute SCPIRaw Enabled Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute SCPIRaw Enabled Required

Explanation: The enabled attribute shall be implemented. Enabled enables the SCPIRaw server at this address.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: 23.12.9-1

23.12.9.1-2 Operating in unsecure mode if SCPIRaw is enabled

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Operating in unsecure mode if SCPIRaw is enabled

Explanation: The device is operating in unsecure mode if SCPIRaw is enabled

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure indicator for false

Check the unsecure indicator state through the Common Configuration and expect it to be false.

Test Procedure

Enable SCPIRaw

Enable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPIRaw not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check interface unsecure state for true

Check the interface unsecure state value for true.

Disable SCPIRaw

Disable SCPIRaw on the device by setting the Enabled attribute of the SCPIRaw element it in the Common Configuration

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check interface unsecure state for false

Check the interface unsecure state value for false.

23.12.9.1-3 Attribute SCPIRaw Port Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute SCPIRaw Port Required
Explanation	The port attribute shall be implemented. The port attribute specifies the port of this SCPIRaw server
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.9-1

23.12.9-2 Report Configuration

Category	LXI Security
Test Type	Vendor Declaration
Rule	Report Configuration
Explanation	When the device reports its configuration, an instance of SCPIRaw shall be provided for each active SCPIRaw connection. Devices should permit multiple clients to connect to a single SCPIRaw port.

23.12.9-3 Service SCPIRaw

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Service SCPIRaw
Explanation	SCPIRaw is required if the device implements SCPIRaw connections.
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check for at least one SCPIRaw instance Depending on the test configuration, at least one SCPIRaw instance is required.

23.12.10-1 SCPITLS Receive LXI Common Configuration

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	SCPITLS Receive LXI Common Configuration
Explanation	When the device receives an LXI Common Configuration, only those secure raw SCPI ports indicated and enabled shall be available on the device.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address

	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Get Capabilities
	Get the Capabilities for this test case from the device via Common Configuration.
	Fill SCPITLS elements to size of capabilities
	Depending on the test configuration, add to the Common Configuration as many SCPITLS elements as possible.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
	Disable SCPITLS
	Disable SCPITLS on the device by setting the Enabled attribute of the SCPITLS element it in the Common Configuration
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	Get current TCP/IP port for SCPITLS
	Get current TCP/IP port for SCPITLS from the Common Configuration.
	Create SCPITLS connection, expect failure
	Create a SCPITLS connection, expect the conenciton to fail.
	Ensure SCPITLS port is not active
	Do a port scan to ensure SCPITLS port is not active.
	Enable SCPITLS
	Enable SCPITLS on the device by setting the Enabled attribute of the SCPITLS element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and SCPITLS not supported.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	Create SCPITLS connection, expect success
	Create a SCPITLS connection, expect the connection to succeed
	Validate SCPITLS connection
	Validate SCPITLS connection by querying the SCPI *IDN command.
	Modify SCPITLS port
	Modify SCPITLS port by setting the attribute port value of the SCPITLS element in the Commom Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Create SCPITLS connection, expect success

Create a SCPITLS connection, expect the connection to succeed

Validate SCPITLS connection

Validate SCPITLS connection by querying the SCPI *IDN command.

Create SCPITLS connection through old port, expect failure

Create a SCPITLS connection using the old port, this is expected to fail as the port has been changed.

Ensure old port is not active.

Ensure old port is not active by doing a port scan. This step depends on the test and may be for example the SCPIRaw, SCPITLS, Telnet or even HiSLIP port.

23.12.10.1-1 Attribute SCPITLS Enabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute SCPITLS Enabled Required
Explanation	The enabled attribute shall be implemented. Enables the secure raw SCPI server at this port.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.10-1

23.12.10.1-2 Attribute SCPITLS Port Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute SCPITLS Port Required
Explanation	The port attribute shall be implemented. Port specifies the port of this secure raw SCPI server..
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.10-1

23.12.10.1-3 Attribute SCPITLS ClientAuthenticationRequired Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute SCPITLS ClientAuthenticationRequired Required
Explanation	The client Authentication Required attribute shall be implemented. The ClientAuthenticationRequired attribute indicates if client authentication is required. Secure raw SCPI connections use mutual TLS (mTLS) for client authentication.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Disable ClientAuthentication

Disable the ClientAuthentication of the SCPITLS connection.

Create SCPITLS connection with unknown, self-signed certificate

Create SCPITLS connection with a unknown, self-signed certificate and expect a valid connection as cleint authentication is disabld.

Enable ClientAuthentication

Enable the ClientAuthentication of the SCPITLS connection.

Create SCPITLS connection with unknown, self-signed certificate, expect failure

Create SCPITLS connection with an unknown, self-signed certificate and expect the connection to fail as client authentication is enabled.

Create SCPITLS connection with known certificate

Create SCPITLS connection with a known certificate and expect a valid conenction.

23.12.10.1-4 Attribute SCPITLS Capability Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute SCPITLS Capability Required

Explanation: The capability attribute shall be implemented. Capability is a read-only attribute. It indicates the approximate number of SCPITLS ports that the client may configure.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies: 23.12.10-1

23.12.10-2 SCPITLS Configuration Device Report

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: SCPITLS Configuration Device Report

Explanation: When the device reports its configuration, an instance of SCPITLS shall be included for each configured secure raw SCPI connection. If none are enabled, a single disabled SCPITLS element shall be returned to indicate to the client that the capability is available.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Ensure at least one SCPITLS element is available If the test configuration indicates SCPITLS to be supported, at least one SCPITLS element must be available. Disable all SCPITLS elements Disable all SCPITLS elements via the Common Configruation. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Ensure one SCPITLS element is available with capabilities Ensure one SCPITLS element is available with capabilities.

23.12.10-3 Requirements Raw SCPI connection

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Requirements Raw SCPI connection
Explanation	SCPITLS is required by LXI Security if the device implements secure raw SCPI connections.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.10-2

23.12.11.1-1 Attribute Telnet Enabled Required

Category	LXI Security
Test Type	Vendor Declaration
Rule	Attribute Telnet Enabled Required
Explanation	The enabled attribute shall be implemented. It indicates if the Telnet server is enabled.

23.12.11.1-2 Attribute Telnet Port Required

Category	LXI Security
Test Type	Vendor Declaration
Rule	Attribute Telnet Port Required
Explanation	The port attribute shall be implemented. The port attribute specifies the Telnet server port.

23.12.11.1-3 Requirements TLS On Telnet

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Requirements TLS On Telnet

Explanation	If the device implements TLS on Telnet it shall include the TLSRequired attribute in the query response regardless of the state of Telnet/@enabled
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check device supports Telnet Check device supports Telnet via Common Configuration. Disable Telnet Disable Telnet via Common Configuration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check availability of TLSRequired Check availability of TLSRequired, this is a required attribute. Enable Telnet Enable Telnet via Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and Telnet not supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check availability of TLSRequired Check availability of TLSRequired, this is a required attribute.

23.12.11.1-4 Attribute Telnet TLSRequired Required

Category	LXI Security
Test Type	Vendor Declaration
Rule	Attribute Telnet TLSRequired Required
Explanation	TLSRequired shall be implemented if the device Telnet implementation supports TLS.

23.12.11.1-5 Telnet MTLS Client Certificate Authentication

Category	LXI Security
Test Type	Vendor Declaration
Rule	Telnet MTLS Client Certificate Authentication
Explanation	The mTLS client certificate authentication configured in Interface/ClientAuthentication/ClientCertAuthentication shall be used.

23.12.11.1-6 Requirements mTLS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Requirements mTLS
Explanation	If the device implements mTLS (client authentication) on telnet it shall include the clientAuthenticationRequired attribute in the query response regardless of the state of Telnet/@enabled.
Pre Condition	Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check device supports Telnet Check device supports Telnet via Common Configuration. Disable Telnet Disable Telnet via Common Configuration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check the availability of clientAuthenticationRequired Check the availability of the attribute clientAuthenticationRequired for this test case. This attribute is expected to be available. Enable Telnet Enable Telnet via Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and Telnet not supported. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the availability of clientAuthenticationRequired

Check the availability of the attribute clientAuthenticationRequired for this test case. This attribute is expected to be available.

23.12.11.1-7 Attribute Telnet ClientAuthenticationRequired Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Telnet ClientAuthenticationRequired Required
Explanation	The clientAuthenticationRequired attribute shall be implemented if the device Telnet implementation supports TLS.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.11.1-6

23.12.11.1-8 Attribute Telnet Capability Required

Category	LXI Security
Test Type	Vendor Declaration
Rule	Attribute Telnet Capability Required
Explanation	The capability attribute shall be implemented. Capability is a read-only attribute. It indicates the approximate number of Telnet ports that the client may configure.

23.12.11.1-9 Telnet Devices Without additional Attributes

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Telnet Devices Without additional Attributes
Explanation	Devices that do not understand additional attributes shall ignore them.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the device supports TELNET Check the device supports TELNET via Common Configuration. Add unrecognized Telnet attribute Add an unrecognized Telnet attribute via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.12.1-1 Attribute HiSLIP Enabled Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute HiSLIP Enabled Required
Explanation	The enabled attribute shall be implemented. The enabled attribute indicates if the HiSLIP server is enabled.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check the device supports HiSLIP Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester. Check all HiSLIP elements for Enabled attribute Check all HiSLIP elements have an Enabled attribute available. Disable HiSLIP Disable HiSLIP by setting the enabled attribute of the HiSLIP element to false via Common Configuration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Get service name from mdns Get the service name for the device under test from mDNS. Wait HiSLIP service to disappear Wait for the HiSLIP mDNS service (_hislip._tcp) to disappear from the mDNS system. Get configured HiSLIP port and expect failure response Try to get the configured HiSLIP port via mdns and expect a failure response as the HiSLIP service should not be advertised anymore. Create HiSLIP connection, expect failure Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required. Ensure HISLIP port is not active Do a port scan of the device to ensure the HiSLIP port is not active. Enable HiSLIP Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Disable HiSLIP attributes mustStartEncrypted and encryptionMandatory

Disable the HiSLIP attribues mustStartEncrypted and encryptionMandatory attributes to establish HiSLIP connection without encryption. This may only be required if LXI Security is supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Create HiSLIP connection, expect success

Create a HiSLIP connection to the device-under-test (DUT) and expect a valid connection.

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Modify HiSLIP port via Common Configuration

Modify the HiSLIP port to something other than the dafult(4880) port.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Create HiSLIP connection, expect success

Create a HiSLIP connection to the device-under-test (DUT) and expect a valid connection.

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Ensure HiSLIP old port is not active

Do a port scan of the device to ensure the previous HiSLIP port is no more active after modifying the port.

23.12.12.1-2 HiSLIP unsecureMode

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HiSLIP unsecureMode
Explanation	The device is in unsecure mode unless both HiSLIP/@mustStartEncrypted and HiSLIP/@encryptionMandatory are true.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Check availability of LXI defined Authentication mechanisms

Check the availability of LXI defined Authentication mechanisms. At least one defined mechanism must be available such as ANONYMOUS, PLAIN, SCRAM, MTLS, etc.

Enable each authentication mechanism

Enable each given authentication mechanism via Common Configuration. This could be ANONYMOUS, PLAIN, SCRAM, MTLS, etc.

Setup User/Password with API-Access

Setup User/Password with API-Access via Common Configuration.

Generate root certificate

Generate a root certificate for testing. This certificate will be used for example to generate a derived certificate.

Add root certificate

Add root certificate to DUT via Common Configuration.

Set attribute mustStartEncrypted

Set the attribute mustStartEncrypted to true or false depending on the test case loop.

Set attribute encryptionMandatory

Set the attribute encryptionMandatory to true or false depending on the test case loop.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure indicator state

Verify the unsecure indicator state through Common Configuration. It can be true/false as per expected result. If the MustStartEncrypted is set to true and EncryptionMandatory is set to false, the unsecure flag should be true and vice versa. In the case both attributes are true,the unsecure flag should be false

Create HiSLIP connection without encryption

Create successful HiSLIP connection without encryption. This succeeds if the mustStartEncrypted and encryptionMandatory are both disabled, otherwise the connection fails.

Establish HiSLIP secure connection using specific authentication mechanism

Establish HiSLIP secure connection using specific authentication mechanism. Depending on the current test case iteration, the apropriate mechanism PLAIN, SCRAM, MTLS, Anonymous shall be used.

Turn off HiSLIP encryption on client side

Turn off the HiSLIP encryption on client side. If the DUT has encryptionMandatory disabled, the HiSLIP connection will not disconnect. HiSLIP connection should be disconnected when encryptionMandatory is enabled. A new HiSLIP connection will fail, if server has mustStartEncrypted enabled.

Turn on HiSLIP encryption on client side

Turn on HiSLIP encryption on client side. Successfully establish a HiSLIP secure connection using an authentication mechanism except in the case where mustStartEncryption is set to false and encrytionMandatory is set to true.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.12.1-3 Attribute HiSLIP Port Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute HiSLIP Port Required

Explanation: The port attribute shall be implemented. The port attribute indicates the TCP port from which the HiSLIP server is served.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies	23.12.12.1-2

23.12.12.1-4 Attribute HiSLIP MustStartEncrypted Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute HiSLIP MustStartEncrypted Required
Explanation	The mustStartEncrypted attribute shall be implemented. mustStartEncrypted controls the initial encryption. If enabled, a secure connection must be initially made to this server. It can be subsequently stepped down to an unsecure connection if encryptionMandatory is not true.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.12.1-3

23.12.12.1-5 HiSLIP MustStartEncrypted unsecure Mode

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	HiSLIP MustStartEncrypted unsecure Mode
Explanation	The device is in unsecure mode if mustStartEncrypted is false.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.12.1-3

23.12.12.1-6 Attribute HiSLIP encryptionMandatory Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute HiSLIP encryptionMandatory Required
Explanation	The encryptionMandatory attribute shall be implemented. The encryptionMandatory attribute indicates that this HiSLIP Server must always have encryption on. That is, the connection must be started securely, and the encryption may not be subsequently turned off.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check all HiSLIP elements for encryptionMandatory attribute Check all HiSLIP elements hae an encryptionMandatory attribute available.

23.12.12.1-7 HiSLIP EncryptionMandatory unsecure Mode

Category	LXI Security
Test Type	Kerberos Test, automated

Rule	HiSLIP EncryptionMandatory unsecure Mode
Explanation	The device is in unsecure mode if encryptionMandatory is false for any enabled HiSLIP servers.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.12.1-3

23.12.12.2-1 Support of Client Authentication

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Support of Client Authentication
Explanation	Devices that support the LXI Security Extended Function and the LXI HiSLIP Extended function shall support Client Authentication.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check all HiSLIP elements for 'ClientAuthenticationMechanisms' element Check all HiSLIP elements have a 'ClientAuthenticationMechanisms' element available.

23.12.13-1 ClientAuthenticationMechanisms Includes In Response

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthenticationMechanisms Includes In Response
Explanation	The device shall include in its response each element that it implements, indicating a false enable attribute where disabled. Devices shall omit the elements that represent mechanisms they do not support.
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies			
	23.12.13.1-1	23.12.13.1-3	23.12.13.1-4
	23.12.13.1-7		

23.12.13.1-1 AuthenticationMechanism Support Of ANONYMOUS

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	AuthenticationMechanism Support Of ANONYMOUS
Explanation	Devices that support LXI Security and the LXI HiSLIP Extended function shall support ANONYMOUS. The element ANONYMOUS indicates that clients can authenticate using the SASL anonymous mechanism.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Check ClientAuthentication mechanism ANONYMOUS is available

Check the ClientAuthentication element for AONYMOUS authentication mechanism is available.

Enable ANONYMOUS via Common Configuration

Enable the authentication mechanism ANONYMOUS via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection with ANONYMOUS

Establish a secured connection using ANONYMOUS authentication mechanism.

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Disable ANONYMOUS via Common Configuration

Disable the authentication mechanism ANONYMOUS via Common Configuration

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection with ANONYMOUS, expect failure

Establish a secured connection using ANONYMOUS authentication mechanism and expect the connection to fail.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

23.12.13.1-2 ClientAuthenticationMechanisms ANONYMOUS IVI Device Requirements

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthenticationMechanisms ANONYMOUS IVI Device Requirements
Explanation	The IVI-6.5 SASL Mechanism Specification details the specific device and client requirements for the generation of usernames and passwords. Devices shall comply with the IVI device requirements.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.17.1-2

23.12.13.1-3 ClientAuthenticationMechanisms Plain IVI Device Requirements

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthenticationMechanisms Plain IVI Device Requirements
Explanation	The IVI-6.5 SASL Mechanism Specification details the specific device and client requirements for the generation of usernames and passwords. Devices shall comply with the IVI device requirements.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.17.1-2

23.12.13.1-4 ClientAuthenticationMechanisms Support Of PLAIN

Category
LXI Security

Test Type
Kerberos Test, automated

Rule
ClientAuthenticationMechanisms Support Of PLAIN

Explanation
Devices that support LXI Security and the LXI HiSLIP Extended function shall support PLAIN. Configuring PLAIN does not put the device into unsecure mode.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Check the device supports HiSLIP

Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Set the DUT to Non-Unsecure Mode

Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

Setup User/Password with API-Access

Setup User/Password with API-Access via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Check clientAuthentication PLAIN is available

Check the ClientAuthentication element for PLAIN is available in the Common Configuration.

Enable PLAIN

Enable PLAIN authentication mechanism via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using PLAIN

Establish secure connection, using PLAIN Authentication

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Disable PLAIN via Common Configuration

Disable the authentication mechanism PLAIN via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using PLAIN, expect failure

Establish a secure connection using PLAIN Authentication and expect the connection to fail.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.13.1-5 ClientAuthenticationMechanisms SCRAM IVI Device Requirements

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthenticationMechanisms SCRAM IVI Device Requirements
Explanation	The IVI 6.5 SASL Mechanism Specification details the specific device and client requirements for the use of the SASL SCRAM mechanism with HiSLIP. Devices shall comply with the IVI device requirements.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.16.1-2

23.12.13.1-6 ClientAuthenticationMechanisms Support Of SCRAM

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthenticationMechanisms Support Of SCRAM
Explanation	Devices that support LXI Security and the LXI HiSLIP Extended function shall support SCRAM. Configuring SCRAM does not put the device into unsecure mode.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Check the device supports HiSLIP Check the device supports HiSLIP. This is validated by checking the test configuration input from the Tester. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Set the DUT to Non-Unsecure Mode Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode. Enable HiSLIP Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported. Setup User/Password with API-Access Setup User/Password with API-Access via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Check clientAuthentication mechanism SCRAM is available

Check the ClientAuthentication element for SCRAM authentication mechanism is available.

Enable SCRAM

Enable SCRAM authentication mechanism via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using SCRAM

Establish a secure connection using SCRAM Authentication and expect the conenction to succeed.

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Disable SCRAM via Common Configuration

Disable the authentication mechanism SCRAM via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using SCRAM, expect failure

Establish a secure connection using SCRAM Authentication and expect the connection to fail.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.13.1-7 ClientAuthenticationMechanisms Not Implemented Mechanisms

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: ClientAuthenticationMechanisms Not Implemented Mechanisms

Explanation: Devices shall ignore mechanisms that they do not implement.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Add unknown element in ClientAuthenticationMechanisms

Add an unknown element in ClientAuthenticationMechanisms in the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.13-2 **Device-specific SASL Mechanisms**

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Device-specific SASL Mechanisms
Explanation	Devices that implement device-specific SASL mechanisms shall follow the pattern of defining additional elements that enable and configure those mechanisms using the AuthenticationMechanism complex type, or types derived from it. The ClientAuthenticationMechanisms complex type has no attributes
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Check each AuthenticationMechanism element for enabled attribute Check each AuthenticationMechanism element has an enabled attribute.

23.12.14-1 **AuthenticationMechanism Client Authentication Capabilities**

Category	LXI Security
Test Type	Vendor Declaration
Rule	AuthenticationMechanism Client Authentication Capabilities
Explanation	Where possible, additional client authentication capabilities beyond the scope of the LXI Security Extended Function shall be created using this type. However, if those capabilities require additional configuration, they shall define their own type by extending the AuthenticationMechanism ComplexType.

23.12.14.1-1 **LCI Enable mechanism**

Category	LXI Security
Test Type	Kerberos Test, manual
Rule	LCI Enable mechanism
Explanation	On LCI, the enabled mechanisms do not change.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure

Get all authentication mechanism values

Get all of the authentication mechanism values from the Common Configuration for further processing.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get all authentication mechanism values

Get all of the authentication mechanism values from the Common Configuration for further processing.

Match enabled mechanisms did not change

Check enabled mechanisms in the Common Configuration. Ensure the configured mechanisms did not change after a PUT Common Configuration.

Invert enabled mechanisms

Invert enabled mechanisms in the Common Configuration. Iterate through all mechanism and invert the enabled attribute.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Do LCI

The tester is prompted to do a manual LAN reset on the DUT.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Get all authentication mechanism values

Get all of the authentication mechanism values from the Common Configuration for further processing.

Match enabled mechanisms did not change

Check enabled mechanisms in the Common Configuration. Ensure the configured mechanisms did not change after a PUT Common Configuration.

23.12.14.1-2 Attribute AuthenticationMechanisms Enable Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute AuthenticationMechanisms Enable Required

Explanation: Attribute enabled shall be implemented. The enabled attribute indicates that the SASL mechanism or HTTP scheme is enabled.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies

23.12.13.1-1	23.12.13.1-3	23.12.13.1-4
23.12.13.1-7		

23.12.15.1-1 Attribute VXI11 Enable Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute VXI11 Enable Required
Explanation	Attribute enabled shall be implemented. The device is in unsecure mode if VXI-11 is enabled. Enabled state of the VXI11 server at this address.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check the availability of VXI-11 element Check the availability of VXI-11 element in the Common Configuration Set the DUT to Non-Unsecure Mode Set all the Interface attributes value to Non-unsecure, which has impact on unsecure mode. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check unsecure mode for interface is false Check the unsecure mode of the interface is set to false in the Common Configuration.
Test Procedure	Enable VXI-11 Set VXI11 'enabled' attribute to true via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Check unsecure mode for interface is true Check the unsecure mode of the interface is set to true in the Common Configuration.

Disable VXI-11

Set VXI11 'enabled' attribute to false via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check unsecure mode for interface is false

Check the unsecure mode of the interface is set to false in the Common Configuration.

23.12.16-1 ClientAuthentication Information

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientAuthentication Information
Explanation	Information in ClientAuthentication shall be used by all protocols that provide client authentication. For instance, a certificate thumbprint that the device accepts for HiSLIP EXTERNAL authentication, will also be accepted for telnet mTLS.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check device supports HISLIP

Check device supports HISLIP via test configuration.

Check device supports Telnet

Check device supports Telnet via Common Configuration.

Check device supports SCPITLS

Check device supports SCPITLS via Common Configuration.

Enable HiSLIP

Enable HiSLIP on the device by setting the Enabled attribute of the HiSLIP element it in the Common Configuration. A PUT Common Configuration may fail, if strict mode is enabled and HiSLIP not supported.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Setup a root certificate and a thumbprint

Setup a root certificate and a thumbprint. Set a root certificate and a thunmprint via the Common Configuration.

Add root certificate and thumbprint to device

Add a root certificate and a thumbprint to the device by sending this via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection via HiSLIP with root certificate/thumbprint

Establish secure connection via HISLIP using a certificate derived from a root certificate or matches the thumbprint of a certificate on the device.

HiSLIP query *IDN

Query the SCPI *IDN command via HiSLIP and expect a valid response.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Create Telnet connection using root certificate/thumbprint

If supported, create a Telnet connection with the MTLS mechanism using a valid certificate to match against a root certificate or thumbprint.

Create SCPI-TLS connection using root certificate/thumbprint

If supported, create a SCPI-TLS connection with the MTLS mechanism using a valid certificate to match against a root certificate or thumbprint.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete Root certificates

Delete all Root certificates from the device via Common Configuration.

Delete CertThumbprint

Delete all CertThumbprint from the device via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.16.1-1 Attribute ClientAuthentication ScramHashIterationCount Required

Category	LXI Security
Test Type	Vendor Declaration
Rule	Attribute ClientAuthentication ScramHashIterationCount Required
Explanation	Attribute scramHashIterationCount shall be implemented. The attribute scramHashIterationCount sets the minimum iteration count that SCRAM uses to hash the client credentials. Required for devices that support the SCRAM SASL mechanism via the LXICommonConfiguration.

23.12.16.1-2 Attribute ClientAuthentication ScramChannelBindingRequired

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute ClientAuthentication ScramChannelBindingRequired
Explanation	Attribute scramChannelBindingRequired shall be implemented. Required for devices that support the SCRAM SASL mechanism via the LXICommonConfiguration.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Setup User/Password with API-Access Setup User/Password with API-Access via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Get service name from mdns Get the service name for the device under test from mDNS. Get HiSLIP Port Get the HiSLIP port, which is advertised via the mDNS service. Check SCRAM support Check SCRAM is supported via Common Configuration. Enable SCRAM Enable SCRAM authentication mechanism via Common Configuration. Modify ScramChannelBinding attribute Modify ScramChannelBinding attribute. Dependign on the test case this is changed between true and false. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using SCRAM without channel binding

Establish secure connection using SCRAM authentication mechanism without channel binding. If ScramChannelBinding is false, then expect success response otherwise expect failure response

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish secure connection using SCRAM with channel binding, expect success

Establish secure connection using SCRAM authentication mechanism with channel binding. The call is expected to succeed.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.16.2-1 Attribute ClientAuthentication ClientCredential

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute ClientAuthentication ClientCredential

Explanation: Element ClientCredential shall be implemented. ClientCredential contains an individual user with an optional password and an indication if this used has API Access rights.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of ClientCredential

Check availability of ClientCredential via Common Configuration.

23.12.16.2-2 Attribute ClientAuthentication ClientCertAuthentication

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute ClientAuthentication ClientCertAuthentication

Explanation: Element ClientCertAuthentication shall be implemented.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of ClientCertAuthentication

Check availability of ClientCertAuthentication via Common Configuration.

23.12.17.1-1 ClientCredential User Name Rule

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: ClientCredential User Name Rule

Explanation: LXI devices shall accept user names composed of alpha-numeric strings. User names shall be case-sensitive.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable API-LXISecurity with basic authentication

Enable the service API-LXISecurity with basic authentication.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure: Setup User/Password with API-Access

Setup User/Password with API-Access via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration with username/password, expect success

GET Common Configuration with valid username/password. Expect the call to succeed.

GET Common Configuration with username/password (wrong case), expect failure

GET the Common Configuration with a username/password pair which is not setup on the device. Expect the call to fail.

Check device supports HISLIP

Check device supports HISLIP via test configuration.

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish HISLIP secure connection with username/password, expect success

Establish HISLIP secure connection with username/password, expect success.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish HISLIP secure connection with username/password (wrong case), expect failure

Establish HISLIP secure connection with a username/password pair which is not setup on the device. Expect the connection to fail.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.17.1-2 ClientCredential User IVI Device Requirements

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientCredential User IVI Device Requirements
Explanation	The IVI-6.5 SASL Mechanism Specification details the specific device and client requirements for the generation of usernames and passwords. Devices shall comply with the IVI device requirements.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Create the client credential Create the client credential with empty user name/ user name larger than 255 octets/user name smaller than 255 octets/user name with @/user name with back slash PUT Common Configuration with client credential PUT Common Configuration with client credential. Expect failure response if empty user name/ user name larger than 255 octets otherwise expect success response

23.12.17.1-3 Attribute ClientCredential User

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute ClientCredential User
Explanation	Attribute user shall be implemented. Attribute user that may be authenticated on the device.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.17.1-1

23.12.17.1-4 Attribute ClientCredential APIAccess Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute ClientCredential APIAccess Required
Explanation	Attribute APIAccess shall be implemented. The attribute APIAccess indicates if this user is authorized to use the API.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable API-LXISecurity with basic authentication

Enable the service API-LXISecurity with basic authentication.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Setup User/Password with API-Access

Setup User/Password with API-Access via Common Configuration.

Setup User/Password without API-Access

Create client credential with user and password without API-Access.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration with API-Access, expect success

GET the Common Configuration with API-Access and expect a valid response XML.

GET Common Configuration with username/password without API Access, expect failure

GET Common Configuration with username/password without API Access and expect the call to fail as no API access for the username and password.

Check device supports HISLIP

Check device supports HISLIP via test configuration.

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish HISLIP secure connection with username/password, expect success

Establish HISLIP secure connection with username/password, expect success.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish HISLIP secure connection with username/password without API-Access, expect success

Establish HISLIP secure connection with username/password without API-Access, expect success.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.18.1-1 Attribute ClientCredential Password format Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute ClientCredential Password format Required
Explanation	Devices shall implement the formats specified.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.18.1-3

23.12.18.1-2 Attribute ClientCredential Password value Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute ClientCredential Password value Required
Explanation	Value contains the password in the format specified by format attribute.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.12.18.1-3

23.12.18.1-3 ClientCredential Password supported hash algorithm

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientCredential Password supported hash algorithm
Explanation	If the device does not support the requested hash algorithm, then Common Configuration put requests shall fail.The returned LXIProblemDetails/Title element shall contain an indication that the hash algorithm specified in the value attribute was invalid. The LXIProblemDetails / Instance shall have a comma separated list of accepted values.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Enable API-LXISecurity with basic authentication

Enable the service API-LXISecurity with basic authentication.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check device supports HISLIP

Check device supports HISLIP via test configuration.

Test Procedure

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Setup User/Password with an unsupported Hash

Create client credential for a unsupported hash algorithm via Common Configuration.

PUT Common Configuration, expect failure

PUT the Common Configuration to the device and expect failure response. Check previous step for better understanding. This may be due to incorrect data, no authentication or any other reason for the API call to fail.

Read LxiProblemDetails for supported hash algorithms

Read out the list of supported hash algorithms from the LxiProblemDetails

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Setup User/Password with a supported Hash

Create client credential for a supported hash algorithm via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Call webpage via HTTPS using Basic authentication and expect success response

Call webpage via HTTPS using Basic authentication and expect success response.

Enable PLAIN

Enable PLAIN authentication mechanism via the Common Configuration.

Enable SCRAM

Enable SCRAM authentication mechanism via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get service name from mdns

Get the service name for the device under test from mDNS.

Get HiSLIP Port

Get the HiSLIP port, which is advertised via the mDNS service.

Establish secure connection using PLAIN

Establish secure connection, using PLAIN Authentication

Establish secure connection using SCRAM

Establish a secure connection using SCRAM Authentication and expect the conenction to succeed.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Remove User/Password

Remove previously created Usernames and Passwords from the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.18.1-4 Attribute Password value

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute Password value
Explanation	Attribute value shall be implemented. Attribute value that may be authenticated on the device.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.12.18.1-3

23.12.19-1 ClientCertAuthentication Acceptance of Client Certificates

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientCertAuthentication Acceptance of Client Certificates
Explanation	Devices shall accept client certificates as valid if they are signed by a root certificate specified in this element, or if they have a thumbprint that matches a thumbprint specified in this element.
Test Procedure	Computed by other tests This test is computed by the result of other tests.

Dependencies	23.12.16-1

23.12.19.1-1 ClientCertAuthentication Root certification PEMs

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientCertAuthentication Root certification PEMs
Explanation	Root certification PEMs shall be semantically validated. For instance, expired root certificates shall not be used.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
Test Procedure	Setup valid root certificate Setup valid root certificate. Set a valid root certificate via the Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Check device supports HISLIP Check device supports HISLIP via test configuration. Get service name from mdns Get the service name for the device under test from mDNS. Get HiSLIP Port Get the HiSLIP port, which is advertised via the mDNS service. Create HiSLIP connection, expect failure Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required. Establish HISLIP secure connection using mTLS clientAuthentication, expect success Establish a HISLIP secure connection using mTLS clientAuthentication, expect success. Disconnect HiSLIP connection Disconnect the HiSLIP connection from DUT. Setup an expired root certificate Setup an expired root certificate. Set an expired root certificate via the Common Configuration. The device may fail to accept an expired root certificate.

PUT Common Configuration, expect failure

PUT the Common Configuration to the device and expect failure response. Check previous step for better understanding. This may be due to incorrect data, no authentication or any other reason for the API call to fail.

Create HiSLIP connection, expect failure

Connect to DUT via HiSLIP and expect the connection to fail. This could be because HiSLIP has been disabled, the wrong port is being used or encryption is required.

Establish HISLIP secure connection using mTLS clientAuthentication, expect failure

Establish a HISLIP secure connection using mTLS clientAuthentication and expect failure.

Disconnect HiSLIP connection

Disconnect the HiSLIP connection from DUT.

23.12.19.1-2 ClientCertAuthentication Support of RootCertPEM

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ClientCertAuthentication Support of RootCertPEM
Explanation	RootCertPEM shall be supported. RootCertPEM has a single root certificate the device shall use to validate client certificates
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Delete Root certificates Delete all Root certificates from the device via Common Configuration. PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
Test Procedure	Check for RootCertPEM element, expect absent Check for RootCertPEM element in the common-configuration, expect it to be absent. Generate self-signed root certificate Generate self-signed root certificate to be added to the DUT as a root certificate. Add root certificate Add root certificate to DUT via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check for RootCertPEM element

Check for RootCertPEM element. It is expected to be available.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete Root certificates

Delete all Root certificates from the device via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.19.1-3 ClientCertAuthentication Support of CertThumbprint

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: ClientCertAuthentication Support of CertThumbprint

Explanation: CertThumbprint shall be supported. Each instance of this element has the thumbprint of a client certificate.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete CertThumbprint

Delete all CertThumbprint from the device via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure

Check for CertThumbprint element, expect absent

Check for CertThumbprint element. It is expected to be missing/absent.

Generate Thumbprint certificate

Generate a Thumbprint of a certificate. This may be used to set to the DUT for MLS authentication.

Add Thumbprint

Add Thumbprint to the device via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check for CertThumbprint element

Check for CertThumbprint element and expect it to be available in the Common Configuration.

Post Condition

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete CertThumbprint

Delete all CertThumbprint from the device via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.20.1-1 Attribute CertThumbprint Hash Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute CertThumbprint Hash Required

Explanation: Attribute hash shall be implemented. The attribute hash indicates the hash function used to create this thumbPrint.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Generate Thumbprint certificate

Generate a Thumbprint of a certificate. This may be used to set to the DUT for MLS authentication.

Add Thumbprint

Add Thumbprint to the device via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Test Procedure: Check availability of Hash in all CertThumbprint elements

Check the availability of Hash in all CertThumbprint elements.

Post Condition: GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete CertThumbprint

Delete all CertThumbprint from the device via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.12.20.1-2 Attribute CertThumbprint ThumbPrint Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute CertThumbprint ThumbPrint Required

Explanation: Attribute thumbPrint shall be implemented. The attribute thumbPrint contains the certificate thumbPrint.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Test Procedure: Check availability of thumbPrint in all CertThumbprint elements

Check the availability of a thumbPrint in all CertThumbprint elements of the Common Configuration.

Post Condition: GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Delete CertThumbprint

Delete all CertThumbprint from the device via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.13-1 LXIDeviceSpecificConfigurationSchema LXI Device Specific Configuration

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXIDeviceSpecificConfigurationSchema LXI Device Specific Configuration
Explanation	Devices shall retain the LXI Device Specific configuration and only utilize it when automatic configuration is disabled. Thus, writing the LXI Device Specific Configuration while automatic configuration is active then disabling automatic configuration will result in the device using the configuration specified in LXI Device Specific Configuration.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address GET Common Configuration GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly. Ensure DHCP and AutoIP are enabled for IPv4 Ensure DHCP and AutoIP are enabled for IPv4. Use the Common Configuration for automated configuration. Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. GET Device Specific Configuration GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.
Test Procedure	Setup IPv4 static address Setup IPv4 static addressby putting the Device Specific Configuration to the DUT with a valid IPv4 static configuration. Setup IPv6 static address Setup IPv6 static address by putting the Device Specific Configuration to the DUT with a valid IPv6 static configuration. PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response. Ping IPv4 static address for failure Ping the DUT via IPv4 static address and expect it to fail.

Check advertisement of IPv4 static address via mDNS stopped

Check the advertisement of the IPv4 static address via mDNS has stopped.

Enable IPv6 staticAddressEnabled attribute via Common Configuration

Use the Common Configuration from the DUT and set the IPv6 attribute staticAddressEnabled to enabled.

Disable IPv6 DHCPEnabled and RAEnabled attributes via Common Configuration

Use the Common Configuration from the DUT and disable the IPv6 attributes DHCPEnabled and RAEnabled.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Check advertisement of IPv6 static address via mDNS

Ensure the IPv6 static address is being advertised via mDNS. Look for single lxi service, get the IPv6 address from the service and ensure it is the expected static IPv6 address.

Ping IPv6 static address for success

Ping the DUT's IPv6 static address and expect a successful ping.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Ensure IPv4 values are not the configured static values

Get the IPv4 values from the Device Spcific Configuration and ensure the values are not the expected static values.

Ensure IPv6 values are the configured static values

Ensure the given IPv6 values match the previously configured static values.

Enable IPv4 static by disabling DHCP and AutoIP

Enable IPv4 static addressing by disabling DHCP and AutoIP via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Ping IPv4 static address for expect success

Check the device is using IPv4 static address by pinging the static address and expect success

Check advertisement of IPv4 static address via mDNS

Ensure the IPv4 static address is being advertised via mDNS. Look for single lxi service, get the IP address from this service and ensure it is the expected static IPv4 address.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Ensure IPv4 values are the configured static values

Get the IPv4 values from the Device Spcific Configuration and ensure the values are the expected and configured static values.

Disable IPv4 static by enabling DHCP and AutoIP

Disable IPv4 static by enabling DHCP and AutoIP via the Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Remove IPv6 Static IP address from Device

Remove IPv6 Static IP address from Device by sending the Device Specific Configuration without IPv6 static address assigned.

PUT Device Specific Configuration

PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

Ping IPv4 static address for failure

Ping the DUT via IPv4 static address and expect it to fail.

Ping IPv6 static address for failure

Ping the DUT via IPv6 static address and expect it to fail.

Check advertisement of IPv4 static address via mDNS stopped

Check the advertisement of the IPv4 static address via mDNS has stopped.

Check advertisement of IPv6 static address via mDNS stopped

Check the advertisement of the IPv6 static address via mDNS has stopped.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Ensure IPv4 values are not the configured static values

Get the IPv4 values from the Device Spcific Configuration and ensure the values are not the expected static values.

Ensure IPv6 values are not the configured static values

Get the IPv6 values from the Device Spcific Configuration and ensure the values are not the expected static values.

23.13.1.1-1 Attribute LXIDeviceSpecificConfiguration Name Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute LXIDeviceSpecificConfiguration Name Required
Explanation	Attribute name shall be implemented. The attribute name indicates the name of the interface described by this document. name is required on a GET and shall indicate the name used for the interface in the LXICommonConfiguration Interface/@name attribute. Devices with a single interface shall use the name LXI.
Pre Condition	Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Check number of interfaces

Ensure the Device Specific Configuration has at least one interface available.

Test Procedure

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Ensure name attribute is available

Ensure the name attribute is available in the Device Specific Configuration

Ensure name attribute value is 'LXI'

If the device has a single interface, the name attribute value is 'LXI'. If multiple interfaces available, then the main LXI interface should be declared as 'LXI'.

23.13.1.2-1 Acceptance of IPv4

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Acceptance of IPv4

Explanation: LXI Devices shall accept IPv4Device. The element IPv4Device contains the device-specific configuration related to IPv4.

Test Procedure

Computed by other tests

This test is computed by the result of other tests.

Dependencies: 23.13-1

23.13.1.2-2 Absent IPv4

Category: LXI Security

Test Type: Kerberos Test, manual

Rule: Absent IPv4

Explanation: If IPv4Device is absent, and the LXI Common Configuration does not specify automatic configuration, the IPv4 capability is disabled.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Enable IPv6 via Common Configuration

Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)

Enable IPv6 DHCPEnabled attribute

Enable IPv6 DHCPEnabled attribute via Common Configuration.

Enable IPv6 RAEnabled attribute

Enable IPv6 RAEnabled attribute via Common Configuration.

Disable IPv6 staticAddressEnabled

Disable IPv6 staticAddressEnabled attribute via Common Configuration.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Enable IPv6 DHCP router

Enable IPv6 DHCP address assignment on the router.
Ensure the DUT has no RA address any more.
Ensure the DUT has a DHCP address.

Get DHCP IPv6 from mdns

Get the DHCP address only via mDNS.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

Setup IPv4 static address

Setup IPv4 static addressby putting the Device Specific Configuration to the DUT with a valid IPv4 static configuration.

PUT Device Specific Configuration

PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

Ensure IPv4 is enabled

Ensure IPv4 is enabled. This may be by enabling the stack on the webpage, via the frontpanel or via Common Configuraion.

Disable IPv4 DHCP and AutoIP via Common Configuration

Disable the DHCP and AutoIP attributes of the IPv4 element in the Common Configuration and put the Common Configuration to the DUT.

PUT Common Configuration

PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Remove IPv4 Device element

Remove IPv4 Device element from the Device Specific Configuration

PUT Device Specific Configuration

PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

Ping the DUT for failure

Ping the DUT via IPv4 which is expected to fail.

Check the mdns advertisement has stopped

Ensure the mdns advertisement has stopped, this means no _lxi._tcp services are available in the network anymore.

Post Condition	Reenable IPv4 stack
	Reenable IPv4 stack. If IPv6 is supported, this may be done automated via IPv6, otherwise an LCI is required.

23.13.1.2-3 Acceptance Of IPv6

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Acceptance Of IPv6
Explanation	LXI Devices shall accept IPv6Device. IPv6Device contains the device-specific configuration related to IPv6.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.1.2-4 Absent IPv6

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Absent IPv6
Explanation	If IPv6Device is absent, and the LXI Common Configuration does not specify any automatic configuration, the IPv6 capability is disabled.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Common Configuration
	GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.
	Enable IPv6 via Common Configuration
	Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported)
	Enable IPv6 DHCPEnabled attribute
	Enable IPv6 DHCPEnabled attribute via Common Configuration.
	Enable IPv6 RAEnabled attribute
	Enable IPv6 RAEnabled attribute via Common Configuration.
	Disable IPv6 staticAddressEnabled
	Disable IPv6 staticAddressEnabled attribute via Common Configuration.
	PUT Common Configuration
	PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.
	GET Device Specific Configuration
	GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

	Setup IPv6 static address Setup IPv6 static address by putting the Device Specific Configuration to the DUT with a valid IPv6 static configuration. PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response. Disable IPv6 DHCPEnabled and RAEnabled via Common Configuration Disable the IPv6 attributes DHCPEnabled and RAEnabled via the Common Configuration PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used. Get IPv6 from mdns Get all available IPv6 addresses via mDNS. It is possible for a device to have several IPv6 addresses, at a minimum the link-local address will be returned.
Test Procedure	Remove IPv6 Device element Remove the IPv6 Device element from the Device Specific Configuration. PUT Device Specific Configuration PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response. Ping the DUT via IPv6 for failure Ping the DUT via IPv6 using the gloabal IPv6 address and expect it to fail. Check the mdns advertisement has stopped Ensure the mdns advertisement has stopped, this means no _lxi._tcp services are available in the network anymore.
Post Condition	Enable IPv6 via Common Configuration Connect via IPv4 and enable IPv6 via the Common Configuration. (If IPv6 is supported) PUT Common Configuration PUT Common Configuration and expect a valid response from the DUT. A valid port is used, authorization is given and the correct URL is being used.

23.13.2.1-1 Attribute IPv4Device Address Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4Device Address Required
Explanation	Attribute address shall be implemented. The attribute address contains the IPv4 address of the device.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.2.1-2 Attribute IPv4Device SubnetMask Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4Device SubnetMask Required
Explanation	Attribute subnetMask shall be implemented. The attribute subnetMask contains the subnet mask to use.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.2.1-3 Attribute IPv4Device Gateway Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4Device Gateway Required
Explanation	Attribute gateway shall be implemented. The attribute gateway contains the gateway address.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.2.1-4 Attribute IPv4Device DNS1 Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4Device DNS1 Required
Explanation	Attribute dns1 shall be implemented. The attribute dns1 contains the address of the first DNS server.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.2.1-5 Attribute IPv4Device DNS2 Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv4Device DNS2 Required
Explanation	Attribute dns2 shall be implemented. The attribute dns2 dns2 is the address of the second (alternate) DNS server.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.2.1-6 IPv4Device Unrecognized Extensions

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv4Device Unrecognized Extensions
Explanation	LXI devices shall ignore extension attributes they do not recognize.

Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Device Specific Configuration
	GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.
Test Procedure	Add unknown attribute to IPv4 element
	Add an unknown attribute to IPv4 element in the Device Specific Configuration
	PUT Device Specific Configuration
	PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

23.13.3.1-1 IPv6Device Unrecognized Extensions

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6Device Unrecognized Extensions
Explanation	LXI devices shall ignore extension attributes they do not recognize.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
	GET Device Specific Configuration
	GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.
Test Procedure	Add unknown attribute to IPv6 element
	Add an unknown attribute to IPv6 element. Unknown attributes shall be ignored, if not recognized.
	PUT Device Specific Configuration
	PUT the valid Device Specific Configuration to the device via /lxi/api/device-specific-configuration using API-Key. Expect a valid response.

23.13.3.2-1 IPv6 StaticAddress

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 StaticAddress
Explanation	Devices shall accept at least one StaticAddress. Element StaticAddress is optional and contains the device static address
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.3.2-2 IPv6 LinkLocalAddress In Response

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 LinkLocalAddress In Response
Explanation	LXI Devices shall include the link local address in responses. Element LinkLocalAddress is a read-only field that contains the devices current link local address.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.3.2-3 IPv6 GlobalAddress In Response

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	IPv6 GlobalAddress In Response
Explanation	GlobalAddress element shall be included in the response for every device global address. Element GlobalAddress is a read-only element that contains the addresses provided to the device via router advertisement or DHCP.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.4.1-1 Attribute IPv6 Address Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv6 Address Required
Explanation	The address attribute shall be implemented. The attribute address contains the IPv6 address in CIDR notation.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.4.1-2 Attribute IPv6 Router Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute IPv6 Router Required
Explanation	The router attribute shall be implemented. The attribute router contains the router IPv6 address if this IPv6Address has an associated router. The address is in CIDR notation.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.13.4.1-3 Attribute IPv6 DNS Required

Category	LXI Security
Test Type	Kerberos Test, automated

Rule	Attribute IPv6 DNS Required
Explanation	The dns attribute shall be implemented. The attribute dns contains the address of the IPv6 domain name server if this IPv6Address has an associated dns. The address is in CIDR notation.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.13-1

23.14.1.1-1 Attribute LXICertificateRef GUID Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute LXICertificateRef GUID Required
Explanation	The GUID attribute shall be implemented. The GUID identifies the certificate, certificate list, or CSR. The GUID is returned by the Certificate List API.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.10.13 23.10.17

23.15.2.1-1 Attribute CertificateInfo GUID Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute CertificateInfo GUID Required
Explanation	The GUID attribute shall be implemented. GUID is a Globally Unique Identifier generated by the device to represent this certificate.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.10.12

23.15.2.1-2 Attribute CertificateInfo Type Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute CertificateInfo Type Required
Explanation	The Type attribute shall be implemented. Type indicates the kind of entity.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Remove all LDevID and CSR certificates Iterate over the certificates list and delete all certificates which match the types LDevID and CSR from the dut, using the DELETE /lxi/api/certificates/<GUID> API.

Create self-signed certificate

Request the DUT to create a self-signed certificate via API. The created self-signed certificate is used as an LDevID for the device.

Get CSR

Get CSR certificate via the /lxi/api/get-csr API.

Test Procedure

Get certificates

Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS

Check certificate Infos values for each type

Check the Certificate Information values match for the given type.

Identify IDevID, LDevID and CSR

Expect 3 Certificate Infos, one for IDevID, LDevID and CSR. Through the previous steps it ensures that exactly three certificate informations is available. One for each type.

Verify the expiration date attribute for LDevID/CSR certificate

Verify the expiration date attribute for LDevID/CSR certificate in the certificate list received from the DUT.

Verify the Enabled attribute for LDevID/CSR certificate

Verify the Enabled attribute for LDevID/CSR certificate in the certificates list received from the DUT.

23.15.2.1-3 Attribute CertificateInfo DNSName Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute CertificateInfo DNSName Required

Explanation: The DNSName attribute shall be implemented. DNSName is the DNS Name from the certificate.

Test Procedure: Computed by other tests

This test is computed by the result of other tests.

Dependencies: 23.15.2.1-2

23.15.2.1-4 Attribute CertificateInfo Enabled Required

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: Attribute CertificateInfo Enabled Required

Explanation: The Enabled attribute shall be implemented. DNSName is the DNS Name from the certificate. Enabled indicates if the corresponding certificate or certificate chain is enabled for use by the device. Enabled is meaningless for Certificate Signing Requests. Enabled shall be returned true for CSRs.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure	Create self-signed certificate Request the DUT to create a self-signed certificate via API. The created self-signed certificate is used as an LDevID for the device. Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Get certificate Info matching GUID Check the certificate list contains the required GUID and get the certificate Info from the list. Expect enabled attribute is true Check the enabled attribute for the certificate is set to true and therefore enabled. Get active certificate Get the currently used certificate (LDevID) for MTLS authentication and for the webpage. Disable certificate Disable the certificate via the API /lxi/api/certificates/<GUID>/enabled using the apropriate GUID and the boolean value false. Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Get certificate Info matching GUID Check the certificate list contains the required GUID and get the certificate Info from the list. Expect enabled attribute is false Check the enabled attribute for the certificate is set to false and therefore disabled. Enable certificate Enable the certificate via the API /lxi/api/certificates/<GUID>/enabled and the apropriate GUID and the boolean value true. Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Get certificate Info matching GUID Check the certificate list contains the required GUID and get the certificate Info from the list. Expect enabled attribute is true Check the enabled attribute for the certificate is set to true and therefore enabled.

23.15.2.1-5 CertificateInfo Expiration Of Date And Time

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	CertificateInfo Expiration Of Date And Time
Explanation	The expiration date and time shall be expressed in ASN.1 format using ASN.1 GeneralizedTime per RFC5280.

Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Create certificate via certificate-request with ASN.1 GerneralizedTime before 2050
	Get a certificate via a certificate-request with ASN.1 GerneralizedTime before 2050. Expect a valid response.
	Create certificate via certificate-request with ASN.1 GerneralizedTime after 2050
	Get a certificate via a certificate-request with ASN.1 GerneralizedTime after 2050. Expect a valid response.
	Get certificates
	Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS
	Get certificate Info matching GUID
	Check the certificate list contains the required GUID and get the certificate Info from the list.
	Validate expirationDateTime
	Validate the expirationDateTime for ASN.1 GeneralizedTime, and check it matches the known time.

23.15.2.1-6 Attribute CertificateInfo ExpirationDateTime Required

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Attribute CertificateInfo ExpirationDateTime Required
Explanation	The expirationDateTime attribute shall be implemented. The attribute expirationDateTime contains the expiration date and time of the certificate. For a CSR, expirationDateTime shall contain the requested expiration time from the CSR. If the CSR LXICertificateRequest/ ExpirationDateTime was absent an empty string shall be returned.
Test Procedure	Computed by other tests
	This test is computed by the result of other tests.

Dependencies		
	23.15.2.1-2	23.15.2.1-5

23.16.1.1-1 LXICertificateRequest Expiration Of Date And Time

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXICertificateRequest Expiration Of Date And Time
Explanation	The expiration date and time shall be expressed in ASN.1 format using ASN.1 GeneralizedTime per RFC5280.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address

Test Procedure	Get CSR via certificate-request with ASN.1 GerneralizedTime before 2050
	Get a csr via a certificate-request with ASN.1 GerneralizedTime before 2050. Expect a valid response.
	Get CSR via certificate-request with ASN.1 GerneralizedTime after 2050
	Get a csr via a certificate-request with ASN.1 GerneralizedTime after 2050. Expect a valid response.
	Get CSR via certificate-request with incorrect date and time format, expect failure
	Get a CSR via a certificate-request with an incorrect date and time format. Expect an error as response.
	Create certificate via certificate-request with ASN.1 GerneralizedTime before 2050
	Get a certificate via a certificate-request with ASN.1 GerneralizedTime before 2050. Expect a valid response.
	Create certificate via certificate-request with ASN.1 GerneralizedTime after 2050
	Get a certificate via a certificate-request with ASN.1 GerneralizedTime after 2050. Expect a valid response.
	Create certificate via certificate-request with incorrect date and time format, expect failure
	Create a certificate via a certificate-request with an incorrect date and time format. This will end in an error response due to incorrect date and format.

23.16.1.1-2 LXICertificateRequest SignatureAlgorithm Unsupported

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXICertificateRequest SignatureAlgorithm Unsupported
Explanation	If the device does not support the requested crypto suite, then the certificate request shall fail. The element SignatureAlgorithm specifies the cryptography suite that the certificate key set should use.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Create simple certificate requests with unsupported SignatureAlgorithm
	Create a certificate request xml with simple values and an unsupported SignatureAlgorithm.
	GET CSR with unsupported SignatureAlgorithm
	Get a CSR via a certificate-request with an unsupported signature algorithm. Expect an error as response.
	Create self-signed certificate, expect failure
	Create a self signed certificate via a certificate-request with an incorrect SignatureAlgorithm format. Expect an error as response.

23.16.2-1 Default Field Subjectname

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	Default Field Subjectname

Explanation	The default fields for the subject name shall be the values used in the device IDevID. SubjectName contains the various attributes of the requested certificate subject.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network Get IP from mdns Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Get certificates Get the certificates list from device via API /lxi/api/certificates using API-Key, to extract all GUIDS Get IDevID Certificate from the device Get the IDevID Certificate from the device via API. Use the identified GUID from the certificate list to receive the correct certificate. Validate 'IDevId' certificate Validate 'IDevId' certificate. Ensure the given certificate is a valid certificate and that requried attributes are available. Get CSR Get CSR certificate via the /lxi/api/get-csr API. Validate CSR attributes Validate CSR attributes agains the expected and configured values in the CSR request. Validate CSR Attributes against IDevID attributes Validate the attribute values in the received CSR against the IDevID attribute values. Create self-signed certificate Request the DUT to create a self-signed certificate via API. The created self-signed certificate is used as an LDevID for the device. Get LDevID Certificate from the device Get an LDevID Certificate from the device using the API. Validate LDevID certificate Validate the LDevID certificate attributes against te expected and configured vlaues from the certificate request. Validate LDevID Attributes against IDevID attributes Validate the LDevID Attributes against the DUT's IDevID attributes.

23.16.3.1-1 ExtraSubjectAttribute ObjectID

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	ExtraSubjectAttribute ObjectID
Explanation	ObjectID shall be included. ObjectID is the object ID that indicates the subject attribute as specified by the OpenGroup.
Pre Condition	Enable IPv4 DHCP router Enable the dhcp router for IPv4 Connect DUT Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Create simple certificate requests with ExtraSubjectAttribute 'ObjectID'

Create simple certificate requests with ExtraSubjectAttribute 'ObjectID'. One request with a valid ObejctID and an empty ObjectID value.

GET CSR with ObjectID

GET a CSR with ObjectID from the DUT and expect a success response with a valid CSR.

Create self-signed certificate with ObjectID

Request the DUT to create a self-signed certificate with ObjectID and expect a valid self-signed certificate.

Create simple certificate requests without ObjectID

Create simple certificate requests without ObjectID to send to the DUT.

GET CSR without ObjectID and expect failure response

GET a CSR without ObjectID from the DUT and expect a failure response

Create self-signed certificate without ObjectID and expect failure response

Request the DUT to create a self-signed certificate without ObjectID and expect a failure response

23.16.3.1-2 ExtraSubjectAttribute ObjectValue

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: ExtraSubjectAttribute ObjectValue

Explanation: ObjectValue shall be included. ObjectValue is the subject value associated with the specified attribute.

Pre Condition

Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Create simple certificate requests with ExtraSubjectAttribute 'ObjectValue'

Create simple certificate requests with ExtraSubjectAttribute 'ObjectValue' to send to the DUT.

GET CSR with ObjectValue

GET a CSR with ObjectValue and expect success response with a valid CSR.

Create self-signed certificate with ObjectValue

Request the DUT to create a self-signed certificate with ObjectValue and expect a valid self-signed certificate.

Create simple certificate requests without ObjectValue

Create simple certificate requests without ObjectValue to send to the DUT.

GET CSR without ObjectValue and expect failure response

GET a CSR without ObjectValue from the DUT and expect the request to fail.

Create self-signed certificate without ObjectValue and expect failure response

Request the DUT to create a self-signed certificate without ObjectValue and expect a failure response

23.16.4.1-1 CertificateExtension ObjectID

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	CertificateExtension ObjectID
Explanation	ObjectID shall be included. ObjectID is the object ID that indicates the certificate extension as specified by the OpenGroup.
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address
Test Procedure	Create simple certificate requests with CertificateExtension 'ObjectID'
	Create simple certificate requests with CertificateExtension 'ObjectID'. One request with a valid ObejctID and an empty ObjectID value.
	GET CSR with ObjectID
	GET a CSR with ObjectID from the DUT and expect a success response with a valid CSR.
	Create self-signed certificate with ObjectID
	Request the DUT to create a self-signed certificate with ObjectID and expect a valid self-signed certificate.
	Create simple certificate requests without ObjectID
	Create simple certificate requests without ObjectID to send to the DUT.
	GET CSR without ObjectID and expect failure response
	GET a CSR without ObjectID from the DUT and expect a failure response
	Create self-signed certificate without ObjectID and expect failure response
	Request the DUT to create a self-signed certificate without ObjectID and expect a failure response

23.16.4.1-2 CertificateExtension ObjectValue

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	CertificateExtension ObjectValue
Explanation	ObjectValue shall be included. ObjectValue is the subject value associated with the certificate field
Pre Condition	Enable IPv4 DHCP router
	Enable the dhcp router for IPv4
	Connect DUT
	Connect the DUT to the test network
	Get IP from mdns
	Search via mdns for a single lxi service and retrieve its IP address

Test Procedure

Create simple certificate requests with CertifcateExtension 'ObjectValue'

Create simple certificate requests with CertifcateExtension 'ObjectValue' to send to the DUT.

GET CSR with ObjectValue

GET a CSR with ObjectValue and expect success response with a valid CSR.

Create self-signed certificate with ObjectValue

Request the DUT to create a self-signed certificate with ObjectValue and expect a valid self-signed certificate.

Create simple certificate requests without ObjectValue

Create simple certificate requests without ObjectValue to send to the DUT.

GET CSR without ObjectValue and expect failure response

GET a CSR without ObjectValue from the DUT and expect the request to fail.

Create self-signed certificate without ObjectValue and expect failure response

Request the DUT to create a self-signed certificate without ObjectValue and expect a failure response

23.18-1 LXI Problem Details Schema 40X errors

Category: LXI Security

Test Type: Kerberos Test, automated

Rule: LXI Problem Details Schema 40X errors

Explanation: Devices shall return the LXIProblemDetails when the LXI API generates 40X errors.

Pre Condition: Enable IPv4 DHCP router

Enable the dhcp router for IPv4

Connect DUT

Connect the DUT to the test network

Get IP from mdns

Search via mdns for a single lxi service and retrieve its IP address

Test Procedure: GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

POST Common Configuration

POST common configuration instead of PUT. This call is expected to fail due to invalid endpoint.

Validate Xml against local schema

Validate the response Xml against the appropriate local schema.

Check Problem Details title

Check the title of the problem details.

GET Device Specific Configuration

GET the Device Specific Configuration from device via API /lxi/api/device-specific-configuration using API-Key.

PUT Common Configuration with incorrect xml

PUT the Common Configuration with an incorrect xml (e.g. use Xml for Device specific Configuration) and expect the PUT to fail.

Validate Xml against local schema

Validate the response Xml against the appropriate local schema.

Check Problem Details title

Check the title of the problem details.

GET Common Configuration

GET the Common Configuration from the device. Expect the call to succeed. Authentication is given, the correct URL is being used and the device is setup correctly.

Modify Common Configuration for syntax error

Modify the Common Configuration xml received from the DUT in a way to ge a syntax error.

PUT Common Configuration with incorrect syntax

PUT the Common Configuration xml with incorrect syntax and expect failure response due to incorrect syntax.

Validate Xml against local schema

Validate the response Xml against the appropriate local schema.

Check Problem Details title

Check the title of the problem details.

23.18.1.1-1 LXIProblemDetailsElement Title

Category	LXI Security
Test Type	Kerberos Test, automated
Rule	LXIProblemDetailsElement Title
Explanation	Title shall be included. Title is a high level description of the method result, consistent with the HTTP status code returned.
Test Procedure	Computed by other tests This test is computed by the result of other tests.
Dependencies	23.18-1

23.19-1 LXI Pending Details Schema Schema-valid XML Responses

Category	LXI Security
Test Type	Vendor Declaration
Rule	LXI Pending Details Schema Schema-valid XML Responses
Explanation	Schema-valid XML responses, as defined by this schema, shall be returned by devices to indicate pending operations.

23.19.1.1-1 LXIPendingDetails URL

Category	LXI Security
Test Type	Vendor Declaration
Rule	LXIPendingDetails URL
Explanation	URL shall be included. URL provides a URL at which the client can perform a GET to determine the status of the pending operation.