

# IxLoad — IPSEC and Network Access Test

Ensure A Smooth Growth Transition with Pre-Deployment Testing Experience

## Problem: Manage Subscriber Growth and SLA Guarantees

Subscriber growth and exploding service offerings are challenging existing access networks. Service providers are struggling to manage their networks with careful capacity planning and IPv6 transitioning considerations. But with subscribers that range from residential broadband customers using PPPoE or DHCP, to telecommuters using IPsec and enterprises using dedicated leased lines, it is difficult to assess the impact of network volatility as buildout occurs. Managed growth means avoiding outages and interface flaps and controlling quality of experience (QoE) for real-time and business-critical services as your access network evolves.

## Solution: Scalable Emulation Test to Ensure Dynamic and Robust Access Networks

For high-performing multiplay networks, service providers need pre-deployment validation that includes realistic simulations of the dynamic behavior of subscribers accessing the networks. The IxLoad Network Access and VPN test solution provides a rich set of emulations with dynamic interface behavior that adds a new dimension of subscriber and network realism when testing application-aware devices.

# Table of Contents

- Problem: Manage Subscriber Growth and SLA Guarantees..... 1
- Solution: Scalable Emulation Test to Ensure Dynamic and Robust Access Networks..... 1
- Network Access and VPN Technologies Supported ..... 3
- Dynamic Control Plane (DCP) ..... 4
- Network Failure Threshold (NFT)..... 5
- Specifications..... 5
- Platform Options ..... 18
- Technology Solutions..... 18
- IxLoad Ordering Information ..... 19

## Highlights

- Ensure smooth deployment by testing under realistic access network scenarios—mixed subscriber types over same link and multiplay services over emulated subscribers
- Stress-test and measure subscriber management capability KPIs
- Evaluate IPv6 readiness of handling IPv4, IPv6, and transition technologies such as 6RD/DSLite
- Ensure reliable service and subscriber QoE by characterizing performance of multiplay services over variety of network access technologies

## Key features

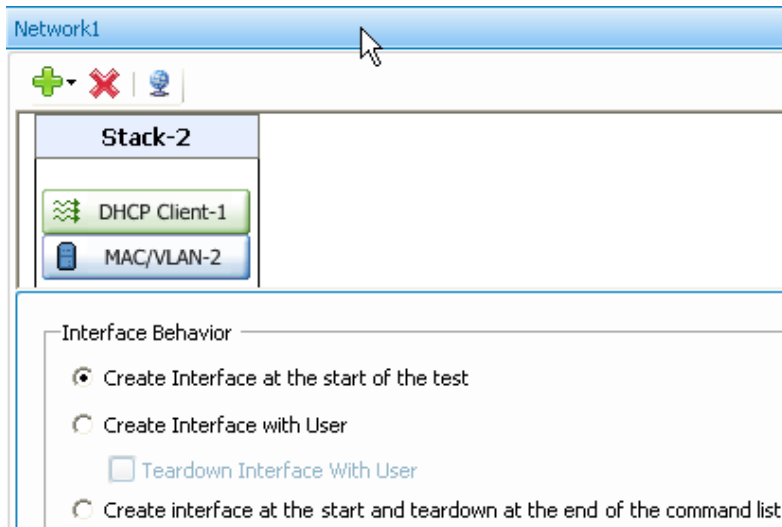
- Realistically simulate dynamic interface setup and tear-down behavior linked with subscriber emulation
- Simulate network 'blackouts' and 'brownouts' and assess the impact of network volatility on application performance and subscriber QoE
- Correlate application-layer performance with network control-plane performance

## Network Access and VPN Technologies Supported

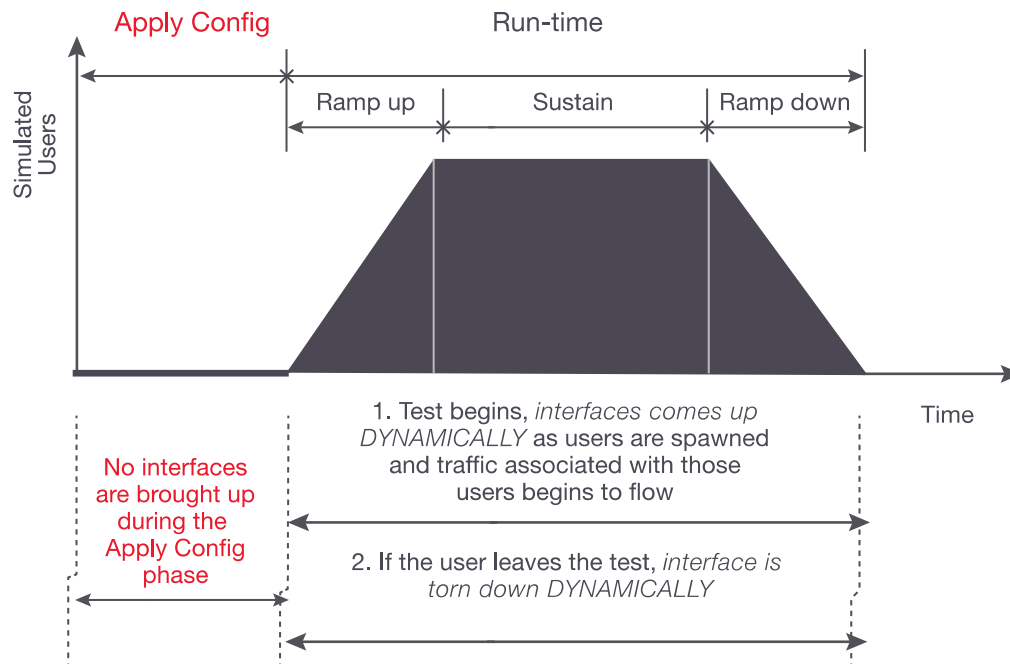
Technology	Protocols
Broadband Access	DHCP, PPPoE, PPTP, L2TP and GRE
IPv6 Transitioning	DSLite, 6RD, and SLAAC
Authentication	802.1x, EAP over UDP, and NAC
Security/VPN	IPsec

# Dynamic Control Plane (DCP)

DCP dynamically creates and tears down interfaces during testing. With DCP, every interface is created in conjunction with the new subscribers and the application traffic begins immediately after the interfaces are configured, replicating real-world subscriber behavior.



Emulated users connect/disconnect from the network dynamically like in real-world



DCP explained in the context of a test timeline

# Network Failure Threshold (NFT)

NFT operates in conjunction with DCP and enables IxLoad to run tests even when some interfaces fail during the test run. A failure threshold controls the number of allowed failures, beyond which the test is aborted.

## Network Features

Dynamic Control Plane Modes	<ul style="list-style-type: none"> <li>• Create interface at the start of the test (static mode)</li> <li>• Create interface with user               <ul style="list-style-type: none"> <li>◦ Teardown interface with user</li> </ul> </li> <li>• Create interface at the start and teardown at the end of the command list</li> </ul>
Network Failure Threshold	<ul style="list-style-type: none"> <li>• Maximum percentage of network interface failures that is accepted for the test to continue running</li> </ul>
Supported Network Protocols	<ul style="list-style-type: none"> <li>• DHCP</li> <li>• PPPoE</li> <li>• PPTP</li> <li>• L2TP</li> <li>• IPsec</li> </ul>
Supported Application Protocols	<ul style="list-style-type: none"> <li>• HTTP</li> <li>• FTP</li> <li>• IMAP</li> <li>• POP3</li> <li>• SMTP</li> <li>• DNS</li> <li>• StatelessPeer</li> <li>• RTSP</li> <li>• SIP</li> </ul>

# Specifications

## IPsec

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• Initiator and Responder mode</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Industry's highest performance and capacity with the CloudStorm and PerfectStorm hardware families</li> <li>• Supports most of the popular encryption, hash, and authentication algorithms</li> <li>• Includes a complete set of IPsec benchmarking test methodologies (IPsec QuickTests)</li> <li>• Measures control plane and data plane performance and capacity</li> <li>• Generates real application traffic over encrypted tunnels</li> <li>• Dynamic tunnel setup and teardown options</li> <li>• Supports IKEv1, IKEv2, and manual keying</li> <li>• Integrated IPsec configuration wizards</li> </ul>

## IPsec

	<ul style="list-style-type: none"> <li>• Site-to-site and remote access scenarios</li> <li>• Comprehensive per-tunnel diagnostics and statistics</li> </ul>
Supported Application Protocols	<ul style="list-style-type: none"> <li>• HTTP</li> <li>• FTP</li> <li>• IMAP</li> <li>• POP3</li> <li>• SMTP</li> <li>• DNS</li> <li>• StatelessPeer</li> <li>• RTSP</li> <li>• SIP</li> </ul>
QuickTests	<ul style="list-style-type: none"> <li>• IPsec Tunnel Setup Rate</li> <li>• IPsec Tunnel Capacity</li> <li>• IPsec RFC2544 Throughput/Latency</li> <li>• IPsec RFC2544 Frame Loss</li> <li>• IPsec RFC2544 Soak</li> </ul>
Keying Methods	<ul style="list-style-type: none"> <li>• IKEv1</li> <li>• IKEv2</li> <li>• Manual keying</li> </ul>
IPsec Parameters IKE Phase1/AUTH_S A	<ul style="list-style-type: none"> <li>• Main and aggressive mode</li> <li>• Hash algorithms:             <ul style="list-style-type: none"> <li>◦ HMAC-MD5</li> <li>◦ HMAC-SHA1</li> <li>◦ AES-XCBC-MAC-96 (RFC3566)</li> <li>◦ HMAC-SHA256</li> <li>◦ HMAC-SHA384</li> <li>◦ HMAC-SHA512</li> </ul> </li> <li>• Encryption algorithms:             <ul style="list-style-type: none"> <li>◦ DES</li> <li>◦ 3DES</li> <li>◦ AES-128-CBC</li> <li>◦ AES-192-CBC</li> <li>◦ AES-256-CBC</li> <li>◦ AES-128-GCM ICV 8/12/16</li> <li>◦ AES-192-GCM ICV 8/12/16</li> <li>◦ AES-256-GCM ICV 8/12/16</li> </ul> </li> <li>• Multiple Proposals</li> <li>• Xauth user authentication</li> <li>• ModeCFG address assignment</li> <li>• IKEv2 Suggested IP address</li> <li>• Pseudo-random functions             <ul style="list-style-type: none"> <li>◦ HMAC-MD5</li> <li>◦ HMAC-SHA1</li> <li>◦ AES-XCBC</li> </ul> </li> </ul>

## IPsec

	<ul style="list-style-type: none"> <li>◦ HMAC-SHA256</li> <li>◦ HMAC-SHA384</li> <li>◦ HMAC-SHA512</li> </ul>
IPsec Parameters Phase 2/CHILD_SA	<ul style="list-style-type: none"> <li>• AH, ESP, AH+ESP</li> <li>• Tunnel mode</li> <li>• Transport mode</li> <li>• Hash algorithms:             <ul style="list-style-type: none"> <li>◦ HMAC-MD5-96</li> <li>◦ HMAC-SHA1-96</li> <li>◦ HMAC-SHA256-128</li> <li>◦ HMAC-SHA384-192</li> <li>◦ HMAC-SHA512-256</li> </ul> </li> <li>• Encryption algorithms:             <ul style="list-style-type: none"> <li>◦ NULL</li> <li>◦ DES and 3DES</li> <li>◦ AES-128-CBC</li> <li>◦ AES-192-CBC</li> <li>◦ AES-256-CBC</li> <li>◦ AES-128-GCM ICV 8/12/16</li> <li>◦ AES-192-GCM ICV 8/12/16</li> <li>◦ AES-256-GCM ICV 8/12/16</li> <li>◦ AES-128-GMAC</li> <li>◦ AES-192-GMAC</li> <li>◦ AES-256-GMAC</li> </ul> </li> <li>• Multiple Proposals</li> <li>• Perfect Forward Secrecy (PFS)</li> <li>• Lifetime negotiation and re-keying</li> <li>• IKEv1: Multiple Phase2 SAs over a single Phase1 SA</li> <li>• IKEv2: Multiple ChildSAs over a single IKE SA</li> </ul>
Authentication Method	<ul style="list-style-type: none"> <li>• Pre-shared key</li> <li>• RSA, ECDSA and DSA Certificates             <ul style="list-style-type: none"> <li>◦ Keys of 512, 1024, 2048, 4096, and 8192 bits for RSA</li> <li>◦ Prime256v1, secp384r1, secp521r1 for ECDSA</li> </ul> </li> <li>• Chained Certificates</li> <li>• EAP (MD5, SIM, TLS, AKA, GTC, OTP)             <ul style="list-style-type: none"> <li>◦ EAP vs. PreSharedKeys</li> <li>◦ EAP vs. Certificates</li> <li>◦ EAP only</li> </ul> </li> </ul>
Certificate Management	<ul style="list-style-type: none"> <li>• SCEP (Simple Certificate Enrollment Protocol)</li> <li>• CMPv2 (Certificate Management Protocol)</li> <li>• CRL (Certificate Revocation List)</li> <li>• OSCP (Online Status Certificate Protocol)</li> </ul>
DH Groups	<ul style="list-style-type: none"> <li>• DH-01 (MODP-768)</li> <li>• DH-02 (MODP-1024)</li> </ul>

## IPsec

	<ul style="list-style-type: none"> <li>• DH-05 (MODP-1536)</li> <li>• DH-14 (MODP-2048)</li> <li>• DH-15 (MODP-3072)</li> <li>• DH-16 (MODP-4096)</li> <li>• DH-17 (MODP-6144)</li> <li>• DH-18 (MODP-8192)</li> <li>• DH-19 (ECP-256)</li> <li>• DH-20 (ECP-384)</li> <li>• DH-21 (ECP-512)</li> <li>• DH-22 (MODP-1024-S160)</li> <li>• DH-23 (MODP-2048-S224)</li> <li>• DH-24 (MODP-2048-S256)</li> <li>• DH-25 (ECP-192)</li> <li>• DH-26 (ECP-224)</li> <li>• DH-27 (ECP-224)</li> <li>• DH-28 (ECP-256)</li> <li>• DH-29 (ECP-384)</li> <li>• DH-30 (ECP-512)</li> </ul>
IPsec features	<ul style="list-style-type: none"> <li>• Site to Site and Remote Access test scenarios</li> <li>• IPsec initiator and responder modes</li> <li>• VLAN and QnQ support</li> <li>• NAT-T</li> <li>• IPsec pre-fragmentation</li> <li>• IPsec post-fragmentation</li> <li>• Initial contact payload</li> <li>• IKEv2 redirect</li> <li>• Multiple Traffic Selectors (IKEv2)</li> <li>• IPsec over GRE</li> <li>• Multiple P2 over P1</li> </ul>
Tunnel control	<ul style="list-style-type: none"> <li>• Tunnel setup and tear down</li> <li>• Persistent and non-persistent tunnels</li> <li>• IPsec tunnel flapping (dynamic sessions)</li> <li>• Dead peer detection (DPD)</li> <li>• Tunnel Reinitiation</li> <li>• Extended Sequence Number</li> <li>• Rekeying support</li> <li>• IKE message retry timers</li> <li>• NAT Traversal (NAT-T)</li> <li>• Lifetime negotiation (IKEv1)</li> <li>• Re-keying</li> </ul>
Addressing	<ul style="list-style-type: none"> <li>• IPv4/IPv4</li> <li>• IPv6/IPv6</li> <li>• IPv4/IPv6</li> <li>• IPv6/IPv4</li> <li>• Single or multiple hosts behind each emulated gateway</li> </ul>

## IPsec

	<ul style="list-style-type: none"> <li>• Unique MAC per emulated gateway</li> <li>• Unique VLAN per emulated gateway</li> <li>• Support for Virtual Router (Emulated Router)</li> </ul>
RFCs	<ul style="list-style-type: none"> <li>• RFC 2394, IP Compression (DEFLATE algorithm)</li> <li>• RFC 2401, Security Architecture for the Internet Protocol</li> <li>• RFC 2402, IP Authentication Header</li> <li>• RFC 2406, IP Encapsulating Security Payload (ESP)</li> <li>• RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP</li> <li>• RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)</li> <li>• RFC 2409, The Internet Key Exchange (IKE)</li> <li>• RFC3566, The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec</li> <li>• RFC 3715, IPsec-Network Address Translation (NAT) Compatibility Requirements</li> <li>• RFC 3748, Extensible Authentication Protocol (EAP)</li> <li>• RFC 3947, Negotiation of NAT-Traversal in the IKE</li> <li>• RFC 3948, UDP Encapsulation of IPsec ESP Packets</li> <li>• RFC 7296, Internet Key Exchange (IKEv2) Protocol</li> <li>• RFC 5996, An Extension for EAP-Only Authentication in IKEv2</li> <li>• RFC 4304, Extended Sequence Number</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• IPsec Global Statistics (all ports and per test port)</li> <li>• IPsec per Tunnel Statistics</li> </ul>

## DHCP

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• Client and Server</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Setup and teardown rates - Initial rate, increment, final rate, max outstanding</li> <li>• Timeout and retransmission timers - Initial discover timeout, timeout factor, reattempt count</li> <li>• Configurable UDP client and server ports</li> <li>• Suggested lease time</li> <li>• Maximum DHCP message size</li> </ul>
Commands	<ul style="list-style-type: none"> <li>• IPv4 - discover, request, renew, decline, release, inform</li> <li>• IPv6 - solicit, request, confirm, renew, rebind, release, reconfigure</li> </ul>
Relay Agent	<ul style="list-style-type: none"> <li>• DHCP relay agent (Option 82) <ul style="list-style-type: none"> <li>◦ Multiple relay agent emulation</li> <li>◦ Trusted network element emulation</li> <li>◦ Circuit ID, remote ID – sequence generator capable</li> </ul> </li> </ul>

## DHCP

	<ul style="list-style-type: none"> <li>◦ Remote DHCP server</li> </ul>
IPv6 Features	<ul style="list-style-type: none"> <li>• IA type - permanent, temporary, prefix delegation (PD)</li> <li>• DUID - LLT, LL, EN</li> <li>◦ DHCP relay agent</li> </ul>
Option Set Builder Types	<ul style="list-style-type: none"> <li>• Hexadecimal</li> <li>• Zero length</li> <li>• Boolean</li> <li>• 8-bit, 16-bit, and 32-bit integer</li> <li>• IPv4 and IPv6 prefix, list</li> <li>• IPv4 and IPv6 address, list</li> </ul>
Default Option List	<ul style="list-style-type: none"> <li>• Subnet mask value (1)</li> <li>• Time offset in sec from UTC (2)</li> <li>• Router addresses (3)</li> <li>• DNS server addresses (6)</li> <li>• Hostname string (12)</li> <li>• DNS name of the client (15)</li> <li>• Interface MTU size (26)</li> <li>• All subnets are local (27)</li> <li>• Broadcast address (28)</li> <li>• Perform mask discovery (29)</li> <li>• Perform router discovery (31)</li> <li>• ARP cache timeout (35)</li> <li>• Vendor specific info (43)</li> <li>• Requested IP address (50)</li> <li>• IP address lease time (51)</li> <li>• DHCP renewal (T1) time (58)</li> <li>• DHCP rebinding (T2) time (59)</li> <li>• User class information (77)</li> <li>• DHCP relay agent (82)</li> <li>• End (255)</li> <li>• IPv6 rapid commit (14)</li> <li>• IPv6 user class (15)</li> <li>• IPv6 vendor class (16)</li> <li>• IPv6 vendor specific info (17)</li> <li>• IPv6 reconfigure accept (20)</li> <li>• IPv6 agent remote ID (37)</li> <li>• IPv6 agent subscriber ID (38)</li> <li>• IPv6 agent echo request (43)</li> <li>• IPv6 custom option (99)</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• RFC 2131 Dynamic Host Configuration Protocol</li> <li>• RFC 1534 Interoperation Between DHCP and BOOTP</li> <li>• RFC 2132 DHCP Options and BOOTP Vendor Extensions</li> <li>• RFC 3046 DHCP Relay Agent Information Option</li> </ul>

## DHCP

	<ul style="list-style-type: none"> <li>• RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6).</li> <li>• RFC 3319 Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers</li> <li>• RFC 3633 IPv6 Prefix Options for DHCP version 6</li> <li>• RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</li> <li>• RFC 3736 Stateless Dynamic (DHCP) Service for IPv6</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• General Session Status</li> <li>• Discovers and Offers</li> <li>• Session Setup and Teardown rates</li> </ul>

## PPPoE

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• Initiator and Terminator</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Full PPP stack</li> <li>• Protocol support for PPPoE, PPPoEoV, PPPoEoQnQ</li> <li>• VLAN and QinQ support</li> <li>• Session control – setup and teardown rates, max outstanding</li> <li>• LCP link control, IPCP network control and NCP address control</li> <li>• DNS options including primary and secondary DNS, options</li> <li>• Domain groups used to direct access to network port traffic</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Desired MRU</li> <li>• Keep alive - enable/disable request/reply, KA interval</li> <li>• LCP configuration timeout and retries</li> <li>• NCP timers and retry counts</li> <li>• Authentication – none, CHAP, PAP with unique per user credentials</li> <li>• Service type, name</li> <li>• Access concentrator type, name, MAC</li> <li>• Redial capability with timeout</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• RFC 1661 PPP</li> <li>• RFC 2516 PPPoE</li> <li>• RFC 1332 IPCP</li> <li>• RFC 1334 PAP</li> <li>• RFC 1570 LCP Extensions</li> <li>• RFC 1994 CHAP</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• General Session Status</li> <li>• Authentication</li> <li>• Establishment and Maintenance</li> <li>• NCP IPCP</li> <li>• Latency</li> </ul>

## L2TP

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• Initiator and Terminator</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Full L2TPv2 LAC and LNS emulation stack</li> <li>• Support for L2TPoE</li> <li>• Multiple PPP sessions per L2TP tunnel</li> <li>• Session control – setup and teardown rates, max outstanding</li> <li>• DNS options including primary and secondary DNS, Options</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Control of PPP sessions per tunnel</li> <li>• Hello requests and responses</li> <li>• Bearer type and capability configuration</li> <li>• Redial capability, redial timeout</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• RFC 2661 L2TPv2</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• General Session Status</li> <li>• Authentication</li> <li>• Establishment and Maintenance</li> <li>• PPP</li> <li>• L2TP Call Mgmt and Control</li> <li>• L2TP Tunnel</li> <li>• NCP IPCP</li> <li>• Latency</li> </ul>

## 6RD

Emulation	<ul style="list-style-type: none"> <li>• Initiator and Terminator</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Emulation of CE and BR elements</li> <li>• Multiple Hosts per CE</li> <li>• Session control – ARP control</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Hosts per CE</li> <li>• 6rd Prefix</li> <li>• 6rd Prefix Length</li> <li>• IPv4 Mask Length</li> <li>• BR IPv4 IP Address</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• RFC 5969, Rapid Deployment on IPv4 Infrastructures (6rd)</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• Neighbor Discovery</li> <li>• 6rd General - Packets Sent</li> <li>• 6rd General - Packets Received</li> <li>• 6rd General - Packets Dropped</li> </ul>

## DSLite

Emulation	<ul style="list-style-type: none"><li>• Initiator and Terminator</li></ul>
Features	<ul style="list-style-type: none"><li>• Emulation of B4 and AFTR elements</li><li>• Multiple Hosts per B4</li><li>• Optional Host IP reuse across B4</li><li>• Fragmentation and Reassembly</li><li>• Session control</li><li>• DSLite Stack with a PCP Client Plug-in</li></ul>
Options	<ul style="list-style-type: none"><li>• Hosts per B4</li><li>• Host IP address</li><li>• Host IP address Increment</li><li>• AFTR IP address</li></ul>
RFC	<ul style="list-style-type: none"><li>• RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion</li></ul>
Statistics	<ul style="list-style-type: none"><li>• Neighbor Discovery</li><li>• DSLite General - Packets Sent</li><li>• DSLite General - Packets Received</li><li>• DSLite General - Packets Dropped</li><li>• DSLite General - Fragmentation</li></ul>

## IPv6 Autoconfiguration (SLAAC)

Emulation	<ul style="list-style-type: none"><li>• Initiator</li></ul>
Features	<ul style="list-style-type: none"><li>• IPv6 Stateless Address Autoconfiguration</li><li>• DHCPv6 Stateless Client</li><li>• IPv6 Neighbor Discovery</li><li>• Duplicate Address Detection (DAD)</li><li>• Session control – setup rates</li></ul>
Options	<ul style="list-style-type: none"><li>• Random Address for DAD</li><li>• Address and Increment for DAD</li></ul>
RFC	<ul style="list-style-type: none"><li>• RFC 4862, IPv6 stateless address autoconfiguration</li></ul>
Statistics	<ul style="list-style-type: none"><li>• IPv6 SLAAC Global Statistics</li><li>• IPv6 SLAAC Range Statistics</li><li>• IPv6 SLAAC Per-Session Statistics</li></ul>

## Port Control Protocol (PCP)

Emulation	<ul style="list-style-type: none"> <li>• Initiator</li> </ul>
Features	<ul style="list-style-type: none"> <li>• MAP Opcode</li> <li>• unsolicited unicast ANNOUNCE (Rx)</li> <li>• PCP Helper</li> <li>• Session control – setup rates</li> <li>• Setup and Teardown Rates – Initiation and Release Procedure Rates</li> <li>• Max Outstanding Procedures – Initiation and Release</li> <li>• Timeout and retransmission timers - Initial Retransmission Time, Retransmission Count, Retransmission Time, Retransmission Duration</li> </ul>
Options	<ul style="list-style-type: none"> <li>• PCP Server IP</li> <li>• Requested Lifetime</li> <li>• PREFER_FAILURE</li> <li>• Filter</li> <li>• Suggested External IP and Port</li> <li>• DS-Lite Mode (Encapsulated or Plain)</li> <li>• Zero Port in Delete Request</li> <li>• Don't Renew Mappings</li> <li>• Force Session Lifetime</li> <li>• Zero Third Party IP for Delete</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• pcp-draft 25, PCPv1</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• PCP General</li> <li>• PCP Rates Control</li> <li>• PCP Latency Buckets</li> <li>• PCP Error</li> <li>• PCP Per-Session</li> </ul>

## PPTP

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• PPTP Network Server (PNS)</li> <li>• PPTP Access Concentrator (PAC)</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Outgoing-Call-Request</li> <li>• Outgoing-Call-Reply</li> <li>• Session control – setup and teardown rates, max outstanding</li> <li>• LCP link control, IPCP network control and NCP address control</li> <li>• DNS options including primary and secondary DNS, options</li> <li>• Domain groups used to direct access to network port traffic</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Desired MRU</li> <li>• Keep alive - enable/disable request/reply, KA interval</li> <li>• LCP configuration timeout and retries</li> </ul>

	<ul style="list-style-type: none"> <li>• NCP timers and retry counts</li> <li>• Authentication – none, CHAP, PAP with unique per user credentials</li> <li>• Service type, name</li> <li>• Access concentrator type, name, MAC</li> <li>• Redial capability with timeout</li> </ul>
RFC	<ul style="list-style-type: none"> <li>• RFC 2637 Point-to-Point Tunneling Protocol (PPTP)RFC 1332 IPCP</li> <li>• RFC 1334 PAP</li> <li>• RFC 1570 LCP Extensions</li> <li>• RFC 1994 CHAP</li> </ul>
Statistics	<ul style="list-style-type: none"> <li>• General Session Status</li> <li>• Authentication</li> <li>• Establishment and Maintenance</li> <li>• NCP IPCP</li> <li>• Latency</li> </ul>

### 802.1x

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• 802.1x supplicant emulation with and without NAC</li> </ul>
Authentication Protocols	<ul style="list-style-type: none"> <li>• MD5, TLS, TTLS (MSHCAPv2), PEAPv0, PEAPv1, PEAPv1 + NAC (MSCHAPv2), FAST, FAST + NAC (MSCHAPv2, GTC)</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Authentication method</li> <li>• Username and password</li> <li>• Host name and password</li> <li>• Host authentication mode</li> <li>• NAC sequence</li> <li>• Setup Rate - Max Rate and Max Outstanding</li> <li>• Teardown Rate - Max Rate</li> <li>• Protocol Parameters <ul style="list-style-type: none"> <li>◦ Authentication Period</li> <li>◦ Start Period</li> <li>◦ Max Start</li> <li>◦ Successive Start</li> <li>◦ Fragment Size</li> </ul> </li> <li>• Session Parameters <ul style="list-style-type: none"> <li>◦ DUT Test Mode</li> <li>◦ Machine Auth Prefix</li> <li>◦ Authorized on No Response</li> <li>◦ Disable sending Logoff</li> <li>◦ Always use multicast</li> <li>◦ Use VLAN to identify the supplicant</li> </ul> </li> <li>• Wait Before Run</li> <li>• Certificate Options</li> </ul>

- Run-Time Certificate Generation
- Certificate Server URL
- NAC
  - Posture List
  - Application State List
  - Posture Sequence List

## EAPoUDP

IP Support	<ul style="list-style-type: none"> <li>• IPv4 and IPv6</li> </ul>
Emulation	<ul style="list-style-type: none"> <li>• Hosts attempting network access via EAPoUDP</li> </ul>
NAC Modes	<ul style="list-style-type: none"> <li>• NAC-L2-IP (switch port) also known as NAC LAN Port IP (LPIP)</li> <li>• NAC-L3-IP (router port) also known as NAC Gateway IP (GWIP)</li> </ul>
Authentication Protocols	<ul style="list-style-type: none"> <li>• PEAPv1 + NAC</li> <li>• FAST + NAC</li> </ul>
Options	<ul style="list-style-type: none"> <li>• Authentication method</li> <li>• Username</li> <li>• User password</li> <li>• Host name</li> <li>• Host password</li> <li>• Host authentication mode</li> <li>• NAC sequence</li> <li>• Setup Rate           <ul style="list-style-type: none"> <li>◦ Max Rate</li> <li>◦ Max Outstanding</li> </ul> </li> <li>• Protocol Parameters           <ul style="list-style-type: none"> <li>◦ Wait for Completion</li> <li>◦ Trigger Origin</li> <li>◦ Trigger Type</li> <li>◦ Trigger Count</li> <li>◦ Cookie Size</li> <li>◦ Timeout</li> <li>◦ Fragment Size</li> <li>◦ Port</li> <li>◦ ChangeNacResponse</li> </ul> </li> <li>• NAC           <ul style="list-style-type: none"> <li>◦ Posture List</li> <li>◦ Application State List</li> <li>◦ Posture Sequence List</li> </ul> </li> <li>• Wait Before Run</li> </ul>

## WebAuth

IP Support	<ul style="list-style-type: none"><li>• IPv4 and IPv6</li></ul>
Emulation	<ul style="list-style-type: none"><li>• Hosts attempting access to web servers</li></ul>
Features	<ul style="list-style-type: none"><li>• Emulation of host authentication through Web Authentication</li><li>• Web-based authentication supported by way of the following HTML pages<ul style="list-style-type: none"><li>◦ Login Page</li><li>◦ Success Page</li><li>◦ Login-Fail Page</li></ul></li><li>• WebAuth ARP Control – useful for IP switches that use ARP probes to determine whether a host is active on a port</li></ul>
Options	<ul style="list-style-type: none"><li>• Input values, e.g. username, password</li><li>• Expect<ul style="list-style-type: none"><li>◦ Success</li><li>◦ Failure</li></ul></li><li>• Setup Rate<ul style="list-style-type: none"><li>◦ Max Rate</li><li>◦ Enable Max Outstanding</li><li>◦ Max Outstanding</li></ul></li><li>• Protocol Parameters<ul style="list-style-type: none"><li>◦ Wait for Completion</li><li>◦ Renew DHCP After Successful Authentication</li><li>◦ Protocol Type</li><li>◦ Port Number</li><li>◦ Response Delay</li><li>◦ Number of Retries</li></ul></li><li>• URL &amp; Fields<ul style="list-style-type: none"><li>◦ Request URL</li><li>◦ Redirect Login URL</li><li>◦ Redirect Failure URL</li></ul></li><li>• Authentication<ul style="list-style-type: none"><li>◦ Success Text</li><li>◦ Failure Text</li><li>◦ Timeout</li></ul></li><li>• Policy Check<ul style="list-style-type: none"><li>◦ Perform Policy Check</li><li>◦ Success Text Timeout</li></ul></li><li>• ARP Control</li></ul>

# Platform Options

Visit [Keysight.com](https://www.keysight.com) for More Information on IxNetwork Platform Options

Virtual Platform	<ul style="list-style-type: none"><li>• IxLoad Virtual Edition (VE)</li></ul>
Public Cloud	<ul style="list-style-type: none"><li>• IxLoad on AWS</li><li>• IxLoad on Azure</li><li>• IxLoad on GCP</li><li>• IxLoad on Oracle</li></ul>
Chassis / Controller	<ul style="list-style-type: none"><li>• APS-M1010</li><li>• XGS-12 HSL/SD/SDL Chassis</li><li>• XGS-2 HSL/SD/SDL Chassis</li></ul>
Load Modules	<ul style="list-style-type: none"><li>• CloudStorm Fusion 10GE, 40GE, 25GE, &amp; 100GE</li><li>• CloudStorm 10GE, 40GE, 25GE, &amp; 100GE</li><li>• CloudStorm-XP Fusion 10GE, 40GE, 25GE, and 100GE</li><li>• CloudStorm-XP 10GE, 40GE, 25GE, and 100GE</li><li>• PerfectStorm Fusion 10/1GbE, 40GbE, &amp; 100GbE</li><li>• PerfectStorm 10/1GbE, 40GbE, &amp; 100GbE</li><li>• Novus-NP 10G/1G/100M</li><li>• Novus 10G/1G/100M</li><li>• Novus 10G/5G/2.5G/1G/100M</li></ul>
Appliances	<ul style="list-style-type: none"><li>• APS-ONE-100</li><li>• PerfectStorm ONE Fusion 10/1GE, 40GE, &amp; 100GE</li><li>• PerfectStorm ONE 10/1GE, 40GE, &amp; 100GE</li><li>• Novus ONE Appliance</li><li>• Novus ONE Plus Appliance</li></ul>

# Technology Solutions

Visit [Keysight.com](https://www.keysight.com) for More Information on IxLoad Technology Solutions

- IxLoad Overview—Converged Multiplay Service Validation
- IxLoad Virtual Edition (VE) L4-7 Application Performance Testing
- IxLoad Data Test Solution
- IxLoad Video Test Solution
- IxLoad Voice Test Solution
- IxLoad IPsec and Network Access Test Solution
- IxLoad on AWS – Cloud Application Performance Testing
- IxLoad on Azure – Cloud Application Performance Testing

# IxLoad Ordering Information

## APS-100/400GE licenses

Part Number	Description
941-0113	APS-M1010 Management Controller. Supports up to 10 x APS-ONE-100 Fusion Compute Nodes (941-0110). Note: APS-ONE-100 Compute Nodes are purchased separately.
941-0114	Ixia, APS-ONE-100, Compute Node for IxLoad with 4x100GE front I/O ports for the APS-M1010 Management Controller (941-0115). Requires 2 optional QSFP28 transceivers/cable assemblies to be ordered separately using QSFP28-SR4-XCVR (QSFP28 100GBASE-SR4 100GE pluggable optical transceiver, MMF (multimode), 850 nm, 100 m reach) or 942-0088 (QSFP28 passive, copper, Direct Attach Cable)
925-6201	Ixia, IxLoad-DATA Perpetual License Bundle for a single APS-ONE-100 appliance, floating license (per controller) (925-6201). The license enables IxLoad-DATA functionality on a single APS-ONE-100 appliance (compute node). It can be used with any single appliance managed by a management controller (APS-M1010 or APS-M8400). It includes an IxLoad Framework license and support for the DATA traffic activities (HTTP, HTTPS, DNS, AppReplay, FTP, IPSec). TAA compliance is determined by the hardware on which the license is enabled.

## Chassis licenses

Part Number	Description
925-3371	<p><b>IxLoad Multiplay-Security-2016</b>, Software Bundle, Layer 4-7 Performance Test Application Data-Video-Voice-Security package. Includes:</p> <ul style="list-style-type: none"> <li>• <b>Data:</b> Enables support for HTTP, HTTPS, TCP Session, FTP, DNS, Mail (SMTP, POP3 and IMAP), Database, SSH, RADIUS, TFTP, Application-Replay, DHCP, LDAP, Telnet, Stateless-Peer and StreamBlaster emulations.</li> <li>• <b>Video:</b> Enables support for basic RTSP, IPTV (Multicast), Video-ADVANCED (VoD), Adobe Flash Client, Apple HLS Client, Microsoft Silverlight Client, Adobe HDS Client and DASH Client emulations. Includes Video Quality VQMON engine for up to 10Gbps and TCP VQ Video quality for TCP video traffic for up to 10 Gbps.</li> <li>• <b>Voice:</b> Advanced VoIP SIP &amp; RTP, Audio Codecs, VoLTE extensions, and Bulk SIP &amp; MGCP. Includes: Voice Quality engine for up to 10Gbps, Video Quality engine for up to 10Gbps conversational video traffic.</li> <li>• <b>ADVNET:</b> Enables support for Advanced Access networking protocols such as DHCP for IP address acquisition, DHCP Server, PPP, L2TP and IPsec.</li> <li>• <b>Storage:</b> iSCSI, CIFSv1, CIFSv2 (SMB2), SMB3, NFSv3 Client, NFSv4 Client, NFS4.1 Client, Cloud Storage Client, DCBX, FCoE and FC; Note the FCoE and FC emulation is only supported on selected load modules.</li> <li>• <b>Access:</b> DHCP, PPP, L2TP, L2TP, IPsec, IPsec Performance Benchmarking QuickTest &amp; SuiteB Cryptographic, 6RD, DSLITE and IPv6 SLAAC, 8021X, NAC and WEBAUTH.</li> <li>• <b>Security:</b> Enables support for a collection of vulnerabilities and malware attacks with 1-year subscription service and DDoSv2.</li> <li>• Software Impairment.</li> </ul> <p>Note: some of the features are available only on specific load modules</p>

Part Number	Description
925-3375	<b>IxLoad-ACCESS-VPN-2016</b> , Software Bundle, Layer 4-7 Performance Test Application; Enables support for IPsec VPN testing and Advanced Access networking protocols; includes DHCP, PPP, L2TP, L2TP, IPsec, IPsec Performance Benchmarking QuickTest & SuiteB Cryptographic, support for IPv6 transition technologies like 6RD, DSLITE and IPv6 SLAAC and network authentication protocols such as 8021X, NAC and WEBAUTH to emulate the network infrastructure for the application traffic. Also includes: basic HTTP, FTP and Stateless (Stateless Peer and StreamBlaster) traffic generation. Note: some of the features are available only on specific load modules.

## Appliance licenses

Part Number	Description
925-6321	<b>IxLoad Appliance Multiplay</b> , Software Bundle, Layer 4-7 Performance Test Application. Enables Data, Storage, Voice, Video and Access & VPN on PerfectStorm ONE and Novus ONE appliances. Includes: <ul style="list-style-type: none"> <li>925-6121 IxLoad Appliance <b>DATA &amp; Storage</b></li> <li>925-6112 IxLoad Appliance <b>VIDEO</b></li> <li>925-6113 IxLoad Appliance <b>VOICE</b></li> <li>925-6117 IxLoad Appliance <b>ACCESS &amp; VPN</b></li> </ul>
925-6117	<b>IxLoad Appliance ACCESS + VPN</b> , Software, Layer 4-7 Performance Test Application. Enables IxLoad Access and VPN functionality on PerfectStorm ONE and Novus ONE appliances. Includes: 925-6104 IxLoad Appliance BASIC (HTTP, HTTPS, DNS, ADVNET-DHCP, Stateless Peer) IPsec, IPsec SUITES B, IPsec Quick Tests, PPP, L2TP, L2TP/IPsec IPv6 Transitioning: SLAAC, 6rd, DSLite ADVNET: DHCP, DHCPv6 (client & server), RADIUS; Includes: ADVNET-802.1X, ADVNET-NAC, ADVNET-WEBAUTH. Requires IxLoad Framework, 925-0001, which is free with adjoining software purchase.

## Virtual edition licenses

See the [IxLoad Virtual Edition \(VE\) Virtualized Multiplay Services Testing datasheet](#) for the IxLoad-VE licenses.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at [www.keysight.com](http://www.keysight.com).



This information is subject to change without notice. © Keysight Technologies, 2019 – 2024, Published in USA, December 14, 2024, 3120-1164.EN