IPv6 Test Service

IPv6 Cloud Platform
Functional Test Plan
Phase 1

Technical Document

Version 0.2

University of New Hampshire
InterOperability Laboratory
IPv6 Test Service
https://www.iol.unh.edu

21 Madbury Road, Suite 100
Durham, NH 03824
Phone: +1-603-862-0090
Fax: +1-603-862-4181

Table of Contents

Acknowledgements

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite:

Ben Patton	University of New Hampshire
Ben Herr	University of New Hampshire
Kyle Ouellette	University of New Hampshire
Michayla Newcombe	University of New Hampshire

References

The following documents are referenced in this text:

[NIST IPv6 Profile] "NIST IPv6 Profile", NIST Special Publication (NIST SP) - 500-267Ar1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Ar1

[USGv6-R1] "USGv6 Profile", NIST Special Publication (NIST SP) - 500-267Br1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Br1

[NIST Cloud] "The NIST Definition of Cloud Computing ", NIST Special Publication (NIST SP) - 800-145, September 2011. https://doi.org/10.6028/NIST.SP.800-145

[RFC 5952] A Recommendation for IPv6 Address Text Representation. S. Kawamura, M. Kawashima. August 2010.

Introduction

The University of New Hampshire's InterOperability Laboratory (UNH-IOL) is an institution designed to improve the interoperability of standards-based products by providing an environment where a product can be tested against other implementations of a standard. This test suite evaluates whether a cloud-based product is fully functional in an IPv6-only environment.

Scope:

The following tests verify the general functionality of a product in an IPv6-only cloud network.

The NIST IPv6 Profile (500-267Ar1) defines an **IPv6-Only** product as capable of operating "in environments with no IPv4 capabilities (e.g., either IPv4 is not implemented or is administratively disabled or IPv4 is not provided on the network)." Some products do not allow IPv4 to be administratively disabled and may automatically provision IPv4 addresses for themselves; in such cases, those IPv4 addresses must not be routable outside of the product's immediate network."

The IPv6-Only capability applies to a product as a whole in its primary role. Additional Application level testing may be warranted for products that serve as a platform to run one or more additional applications or services.

This Test Specification exercises a product to ensure support for the following functions: Installation, Upgrade/Update, Configuration, Management, and Instrumentation.

Phase 1:

This Test Specification is intended as an initial approach ("**Phase 1**") to testing Infrastructure-as-a-Service (IaaS) systems and computing resources when deployed in an IPv6-only cloud network. Reliance on cloud-based services offered by major cloud providers has increased significantly in recent years. Continued testing of these products where applicable for IPv6-only support will be critical to the smooth adoption and transition of IPv6 in next-generation networking technology. As the adoption of IPv6 within cloud providers grows, testing efforts will likely expand as part of a Phase 2 approach to include Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) applications across different cloud providers. This document uses definitions for those cloud service models as described in [NIST Cloud].

Test Organization

This document organizes tests in groups based on related test methodology or goals. Each group begins with a brief set of comments about all tests within that group. This is followed by a series of description blocks; each block describes a single test. The format of the description block is as follows:

Test Label	The **Test Label** is the first line of the test page. It will have the following form: IPv6-Cloud.A.B Where each component indicates the following: Cloud – Test Suite Identifier A – Group Number B – Test Number Scripts implementing this test suite should follow this convention and may also append a character in the set [a-z] indicating a particular test part.
Purpose	The **Purpose** is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.
Applicable Product Types	The **Applicable Product Types** section describes the functional roles applicable to each test case. Functional roles and their definitions are provided in [NIST IPv6 Profile].
Test Setup	The **Test Setup** section describes the configuration of all devices before the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used for that parameter.
Test Evidence Collected	The **Test Evidence Collected** section describes what must be collected for observations as results for a given test case. This will typically include screenshots or logs of passing or failing behavior, commands executed on the SUT or interop partners, or other written observations.
Procedure and Expected Behavior	The **Procedure and Expected Behavior** table contains step-by-step instructions for carrying out the test. These steps include actions such as enabling interfaces, unplugging devices from the network, or sending packets from a test station. The test procedure also cues the tester to make observations of expected behavior, as needed, as not all steps require observation of results. If any behavior is expected for a procedure, it is to be observed before continuing to the next step. Failure to observe any behavior before continuing constitutes a failed test. Note, that while test numbers continue between test parts, each test part is to be executed independently (Following Common Test Setup and Cleanup as indicated), and are not cascaded from the previous part.
Possible Problems	The **Possible Problems** section contains a description of potential exceptions for steps in a given test procedure due to product limitations, which may affect test results in certain situations.

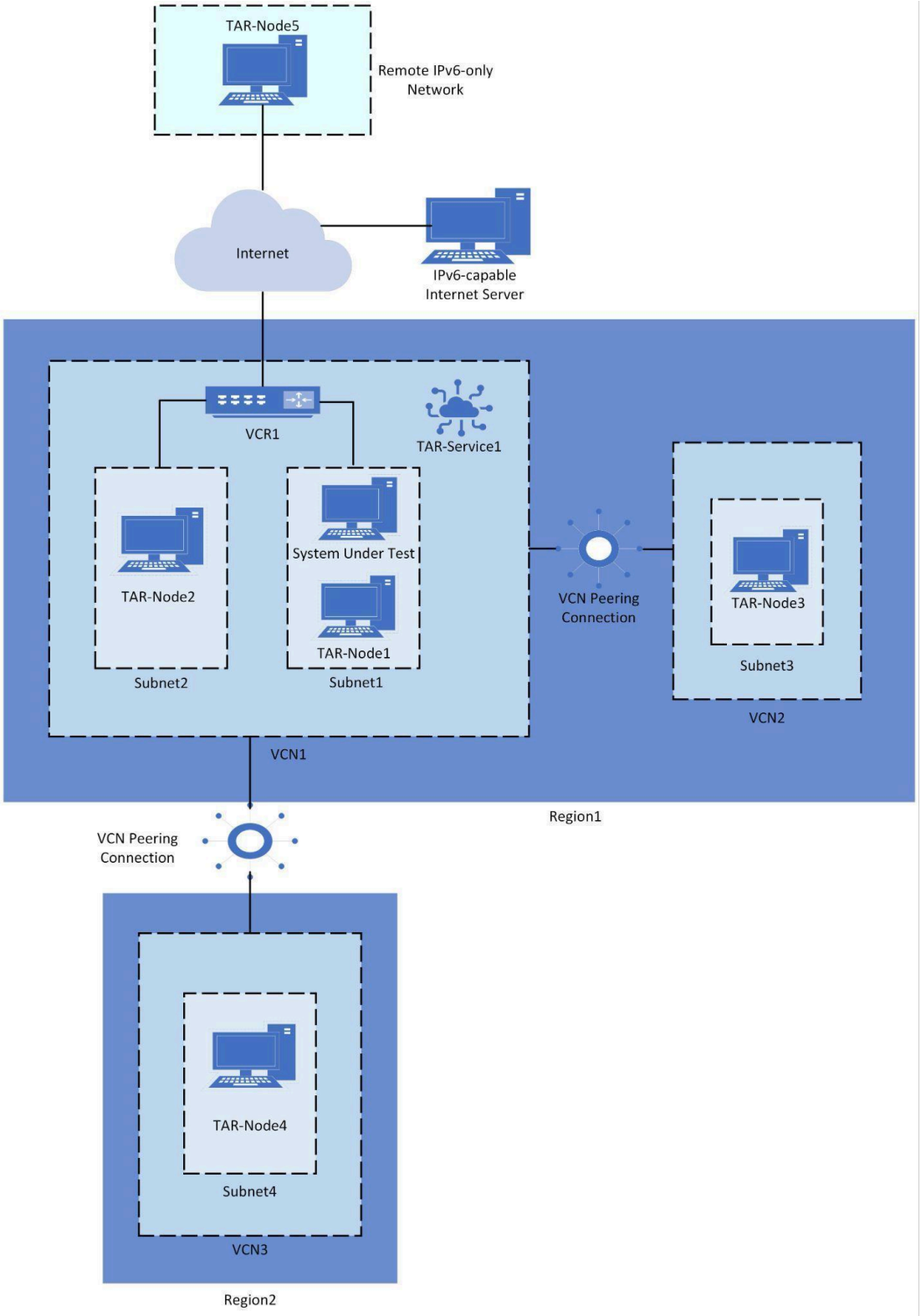
Definitions and Terminology

This section serves to provide clarity and definitions for terms used throughout this document, and to reconcile services available on various public cloud providers that perform the same functions.

Cloud Provider	A company or provider that offers publicly available cloud computing/networking/development resources. Examples of common Cloud Providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
Remote IPv6-only Network	A network hosted outside the target Cloud Provider used for testing. This network has internet connectivity, and can reach resources hosted by the Cloud Provider. In a normal network architecture, this would be an "on-premises" network.
Virtual Cloud Network (VCN)	User-defined, virtual "networks" that allow cloud network engineers to logically isolate resources (such as Virtual Compute Instances) in their cloud infrastructure. A VCN typically comprises one or more individual subnets and routing instances. Examples of this across common Cloud Providers include Virtual Private Clouds (VPCs) in AWS and GCP, and Virtual Networks in Azure.
Subnet	An individual subsection of the VCN where compute resources are deployed. These will typically be assigned a unique 64-bit IPv6 prefix.
Region	A physical/geographical location around the world where Cloud Providers build the data center clusters that support cloud offerings, to allow for highly available service. From a networking standpoint, an individual region can contain one or more VCNs.
Peering Service	A cloud service or resource that allows VCNs to share or "peer" routing information directly. In cloud network architectures, this is a common method for connecting networks owned by the same enterprise or similar teams/business units within an enterprise.
Virtual Compute Instance (VCI)	Virtual compute resources that also include storage and node-level networking capabilities. These are typically virtual machines that run their own Operating System, user-level services, and have their own IPv6 "stack".
Virtual Cloud Router (VCR)	Virtual resource (either provided by a Virtual Compute Instance or by a separate cloud service) that routes traffic between VCI's in the same network or between different networks.

System Under Test (SUT)	The product being targeted and observed by this test suite. This may be composed of one or more compute resources or interconnected services.

Common Topology



Common Test Setup

The following procedure is used for creating the Common Topology as shown above. To simplify resource creation and cleanup, resources may be provisioned once at the beginning of test suite execution and left deployed until testing is completed, or they may be provisioned as needed for appropriate tests.

1. VCNs 1, 2, and 3 are created in Regions 1 and 2 according to the table below. Subnets are created in VCNs according to the table below and allocated IPv6 prefixes with the specified length. VCN1 must be allocated an IPv6 prefix large enough for two /64 subnets.

Subnet	Region	VCN	Prefix length	Compute
Subnet1	1	1	64	TAR-Node1
Subnet2	1	1	64	TAR-Node2
Subnet3	1	2	64	TAR-Node3
Subnet4	2	3	64	TAR-Node4

2. VCR1 is created in VCN1 to route traffic from VCN1 to the Internet.
3. VCN peering connections are established between VCN1 and VCN2, and between VCN1 and VCN3.
4. Virtual Compute Instances are created per the table below. A web server application is installed and initialized on each Virtual Compute Instance.
5. Access Control Lists are configured on all Virtual Compute Instances to allow inbound and outbound connections per the table below.

Protocol	Inbound or Outbound	Source Network
SSH	Inbound	Remote IPv6-only Network
HTTP	Inbound	Remote IPv6-only Network
ICMPv6	Inbound	Remote IPv6-only Network
Any	Outbound	Subnet1, Subnet2, Subnet 3, Subnet4
Any	Inbound	Subnet1, Subnet2, Subnet3, Subnet4

6. TAR-Node5 is initialized in the Remote IPv6-only Network.

Node and Network Requirements

The following constraints are placed on the Common Topology and resources provisioned within:

1. The primary VCN where the SUT is located (VCN1) MUST NOT be provisioned with any IPv4 services (e.g. DHCP).
2. IPv4 Capabilities MUST NOT be configured on devices located in VCN1, and may be administratively disabled.
    a. If IPv4 cannot be administratively disabled, then any automatically provisioned IPv4 addresses MUST NOT be routable outside VCN1.
3. The Remote IPv6-only Network where TAR-Node5 is located MUST NOT be provisioned with any IPv4 services (e.g. DHCP).
4. Virtual Compute Instances used for testing MUST support the installation of a Web Server (e.g. nginx or apache2).
5. IPv4 Capabilities MUST NOT be configured on any devices used for testing and may be administratively disabled.
6. TAR-Node1 MUST support the installation of a service to consume and collect log messages generated by the SUT (e.g. rsyslog or syslog-ng).
7. TAR-Service1 MUST be a IaaS, PaaS, or SaaS service offered by the Cloud Provider which is not the same IaaS service used for provisioning the SUT.

Section 1: Lifecycle Functionality

Overview

The product must support full product lifecycle functions (defined below) in an IPv6-only context and as applicable for a cloud-based product. Note that the product support functions below are commonly provided by additional applications or functions distinct from the main function of the product (e.g., installer applications, update applications, management applications for an OS).
[NIST IPv6 Profile], Section 4.1.1

IPv6-Cloud.1.1: Installation

Purpose: The product must be able to be instantiated and installed in network environments that do not provide IPv4 services. Initial configuration of the product to a state where other remote services are operational are part of the installation functions. [NIST IPv6 Profile], Section 4.1.1. Cloud-based products often rely on IaaS management services for instance deployment.

Applicable Product Types:

- Host, Router, NPP, Application

Test Setup: VCN1, Subnet1, and VCR1 are set up per the Common Topology. The SUT is not deployed as part of the test setup.

Test Evidence Collected: Collect applicable evidence as described below.

- Description of process and any User Intervention needed for network
- Installation URL, Commands, etc.
- Description of the use, input, or display, of IPv6 addresses.
- Screenshots as needed

Procedure:

Step	Action	Expected Observation
1.	Initiate installation or deployment function from TAR-Node5. The SUT must be deployed in Subnet1.	Installation or deployment starts successfully.
2.	Monitor Installation progress.	Installation completes successfully and according to supplier description.
3.	Perform initial configuration of the system to a state where other remote services are operational.	Any use of the network must function without error and any input or display of IPv6 Addresses must follow RFC 5952.

Possible Problems:

- None

IPv6-Cloud.1.2: Update

Purpose: All forms of product update functions (e.g., software, OS updates), both automated and user initiated, must be fully functional in IPv6-only environments.
[NIST IPv6 Profile], Section 4.1.1.

Applicable Product Types:

- Host, Router, NPP, Application

Test Setup: VCN1, Subnet1, VCR1, and the SUT are set up per the Common Topology.

Test Evidence Collected: Collect applicable evidence as described below.

- Update URL, Commands, etc.
- Description of the use, input, or display, of IPv6 addresses.
- Screenshots as needed.

Procedure:

Step	Action	Expected Observation
1.	**Copy/transfer update media (software, installers, etc.) to the SUT.**	**Media copied successfully.**
2.	Initiate update.	Update starts successfully.
3.	Monitor update progress.	Update completes successfully and according to supplier description. Any use of the network must function without error and any input or display of IPv6 addresses must follow RFC 5952.

Possible Problems:

- If the SUT does not support a method for performing updates, this test case may be omitted.
- If the SUT does not require update media to be copied to the system before the update can be initiated, step 1 may be omitted.

IPv6-Cloud.1.3: User Interface

Purpose: All forms of interactive access to the product (e.g., web-based interfaces or APIs) must fully support the use of IPv6 and IPv6 addresses of all forms. If the product displays IP addresses, then IPv6 addresses must be displayed according to [RFC5952]. [NIST IPv6 Profile], Section 4.1.1.

Applicable Product Types:

- Host, Router, NPP, Application

Test Setup: VCN1, Subnet1, VCR1, and the SUT are set up per the Common Topology.

Test Evidence Collected: Collect applicable evidence as described below.

- Description of the use, input, or display, of IPv6 addresses.
- If available, a GUI and API/CLI user interface MUST be tested.
- Screenshots as needed.

Procedure:

Part A: IPv6 Address Display

Step	Action	Expected Observation
1.	Navigate to a function on the SUT for displaying its assigned IPv6 addresses.	
2.	Observe existing link-local IPv6 address(es) on the SUT.	The observed address is displayed in a text format per RFC 5952, section 4.
3.	Observe existing global IPv6 address(es) on the SUT.	The observed address is displayed in a text format per RFC 5952, section 4.
4.	Manually configure an IPv6 address on the SUT that contains leading zeros in a 16-bit field: `2001:0db8::0001`	
5.	Navigate to a function on the SUT for displaying the address configured in step 4.	The SUT displays the address configured in step 4 with leading zeros suppressed: `2001:db8::1`
6.	Manually configure an IPv6 address on the SUT that contains consecutive groups of 16-bit zero fields: `2001:db8:0:0:0:0:2:1`	
7.	Navigate to a function on the SUT for displaying the address configured in step 6.	The SUT displays the address configured in step 6 with multiple groups of leading zeros abbreviated to "::": `2001:db8::2:1`
8.	Manually configure an IPv6 address on the SUT that contains a single 16-bit zero field:	

	`2001:db8:0:1:1:1:1:1`	
9.	Navigate to a function on the SUT for displaying the address configured in step 8.	The SUT does not display the address configured in step 8 with the single 16-bit zero field suppressed with "::": `2001:db8:0:1:1:1:1:1`
10.	Manually configure an IPv6 address on the SUT that contains two sets of consecutive groups of 16-bit zero fields, one longer than the other: `2001:0:0:1:0:0:0:1`	
11.	Navigate to a function on the SUT for displaying the address configured in step 10.	The SUT displays the address configured in step 10 with the longer group of consecutive zeros suppressed with "::": `2001:0:0:1::1`
12.	Manually configure an IPv6 address on the SUT that contains two sets of consecutive groups of 16-bit zero fields, where both are equal length: `2001:db8:0:0:1:0:0:1`	
13.	Navigate to a function on the SUT for displaying the address configured in step 12.	The SUT displays the address configured in step 12 with the first group of consecutive zeros suppressed with "::": `2001:db8::1:0:0:1`
14.	Manually configure an IPv6 address on the SUT that contains characters A-F in uppercase: `2001:DB8:A:B:C:D:E:F`	
15.	Navigate to a function on the SUT for displaying the address configured in step 14.	The SUT displays the address configured in step 14 with characters A-F in lowercase: `2001:db8:a:b:c:d:e:f`

Part B: IPv6 Address Input

Step	Action	Expected Observation
16.	Navigate to a command line interface on the SUT containing a function that accepts IPv6 addresses as input (e.g. ping diagnostic utility).	
17.	Enter an invalid link-local IPv6 address that is too long: `FE80:0:0:0::1:2:3:4:5:6`	Observe that the address is not accepted.
18.	Enter an invalid link-local IPv6 address that contains invalid characters: `FE80::AB:CD:EF:GH`	Observe that the address is not accepted.
19.	Enter an invalid link-local IPv6 address with more "::" than are allowed per RFC 5952: `FE80::1000::2000`	Observe that the address is not accepted.
20.	Enter an invalid global IPv6 address that is too long: `2001:2:0:1:2:3:4:5:6`	Observe that the address is not accepted.

21.	Enter an invalid global IPv6 address that contains invalid characters: `2001:2:0:AB:CD:EF:G:H`	Observe that the address is not accepted.
22.	Enter an invalid global IPv6 address with more "::" than are allowed per RFC 5952: `2001:2::1000::1000`	Observe that the address is not accepted.
23.	Enter a valid link-local IPv6 address assigned to a different device within the same Subnet as the SUT.	Observe that the function accepts the address, and the operation completes successfully.
24.	Enter a valid global IPv6 address assigned to the IPv6-capable Internet Server.	Observe that the function accepts the address, and the operation completes successfully.
25.	Enter a valid FQDN that has a AAAA (IPv6) record assigned to the IPv6-capable Internet Server.	Observe that the function accepts the address, and the operation completes successfully.
26.	Navigate to a graphical user interface on the SUT.	
27.	Repeat steps 17-22 with the selected interface.	Observe that the function accepts valid addresses and does not accept invalid addresses as described in steps 17-22.
28.	Use an appropriate API endpoint exposed by the SUT that accepts IPv6 addresses as input.	
29.	Repeat steps 17-22 with the selected API endpoint.	Observe that the function accepts valid addresses and does not accept invalid addresses as described in steps 17-22.

Possible Problems:

- If the SUT does not have a function for displaying its assigned link-local addresses, then step 2 may be omitted.
- If the SUT does not have a function for displaying its assigned global addresses, then step 3 may be omitted.
- If the SUT does not support a method for manually configuring IPv6 addresses, then steps 4-15 may be omitted.
- If the SUT does not support a CLI-accessible user interface that accepts IPv6 addresses as input, steps 16-22 may be omitted.
- If the SUT does not support a GUI-accessible user interface that accepts IPv6 addresses as input, steps 26 and 27 may be omitted.
- If the SUT does not support an API endpoint that accepts IPv6 addresses as input, steps 28 and 29 may be omitted.

IPv6-Cloud.1.4: Logging

Purpose: All forms of interactive access to the product (e.g., web-based interfaces or APIs) must fully support the use of IPv6 and IPv6 addresses of all forms. If the product displays IP addresses, then IPv6 addresses must be displayed according to [RFC5952]. [NIST IPv6 Profile], Section 4.1.1.
Representation of IPv6 Literals in Logs according to [RFC5952] is of particular importance to enable searching and efficient user review.

Applicable Product Types:

- Host, Router, NPP, Application

Test Setup: VCN1, Subnet1, TAR-Node1, VCR1, and the SUT are set up per the Common Topology. A remote logging service is initialized on TAR-Node1 in Subnet1.

Test Evidence Collected: Collect applicable evidence as described below.

- Description of the logging function used.
- Log locations, commands used, etc.
- Description of the use, input, or display of IPv6 addresses where applicable.
- Screenshots as needed.

Procedure:

Part A: Local Logging

Step	Action	Expected Observation
1.	Navigate to a mechanism for viewing logs locally on the SUT, or where IPv6 addresses are logged.	
2.	Observe link-local IPv6 addresses in log messages.	Addresses observed are in a text format per RFC 5952, section 4.
3.	Observe global IPv6 addresses in log messages.	Addresses observed are in a text format per RFC 5952, section 4.

Part B: Remote Logging

Step	Action	Expected Observation
4.	Configure the SUT to send log messages to a TAR-Node1. The destination address used for TAR-Node1 must be a valid global IPv6 address or an FQDN with a AAAA (IPv6) record that resolves to a valid global IPv6 address.	Observe that the SUT is successfully configured to transmit logs to the requested remote logging server. Observe that TAR-Node1 successfully collects log messages from the SUT.

5.	Observe link-local IPv6 addresses in the logs collected by the remote logging server.	Link-local addresses displayed in remote logs from the SUT are properly formatted per RFC 5952 section 4.
6.	Observe global IPv6 addresses in the logs collected by the remote logging server.	Global addresses displayed in remote logs from the SUT are properly formatted per RFC 5952 section 4.

Possible Problems:

- If the product does not support a method for collecting or viewing local logs, then part A may be omitted.
- If the product does not support a method for sending logs to a remote IP-enabled server, then part B may be omitted.
- If log messages displayed by the product do not contain link-local IPv6 addresses, then steps 2 and 5 may be omitted.
- If log messages displayed by the product do not contain global IPv6 addresses, then steps 3 and 6 may be omitted.

Section 2: Management and Connectivity

Overview

The product must support full product lifecycle functions (defined below) in an IPv6-only context. Note that the product support functions below are commonly provided by additional applications or functions distinct from the main function of the product (e.g., installer applications, update applications, management applications for an OS)
[NIST IPv6 Profile], Section 4.1.1.

All forms of interactive access to the product (e.g., web-based interfaces or APIs) must fully support the use of IPv6 and IPv6 addresses of all forms.
[NIST IPv6 Profile], Section 4.1.1.

All forms of remote management and monitoring functions must be fully functional in IPv6-only environments.
[NIST IPv6 Profile], Section 4.1.1.

Cloud-based products are often interconnected using a variety of different architectures and may also depend on a variety of cloud-based services for management and monitoring, logging, or other network operations. This section aims to test basic network and application connectivity with cloud-based products deployed in some of these architectures using common cloud networking paradigms.

For network-level connectivity tests, ICMPv6 Echo (ping) diagnostics are used by default. For application-level connectivity tests, HTTP requests are used by default.

IPv6-Cloud.2.1: Network and Application Connectivity

Purpose: All forms of remote management and monitoring functions must be fully functional in IPv6-only environments. [NIST IPv6 Profile], Section 4.1.1.

Applicable Product Types:
- Host, Router, NPP

Test Setup: The Common Test Setup procedure is executed before each test part to create the Common Topology.

Test Evidence Collected: Collect applicable evidence as described below.
- Description of the use, input, or display, of IPv6 addresses.
- Screenshots as needed.

Procedure:

Part A: Intra-subnet connectivity

Step	Action	Expected Observation
1.	Initiate an application-level connection from TAR-Node1 with the SUT.	TAR-Node1 establishes network-level and application-level connectivity with the SUT. The SUT returns a valid application response to TAR-Node1's request.

Part B: Inter-subnet connectivity

Step	Action	Expected Observation
2.	Initiate an application-level connection from TAR-Node2 with the SUT.	TAR-Node2 establishes network-level and application-level connectivity with the SUT. The SUT returns a valid application response to TAR-Node1's request.

Part C: Inter-VCN connectivity

Step	Action	Expected Observation
3.	Initiate an application-level connection from TAR-Node3 with the SUT.	TAR-Node3 establishes network-level and application-level connectivity with the SUT. The SUT returns a valid application response to TAR-Node1's request.

Part D: Inter-Region connectivity

Step	Action	Expected Observation

4.	Initiate an application-level connection from TAR-Node4 with the SUT.	TAR-Node4 establishes network-level and application-level connectivity with the SUT. The SUT returns a valid application response to TAR-Node1's request.

Part E: On-premises connectivity

Step	Action	Expected Observation
5.	Initiate an application-level connection from TAR-Node5 with the SUT.	TAR-Node5 establishes network-level and application-level connectivity with the SUT. The SUT returns a valid application response to TAR-Node1's request.

Part F: Cloud service connectivity

Step	Action	Expected Observation
6.	Initiate an application-level connection between the SUT and TAR-Service1.	The SUT establishes a connection successfully with TAR-Service1.

Part G: Internet connectivity

Step	Action	Expected Observation
7.	Initiate an application-level connection between the SUT and an IPv6-capable Internet Server.	The SUT establishes a connection successfully with the IPv6-capable Internet Server.

Possible Problems:

- The SUT may need to initiate communication with different services or compute resources depending on its intended use case or deployment scenario. If this is the case, communication directions for all parts may be reversed.
- The SUT may not allow users to initiate application-level connections with other systems. If this is the case, Part G may be omitted.

IPv6-Cloud.2.2: User Initiated Management/Monitoring Access

Purpose: All forms of remote management and monitoring functions must be fully functional in IPv6-only environments. [NIST IPv6 Profile], Section 4.1.1.

Applicable Product Types:
- Host, Router, NPP, Application

Test Setup: The Common Test Setup procedure is executed before each test part to create the Common Topology.

Test Evidence Collected: Collect applicable evidence as described below.
- Description of the use, input, or display, of IPv6 addresses.
- Screenshots as needed.

Procedure:

Part A: GUI Access

Step	Action	Expected Observation
1.	Connect to a graphical user interface provided by the SUT.	Connection is established.
2.	If applicable, perform a login function.	Access to the management functions of the SUT is granted.
3.	Navigate the management interface to confirm functionality (e.g. confirm version information, IPv6 address(es) etc.).	The management interface is navigable and responsive.

Part B: CLI Access

Step	Action	Expected Observation
4.	Connect to a command line interface provided by the SUT.	Connection is established.
5.	If applicable, perform a login function.	Access to the management functions of the SUT is granted.
6.	Navigate the management interface to confirm functionality (e.g. confirm version information, IPv6 address(es) etc.).	The management interface is navigable and responsive.

Part C: API Access

Step	Action	Expected Observation

7.	TAR-Node5 initiates an API request with an endpoint on the SUT.	The SUT receives the request and the response received by TAR-Node5 indicates that the requested operation was completed successfully.

Possible Problems:

- If the SUT does not support a remote management method (i.e. can only be managed via direct access through the console, or is unmanaged), this test may be omitted.
- If the SUT does not support a graphical user interface for remote management, part A may be omitted.
- If the SUT does not support a command line interface for remote management, part B may be omitted.
- If the SUT does not support an API for requesting SUT state information or performing SUT operations, part C may be omitted.

Modification Record

Version	Date	Editor	Modification
0.2	2024-08-12	Ben Patton	● Clarify scope and IPv6-Only network definitions ● Revise possible problems for Update test to align with existing IPv6-Only Functional Test Plan
0.1	2024-03-22	Ben Patton	● Initial Version