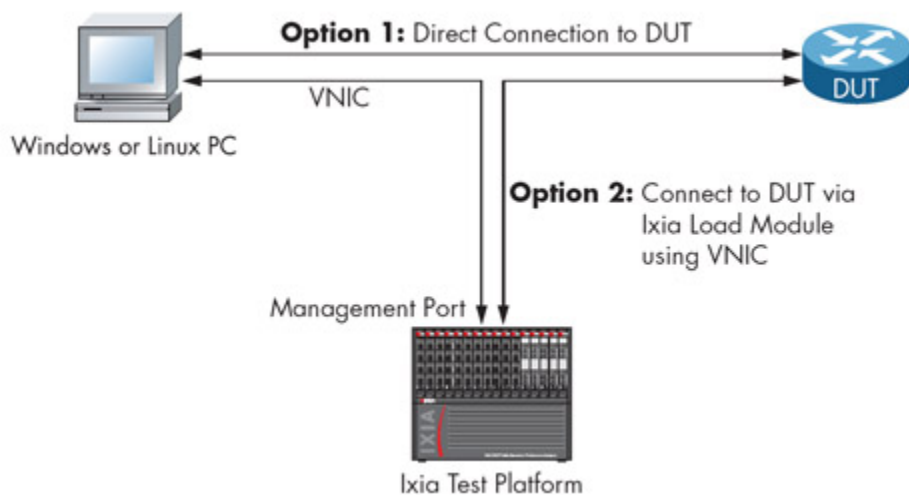


IxANVL™ - Automated Network Validation Library

Ixia's IxANVL (Automated Network Validation Library) is the industry standard for automated network/protocol validation. Developers and manufacturers of networking equipment and Internet devices rely on IxANVL to validate protocol compliance and interoperability. Many customers have chosen IxANVL for its ease-of-use, enhanced GUI, and flexible test automation capabilities. In addition, IxANVL offers a veritable universe of protocol libraries and utilities.

Though IxANVL is able to run on minimal hardware such as a PC with a Linux or Windows operating system and an Ethernet card, it is also well suited for operation on Ixia's powerful test and analysis platform via a VNIC (Virtual Network Interface Card) driver. This flexibility enables IxANVL to support all industry-standard test interfaces including 10/100/1G/10G Ethernet, ATM, serial, async, T1/E1, and POS. IxANVL provides conformance, negative, and regression testing on a vast selection of protocols including bridging, routing, PPP, TCP/IP, L4-7, IPv6, IP storage, IPsec, RMON, VPN, MPLS, voice over IP, Carrier Ethernet, and multicast.



Test Coverage

	IxANVL Test Suites	Target Protocols	Reference Specification	Test Case Count	Required Test Interfaces
IPv6 Test Suites	IPv6 Core	IPv6	RFC 2460, 2464,	111	2
		IPv6CP	RFC 2472	17	1
		ICMPv6	RFC 4443	46	2
	IPv6 Advanced	NDP	RFC 4861	228	2
		Generic Packet Tunneling	RFC 2473	46	2
		AutoConfig	RFC 4862	37	2
		V6oV4	RFC 4213, 2529, 3056, 3068	66	2
		PMTU	RFC 1981	10	1
		IP Router Alert	RFC 2711	13	2
	Mobile IPv6	Home Agent	RFC 3775	159	2
		Correspondence Node	RFC 3775	153	1
		Mobile Node	RFC3775	95	2
	GRE	GRE	RFC 2890, 2784	29	2
	DHCPv6	DHCP Client	RFC 3315	103	1
		DHCP Server	RFC 3315	141	2
IPv4 Test Suites	IPv4	IPv4	RFC 791, parts of 1122, 1812	70	2
		ICMP	RFC 792, parts of 1812	32	2
	DHCPv4	DHCP Client	RFC 2131	90	2
		DHCP Server	RFC 2131	74	2

Routing	IP RIP	RIP	RFC 2453	53	2
		IPGW	RFC 1812, 1122	18	2
	RIPng	RIPng	RFC 2080	60	2
	OSPF Core	OSPF	RFC 1583, 2328	312	3
	OSPF Extensions	Opaque LSA, NSSA, DB Overflow, Stub Router Ext	RFC 2370, 3101, 1765, 3137	56	3
		OSPF TE	RFC 3630	54	2
	OSPFv3	OSPFv3	RFC 5340, parts of RFC 2328	328	3
	OSPF-GR	OSPFv2-GR	RFC 3623	56	2
	VRRP	VRRP	RFC 3768	83	2
	BGP4 Core	BGP	RFC 4271	183	3
	BGP4 Extensions	BGP-OSPF, Communities, Route Flap Damping, Route Reflection, Route Refresh, Confederations	RFC 1403, 1997, 2439, 2918, 4456, 5065, 1771, 4360	147	3
	BGP Plus	BGP+ with IPv6	RFC 4271, 4760, 2545	200	3
	BGP 4-Byte AS	4-byte AS for BGP and BGPPlus	RFC 4893	50	3
	ISIS	ISIS	RFC 1195, 3719, ISO/IEC 10589: 1992(E)	229	2
	ISIS	ISIS-TE	RFC 3784	31	1
	ISISv6	ISIS-v6	ISO/IEC 10589: 1992(E), RFC 3719, 1195, 5308	221	2

MPLS	MPLS	Label Encapsulation	RFC 3032	59	2
	RSVP-TE	RSVP-TE	RFC 3209, draft-ietf-mpls-rsvp-lsp-tunnel-07	87	3
	RSVP-TE	RSVP-TE P2MP	RFC 4875	48	3
	LDP	LDP	RFC 3036	329	3
	mLDP	mLDP P2MP	draft-ietf-mpls-ldp-p2mp-10	97	4
	LSP-Ping-Tr	LSP Ping and Traceroute	RFC 4379	128	2
	VCCV	Pseudo wire VCCV	RFC 5085	70	2
	L2VPN (PWE3)	PWE3-Control	RFC 4447	69	2
		PWE3-Encapsulation	RFC 4448, 4618, 4717, 4385, 4623	78	2
	VPLS	VPLS	RFC 4762	58	4
	VPLS-BGP	VPLS with BGP AD and signalling	RFC 4761	46	4
	L3 VPN	L3 VPN	RFC 4364	101	3

MPLS-TP	MPLS-TP-Y1731-CC-LD	MPLS-TP-Y1731-CC-LD	RFC 5586 (GACH), draft-bhh-mpls-tp-oam-y1731-06.txt, ITU-T-REC Y.1731-200605-I	85	1
	MPLS-TP-IETF-CC-CV-LD	MPLS-TP-IETF-CC-CV-LD	RFC 5586 (GACH), draft-ietf-mpls-loss-delay-01, draft-ietf-mpls-tp-on-demand-cv-02, draft-ietf-mpls-tp-cc-cv-rdi-03	210	1
	MPLS-TP-G.8031-APS-Y.1731	MPLS-TP-G.8031-APS-Y.1731	G.8031_Y.1342-2006-06	140	2
Multicasting Test Suites	IGMP	IGMPv2	RFC 2236	49	2
		IGMPv3	RFC 3376	153	2
	DVMRP	DVMRP	draft-ietf-idmr-dvmrp-v3-07	66	3
	PIM	Dense Mode	draft-ietf-pim-dm-new-v2-04	162	3
		Sparse Mode, SSM	RFC 4601, draft-ietf-pim-sm-bsr-12	327	3
	PIMv6	Sparse Mode	draft-ietf-pim-sm-v2-new-12, draft-ietf-pim-sm-bsr-12	283	3
	MLD	MLDv1	RFC 2710	98	2
		MLDv2	RFC 3810	202	2

High Availability	BFD	BFD Base, BFD Generic, BFD-v4v6-1hop for OSPFv2/v3, ISIS and BGP BFD-MPLS	drafts draft-ietf-bfd-base-09.txt, draft-ietf-bfd-generic-05.txt, draft-ietf-bfd-v4v6-1hop-09.txt, draft-ietf-bfd-mpls-07.txt	178	3
TCP Test Suites (see Note 1)	TCP Core	TCP	RFC 793, 1122, 2460	179	2
	TCP Advanced	Slow Start, Congestion Control, PMTU Disc, MD5	RFC 2001, 2581, 1191, 2385, 2463, 1981	48	1
	TCP High Performance	Ext for High Performance, Selective Ack	RFC 1323, 2018	48	1
UDP Test Suite	UDP	UDP	RFC 768, 1122	35	1
Layer 4-7 Test Suite	HTTP	HTTP Server	RFC 2616	346	1
	Telnet	Telnet Client/Server	RFC 854	43	1
IP Storage Suites	iSCSI	iSCSI Target	RFC 3720	210	1
		iSCSI Initiator	RFC 3720	205	1

VPN Test Suites	IPSec AH	MD5, SHA	RFC 4301, 4302	58	2
	IPSec ESP	MD5, SHA, DES, 3DES, Blowfish, AES	RFC 4301, 4303, 2403, 2404, 2405	72	2
	IPSec IKE	ISAKMP, IKE	RFC 2407, 2408, 2409	373	2
	IPSec AH / IPv6	MD5, SHA, IPSecv6	RFC 4301, 4302	66	2
	IPSec ESP / IPv6	MD5, SHA, DES, 3DES, Blowfish, AES	RFC 4301, 4303, 2403, 2404, 2405, 2406	74	2
	IPSec IKE / IPv6	ISAKMP, IKE	RFC 2407, 2408, 2409	384	2
	IKEV2	IKEV2, DES, 3DES, AES-128, 256, 192, MD5, SHA, DH-768, 1024, 1536, 2048, 3072	RFC 4306	189	2
	L2TP	L2TP	RFC 2661	105	1
	PPTP	PPTP	draft-ietf-pppext-pptp-02	55	1
PPP Test Suites	PPP	LCP, PPP, PPP in HDLC	RFC 1661, 1662	111	2
		Authentication (PAP, CHAP)	RFC 1334, 1994	37	1
	IPCP	IPCP	RFC 1332	19	2
	VJ	VJ Compression	RFC 1144	48	2
	PPPoE	PPP over Ethernet	RFC 2516	75	2
	Multilink PPP	MPPP	RFC1717, 1990	59	3
	Multilink PPP	Multi-class Extension	RFC 2686	9	3

Carrier Ethernet	MEF9	MEF9	MEF1, MEF9, Iometrix Test Plan version 1.4	247	6
	EtherCFM	Ethernet CFM	IEEE P802.1ag/D8.1 2007	246	3
	EtherOAM	Ethernet OAM	IEEE 802.3-ah-2004	166	3
	MEF OAM	MEF21 OAM	MEF 21 Abstract Test Suite for UNI Type 2	187	2
	Service OAM	Y.1731	ITU-T Y.1731 05/2006, IEEE P802.1ag/D8.1 June 8,2007	106	2
	Provider BB	PBB	IEEE 802.1ah D4.2 2005	55	2
	MEF Service OAM	MEF Service OAM	ATS for UNI Type 2 Part 3 - Service OAM	157	2
	MEF ELMI	MEF ELMI	D00063_004 ATS for UNI Type 2 Part 2 ELMI TC MEF 16	239	2
	G8031	G.8031 1:1 protection	Ethernet Automatic Protection Switching – ITU-T G8031/Y.1342	283	3

Bridging	STP	802.1d	IEEE Std. 802.1D-1998	53	3
	RSTP	802.1w	IEEE Std. 802.1D-2004	126	4
	EAPOL	802.1x, MD5, TLS, TTLS	IEEE 802.1x-2004	83	3
	MSTP	802.1s	IEEE 802.1Q-2005	247	4
	LLDP	LLDP	IEEE 802.1AB 2005	104	3
	DCBX	DCBX	DCB Capability Exchange Protocol Specification (Rev 1.0), DCB Capability Exchange Protocol Base Specification (Rev 1.01)	92	1
	Mcast Snooping	IGMP/MLD Snooping	RFC 4541	42	3
	VLAN	802.1q, GMRP, GVRP	IEEE Std. 802.1Q-2005	161	4
	LACP	802.3ad	IEEE Std. 802.3-2005 Clause 43	118	4
	QinQ	QinQ	IEEE 802.1ad-2005	127	2
	MVRP/MMRP	MVRP, MMRP	IEEE Std 802.1ak-2007 IEEE Std 802.1Q™-2005/Cor 1-2008	321	3
VoIP	SIP	SIP Server	RFC 3261	297	2

Fiber Chanel over Ethernet (FCoE)	FIP	FCoE Initialization Protocol	FCoE Initialization Protocol, FIBRE CHANNEL BACKBONE-5, Rev 1.04, Prepared by the INCITS, T11/ Project 1871-D	169	1
	FCoE FCF	FCoE FCF	FIBRE CHANNEL LINK SERVICES, Rev 2.11, Prepared by the INCITS, T11/Project 2103-D	56	1
RMON Test Suites	RMON	Ethernet General	RFC 1757 RFC 1757	116 372	1 1
Toolkits	TCP Toolkit		N/A	4	1
Toolkits	SNMP Toolkit	Toolkit & sample tests only	N/A	9	1

Note 1: TCP test suites require a connection with the device under test (DUT) from both below and above the targeted TCP layer. Connection from below the TCP layer is achieved via a traditional physical layer interface. Connection from above the TCP layer can only be achieved with a unique application called "TCP Stub," developed by Ixia. The TCP Stub is controlled and managed remotely by Ixia TCP Test Suites. The purpose of the TCP Stub is to generate the necessary stimulus above the TCP layer required for testing. The TCP Stub is a portable C-code application bundled with TCP test suites. Customers are required to compile the TCP Stub onto their target systems.

Benefits

IxANVL Saves Time and Money

IxANVL allows vendors to verify the design during their product's entire life cycle. Problems can be identified earlier so as to prevent costly last-minute reworks. IxANVL emulates large, multi-node networks that previously were cost prohibitive – resulting in more efficient tests and quicker product release times.

IxANVL Increases Confidence

IxANVL increases confidence in product quality by enabling extensive and thorough testing, performed automatically and without supervision. IxANVL's test results allow users to:

- Determine exactly where a device's protocol software does and does not meet the specification
- Observe how well the device handles traffic from non-complying network components
- Determine how new development effects existing code, via regression testing

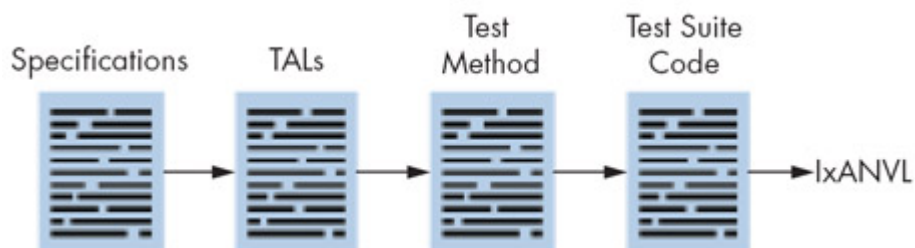
IxANVL Expands Easily

With a source code license, users can easily add new interface types, protocols, and/or test cases to their IxANVL system.

IxANVL Supports More Protocols

IxANVL supports a comprehensive list of protocols, including unicast/multicast routing, bridging, IPv6, VPN, MPLS, PPP, TCP/IP, RMON, voice over IP, metro Ethernet, and IP storage.

Test Methodology



IxANVL follows a rigorous test suite development process:

- Analyze a protocol specification line-by-line
- Develop a test assertion list (TAL), which is a list of testable statements
- Augment TALs with more negative tests
- Prioritize and group TALs for the test suite
- Develop a test method for each accepted test assertion

IxANVL performs continual verification of protocol standard authors or implementers during the development process.

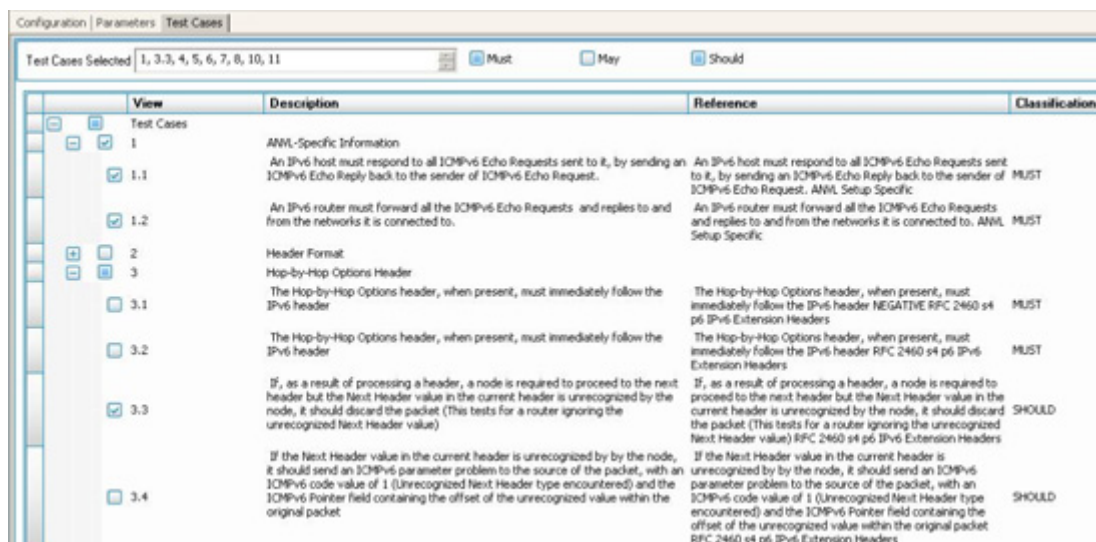
Test Configuration

The IxANVL test suite can run on a Linux or Windows PC with off-the-shelf network interface cards, or on Ixia's load modules through a virtual network interface card (VNIC) connection. The tester (PC) connects with the DUT via test interfaces. Up to four interfaces may be used, depending on the test configuration. IxANVL flexibly emulates various system topologies, and creates virtually any test scenarios for almost any DUT.

IxANVL offers both a command-line interface for test automation and a user-friendly graphical user interface, allowing intuitive test execution management and detail reporting. A batch runner is also available for scheduling regression test-run sequences.

Test Execution

IxANVL classifies test cases into three categories: MUST, SHOULD, and MAY. Tests can be selected and executed based on their categories or test topologies.



View	Description	Reference	Classification
Test Cases			
1	ANVL-Specific Information		
1.1	An IPv6 host must respond to all ICMPv6 Echo Requests sent to it, by sending an ICMPv6 Echo Reply back to the sender of ICMPv6 Echo Request.	An IPv6 host must respond to all ICMPv6 Echo Requests sent to it, by sending an ICMPv6 Echo Reply back to the sender of ICMPv6 Echo Request. ANVL Setup Specific.	MUST
1.2	An IPv6 router must forward all the ICMPv6 Echo Requests and replies to and from the networks it is connected to.	An IPv6 router must forward all the ICMPv6 Echo Requests and replies to and from the networks it is connected to. ANVL Setup Specific.	MUST
2	Header Format		
3	Hop-by-Hop Options Header		
3.1	The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header	The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header NEGATIVE RFC 2460 s4 p6 IPv6 Extension Headers	MUST
3.2	The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header	The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header RFC 2460 s4 p6 IPv6 Extension Headers	MUST
3.3	If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet (This tests for a router ignoring the unrecognized Next Header value)	If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet (This tests for a router ignoring the unrecognized Next Header value) RFC 2460 s4 p6 IPv6 Extension Headers	SHOULD
3.4	If the Next Header value in the current header is unrecognized by the node, it should send an ICMPv6 parameter problem to the source of the packet, with an ICMPv6 code value of 1 (Unrecognized Next Header type encountered) and the ICMPv6 Pointer field containing the offset of the unrecognized value within the original packet	If the Next Header value in the current header is unrecognized by the node, it should send an ICMPv6 parameter problem to the source of the packet, with an ICMPv6 code value of 1 (Unrecognized Next Header type encountered) and the ICMPv6 Pointer field containing the offset of the unrecognized value within the original packet RFC 2460 s4 p6 IPv6 Extension Headers	SHOULD

The IxANVL test can be run using two options - GUI or command line input. In GUI mode, the user selects which test suite and test cases to run. In command line mode, the user types a command with options indicating which tests should run and the desired output level.

In the test, IxANVL sends packets to the DUT based on the test designed, and compares the received DUT packets to what was expected. After receiving these packets, IxANVL reacts according to the returned information - it may continue the test, stop the test, log an error message, or a host of other functions.

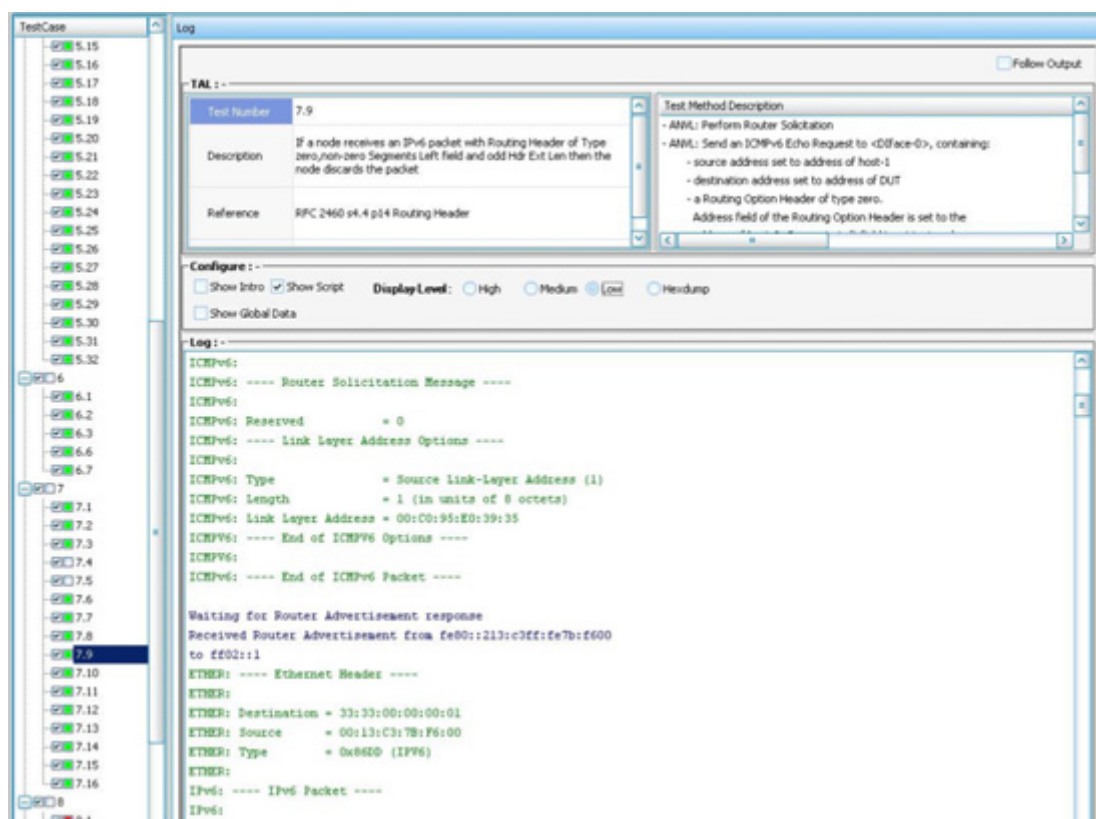
During the test, IxANVL logs the progress in real-time. After completion, IxANVL indicates whether the test passed or failed. IxANVL then repeats the process with the next test until all selected tests have been run.

Test Results

Users can specify four levels of test outputs:

- High level - basic pass/fail
- Medium level - pass/fail and test event status
- Low level - comprehensive report with packet decode
- Hexdump - detail report with hexdump of every packet exchanged between tester and DUT

IxANVL results include detailed trace outputs with a description of the test methodology for side by side reference.



The screenshot displays the IxANVL software interface. On the left, a 'Test Case' list shows various test cases, with test case 7.9 selected. The main window is divided into several sections:

- Log:** A table showing test details for test case 7.9.

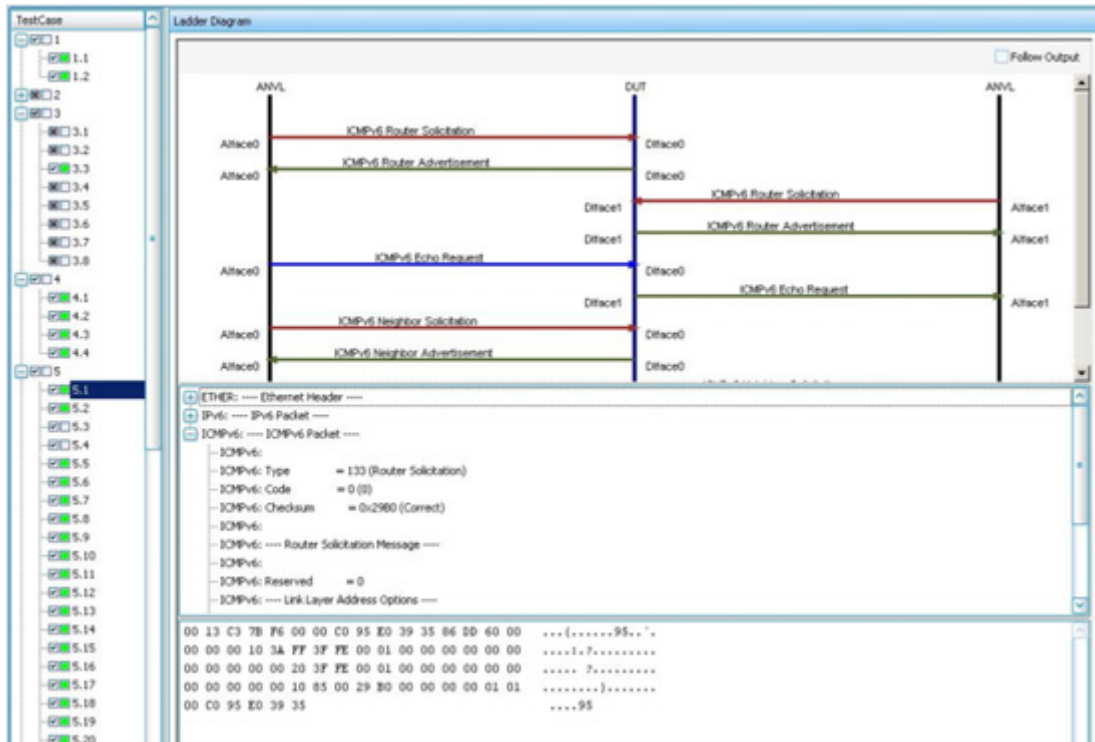
Test Number	Description	Reference
7.9	If a node receives an IPv6 packet with Routing Header of Type zero, non-zero Segments Left field and odd Hdr Ext Len then the node discards the packet.	RFC 2460 s4.4 p14 Routing Header
- Test Method Description:** A text area providing details about the test methodology, including ANVL: Perform Router Solicitation and ANVL: Send an ICMPv6 Echo Request to <Df ace>, containing:
 - source address set to address of host-1
 - destination address set to address of DUT
 - a Routing Option Header of type zero.
 - Address field of the Routing Option Header is set to the
- Configure:** A section with checkboxes for 'Show Intro', 'Show Script', and 'Show Global Data'. The 'Display Level' is set to 'Low' (radio buttons for High, Medium, Low, Hexdump).
- Log:** A text area showing network traffic traces. The traces include:


```

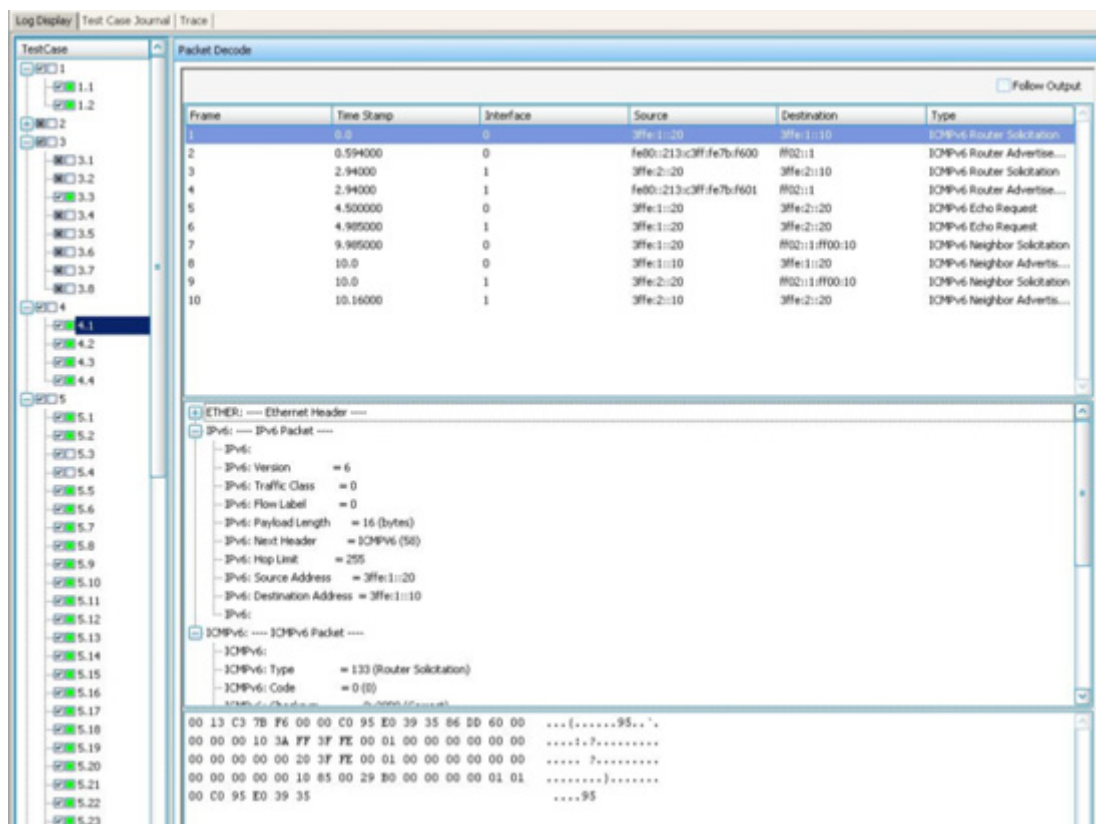
      ICMPv6: ---- Router Solicitation Message ----
      ICMPv6:
      ICMPv6: Reserved          = 0
      ICMPv6: ---- Link Layer Address Options ----
      ICMPv6:
      ICMPv6: Type                = Source Link-Layer Address (1)
      ICMPv6: Length              = 1 (in units of 8 octets)
      ICMPv6: Link Layer Address = 00:00:95:E0:39:35
      ICMPv6: ---- End of ICMPv6 Options ----
      ICMPv6:
      ICMPv6: ---- End of ICMPv6 Packet ----

      Waiting for Router Advertisement response
      Received Router Advertisement from fe80::213:c3ff:fe7b:f600
      to ff02::1
      ETHER: ---- Ethernet Header ----
      ETHER:
      ETHER: Destination = 33:33:00:00:00:01
      ETHER: Source      = 00:13:C3:7B:F6:00
      ETHER: Type        = 0x86DD (IPv6)
      ETHER:
      IPv6: ---- IPv6 Packet ----
      IPv6:
      
```

In addition to log outputs, IxANVL provides a timing diagram that represents the relationship of the test packets exchanged between IxANVL and DUT.



IxANVL provides comprehensive packet-by-packet analysis for every test case.



Frame	Time Stamp	Interface	Source	Destination	Type
1	0.0	0	3ffe:1::20	3ffe:1::10	ICMPv6 Router Solicitation
2	0.594000	0	fe80::213:c3ff:fe7b:f600	#02::1	ICMPv6 Router Advertisement
3	2.94000	1	3ffe:2::20	3ffe:2::10	ICMPv6 Router Solicitation
4	2.94000	1	fe80::213:c3ff:fe7b:f601	#02::1	ICMPv6 Router Advertisement
5	4.500000	0	3ffe:1::20	3ffe:2::20	ICMPv6 Echo Request
6	4.985000	1	3ffe:1::20	3ffe:2::20	ICMPv6 Echo Request
7	9.985000	0	3ffe:1::20	#02::1#ff00:10	ICMPv6 Neighbor Solicitation
8	10.0	0	3ffe:1::10	3ffe:1::20	ICMPv6 Neighbor Advertisement
9	10.0	1	3ffe:2::20	#02::1#ff00:10	ICMPv6 Neighbor Solicitation
10	10.16000	1	3ffe:2::10	3ffe:2::20	ICMPv6 Neighbor Advertisement

```

ETHER: --- Ethernet Header ---
IPv6: --- IPv6 Packet ---
  -IPv6:
  -IPv6: Version = 6
  -IPv6: Traffic Class = 0
  -IPv6: Flow Label = 0
  -IPv6: Payload Length = 16 (bytes)
  -IPv6: Next Header = ICMPv6 (58)
  -IPv6: Hop Limit = 255
  -IPv6: Source Address = 3ffe:1::20
  -IPv6: Destination Address = 3ffe:1::10
  -IPv6:
  -ICMPv6: --- ICMPv6 Packet ---
  -ICMPv6:
  -ICMPv6: Type = 133 (Router Solicitation)
  -ICMPv6: Code = 0 (0)
  -ICMPv6: Checksum = 0x0000 (0x0000)
00 13 c3 7b f6 00 00 c0 95 e0 39 35 86 00 60 00 ...{.....95..
00 00 00 10 3a ff 3f fe 00 01 00 00 00 00 00 00 ...:.....
00 00 00 00 00 20 3f fe 00 01 00 00 00 00 00 00 ...?.....
00 00 00 00 00 10 85 00 29 80 00 00 00 00 01 01 ...}.....
00 c0 95 e0 39 35 .....95
  
```

All IxANVL tests are logged for post analysis.

Platform

An IxANVL workstation supports the following configuration:

- CentOS 5.3 (kernel 2.6.18-128.el5xen); Redhat Enterprise 4.0 with kernel 2.6.9-11 or 2.6.22.0.2.EL; Redhat Enterprise 5.0 (with kernel 2.6.18-53.el5)
- Microsoft Windows XP Professional or Windows 2003 Server (US English versions)
- 1.5 GHz Pentium CPU or faster (32 bit system only)
- 1GB RAM
- 512 MB Free Disk Space

Supported Interfaces

IxANVL supports a wide range of network interface cards that directly attach to a Linux or Windows PC:

- Ethernet 10/100
- Gigabit Ethernet
- Async serial
- Sync serial
- T1/E1
- PPPoE

IxANVL also supports Ixia's virtual network interface card (VNIC). Ixia's VNIC is an interface driver that resides on a Linux workstation and Ixia chassis, and allows the IxANVL test suites to access Ixia's load modules.

Ixia VNIC supports the following types of Ixia load modules (per-port CPU required):

- 10 Gigabit Ethernet including NGY family
- Ethernet family (10/100/1000 Mbps)
- Packet over SONET OC3/12/48/192
- ATM OC-3/12

VNIC requires the following software:

- Client (IxANVL Workstation): Redhat 9.0 with kernel 2.4.20-8 or 2.4.20-6, Redhat Enterprise 4.0 with kernel 2.6.9-11.EL or 2.6.22.0.2.EL, Redhat Enterprise 5.0 with kernel 2.6.18-53.el5, Microsoft Windows XP Professional or Windows 2003 Server (US English versions)
- Server (Ixia Chassis): 5.20 GA Patch 2 or 5.30 EA SP2(or higer)

Each conformance test suite supports different sets of test interfaces. Please contact Ixia for applicable test interfaces for the test suite of your interest.

Product Ordering Information

924-00x-10xx

IxANVL Framework license

924-040-91xx

IPv6 Framework Upgrade if IPv6 test is needed

924-030-xxx

Interface Support Software for each individual test interface. This is the custom interface driver needed to run IxANVL test suite

924-xxx-xxx

Individual IxANVL test suite

This material is for informational purposes only and subject to change without notice. It describes Ixia's present plans to develop and make available to its customers certain products, features and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.