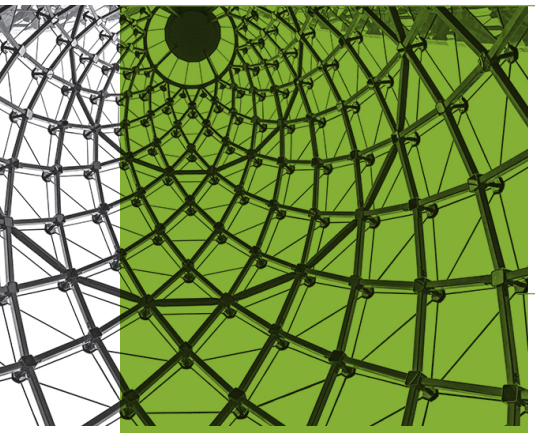

# JUNIPER PARAGON ACTIVE ASSURANCE

## Product Overview

*The transition to hybrid virtual/physical networks and service chains introduces new points of failure. Traditional service assurance techniques, which collect counters and telemetry data from devices in the infrastructure, are not designed to determine whether a service is properly working from the end user's perspective. Furthermore, traditional assurance solutions have limitations in helping service operations centers (SOCs) assess the real customer experience over the lifetime of the service. With Paragon Active Assurance, customer-facing teams can automate turn-up testing processes and gain continuous end-to-end service quality insights to proactively enhance the customer experience.*

## Product Description

Juniper® Paragon Active Assurance (formerly known as Netrounds) is a programmable, active test and service assurance platform for physical, hybrid, and virtual networks. Unlike passive test and assurance approaches, Paragon Active Assurance uses active, synthetic traffic to verify application and service paths at the time of delivery and throughout the life of the service.

Service delivery teams leverage Paragon Active Assurance to verify new service deployments and changes. Paragon Active Assurance verifies and ensures that services are configured correctly the first time. It also validates service changes to make sure they do not impact service performance. By automating initial service verification and testing, service delivery teams reduce time to revenue, lower operating expenses associated with service delivery, and reduce failed service delivery rates.

Network operations teams use Paragon Active Assurance to identify, understand, troubleshoot, and resolve issues before customers notice them. The visibility into service performance provided by Paragon Active Assurance reduces incident resolution times by as much as 50%, resulting in greater customer satisfaction and retention.

Paragon Active Assurance provides a fully integrated solution for multilayer, multidomain service life-cycle management, letting you verify that each provisioned service works when delivered and continues working throughout its lifetime. It also reduces manual efforts through automation, significantly decreasing operational costs and improving operating margins.

## Architecture and Key Components

Leveraging a virtual, cloud-ready platform, Paragon Active Assurance is easy to deploy and adopt, enabling you to start small and scale as your business needs grow.

The core component of Paragon Active Assurance is a cloud-ready multitenant Control Center, which provides a user-friendly Web portal GUI where operations staff can run on-demand tests and view real-time and aggregated results as well as key performance indicators (KPIs) and service-level agreement (SLA) monitoring metrics. The Control Center includes a feature-rich cloud API allowing external operations support systems (OSS) and Network Functions Virtualization (NFV) orchestrators to easily automate distributed activation tests or monitoring scenarios.

The Control Center remotely controls Paragon Active Assurance software-based and traffic-generating Test Agents, which provide distributed measurement metrics for service activation testing, quality monitoring, and troubleshooting. It also displays detailed, real-time results and statistics actively measured by the Test Agents and reflector streams across multiple applications, services, and interfaces. Test Agent capabilities include service activation (Y.1564, MEF 48), network performance (UDP, TCP, Y.1731, TWAMP, path trace), Internet performance (HTTP, DNS), rich media (IPTV,OTT video, VoIP telephony, and SIP), as well as support for controlling Wi-Fi interfaces, and performing remote packet inspection.

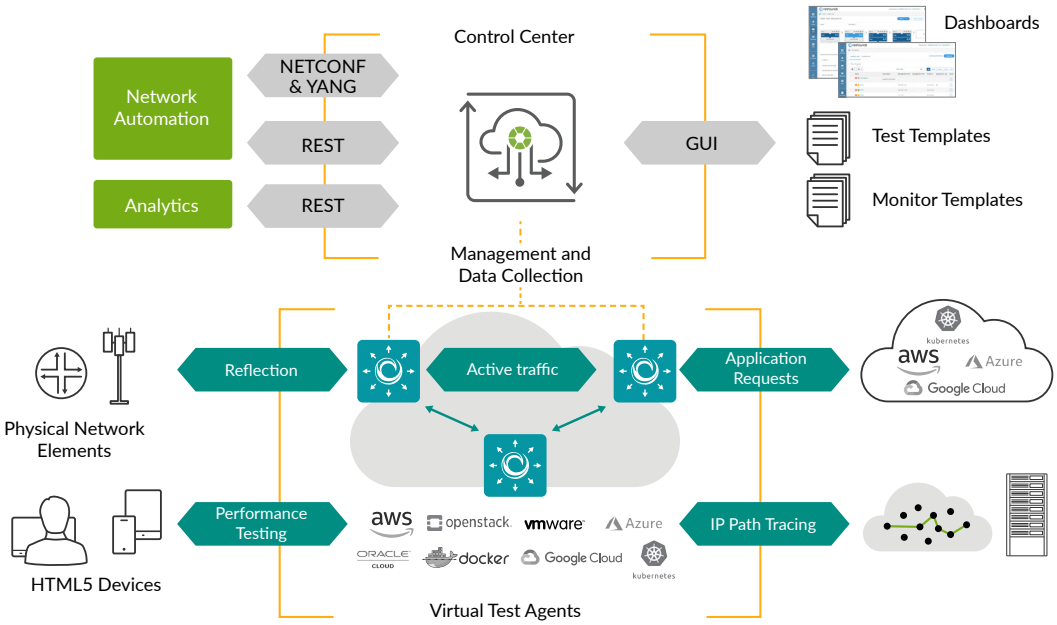


*Figure 1: Paragon Active Assurance architecture*

Test Agents may be placed in strategic locations across your network for continuous quality monitoring. They may also be installed on demand for more temporary purposes, such as activation testing of newly deployed services. Test Agents are available in several formats: as software to be run as a virtual machine on a hypervisor, as a container application, or as a software appliance for installation on dedicated x86 hardware.

## Key Capabilities

### Real-Time Aggregated Views of Monitoring and Tests

Paragon Active Assurance calculates and visualizes errored seconds (ES) and SLA compliance indicators. Aggregated result views show large numbers of distributed active measurements. Measured data can be presented down to 1 second resolution, with an historical timespan adjustable from the last 15 minutes to years in the past.

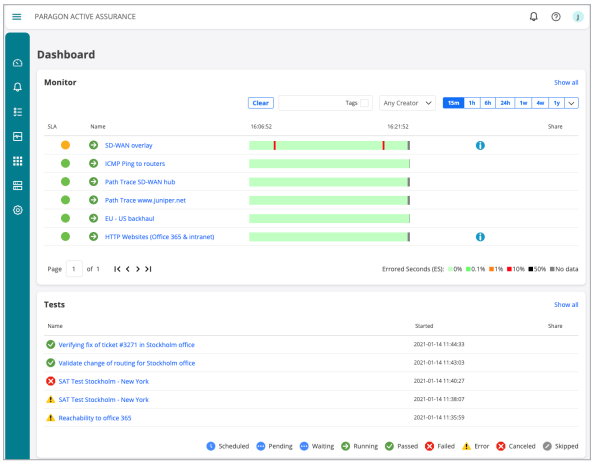


*Figure 2: Real-time aggregated views of monitoring and tests*

### Periodic Reports and Alarm Generation

SLA compliance is presented for each quality monitoring scenario and periodic test in comprehensive and configurable reports. These reports can be scheduled and e-mailed to stakeholders at custom intervals, or they can be retrieved programmatically through the Control Center's API. Alarms with multiple severity levels (critical, major, minor, warning) can be sent as SNMP traps.

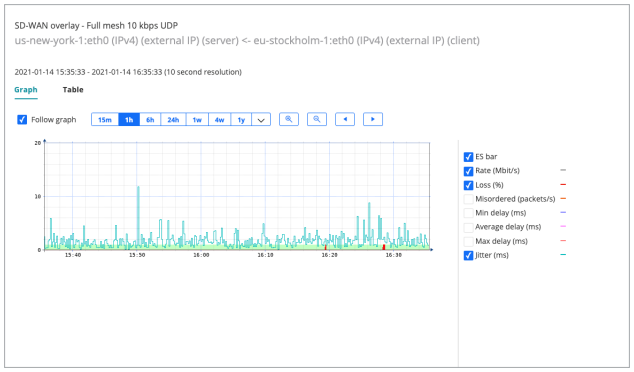


*Figure 3: SLA monitoring*

### Dynamic Test Agent Inventory

Test Agents automatically discover and register Control Center login servers. Test Agents appear as resources in the inventory once launched by the NFV orchestrator or OSS, or connected physically to the network.

Test Agents can be tagged for simple grouping and structuring. Test Agent interfaces can be configured remotely from the Control Center.

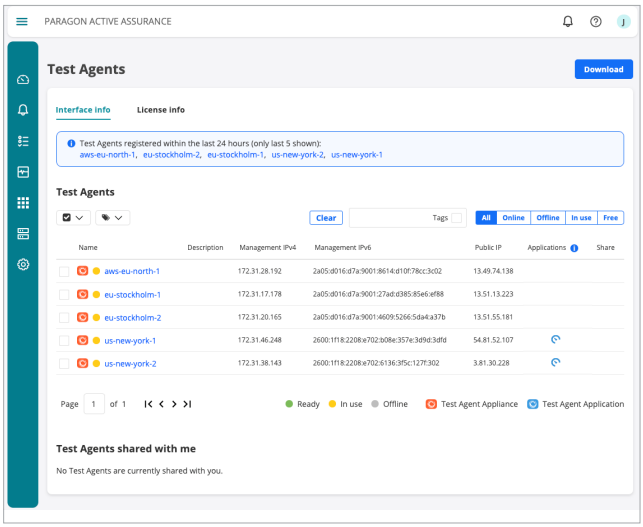


*Figure 4: Inventory of Tests Agents registered with the Control Center*

### Builder GUI for Scenarios and Templates

The Paragon Active Assurance Web GUI has an intuitive test sequence builder which can be used in the service design process. SLA compliance thresholds can be set for each monitoring scenario.

Test building blocks can be saved as reusable templates, where parameters can be left to be defined at runtime. Tests and monitoring sessions can be triggered by the OSS through APIs.

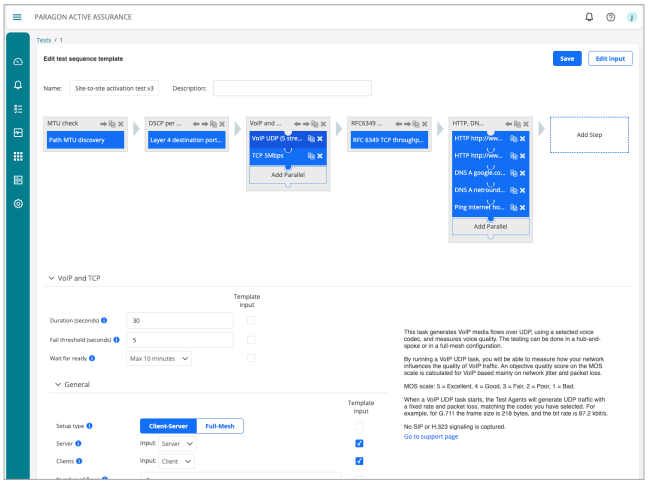


*Figure 5: Test Templates Builder*

### Sharing and Collaboration

Test and monitoring scenarios and templates, active Test Agents, and all test results and reports obtained can be freely shared among users in the same multitenant Control Center.

## Key Benefits of Paragon Active Assurance

Paragon Active Assurance offers the following benefits:

- Integrated, dynamic solution for full multilayer, multidomain service life-cycle management—Combined service activation testing, quality monitoring, and troubleshooting provide fully orchestrated assurance.
- Virtualized and cloud-ready—Flexible deployment and elastic scaling on all major modern virtualization platforms allows you to start small and scale.
- Easy to get started—Software-only and hosted components allow for smooth introduction, enable immediate use, and bring instant value.
- Automation through well-documented complete API—Simple integration of fulfillment and assurance workflows eliminates manual work and reduces cost of complex integration.

## Features and Benefits

### Control Center

The Control Center is either hosted by Juniper Networks and offered as a Software as a Service (SaaS) solution or deployed on premises in a private cloud. In either case, it displays both second-by-second and aggregated real-time results, as well as KPIs and SLA monitoring metrics.

Table 1. Features and Benefits of Control Center

| Feature | Benefit |
|---|---|
| Feature-rich cloud API for distributed on-demand tests and live monitoring of end-user KPIs | Enables closed-loop, fully automated workflow by providing KPIs of actual end-user experience to service orchestrators/OSS |
| Centralized storage and aggregation of test results and SLA monitoring metrics | Allows effortless handling of hundreds or even thousands of concurrent measurements across your network |
| Web portal for creation and initiation of test scenarios and automation templates | Supports design time and runtime dynamic test processes, as well as remote troubleshooting |
| Real-time KPIs, dashboards, and drill-down charts | Provides real-time actionable insights into how your network and services perform from a customer perspective |
| Centralized and dynamic inventory of distributed, traffic-generating Test Agents | Presents a consolidated user interface for all Test Agents—no need to manage Test Agents individually |
| Remote updates of Test Agent software | Reduces maintenance costs with remote and automated updates, keeping your Test Agents up to date |

The Control Center has a wide range of built-in core features that are exposed over either an intuitive Web portal user interface or a complete read/write API. The Web portal is used for test design, on-demand initiation of tests, remote troubleshooting, and real-time reconfiguration of service assurance scenarios and thresholds. The API is used by external systems such as OSS and NFV orchestrators to dynamically launch new Test Agents and initiate activation tests and quality monitoring scenarios.

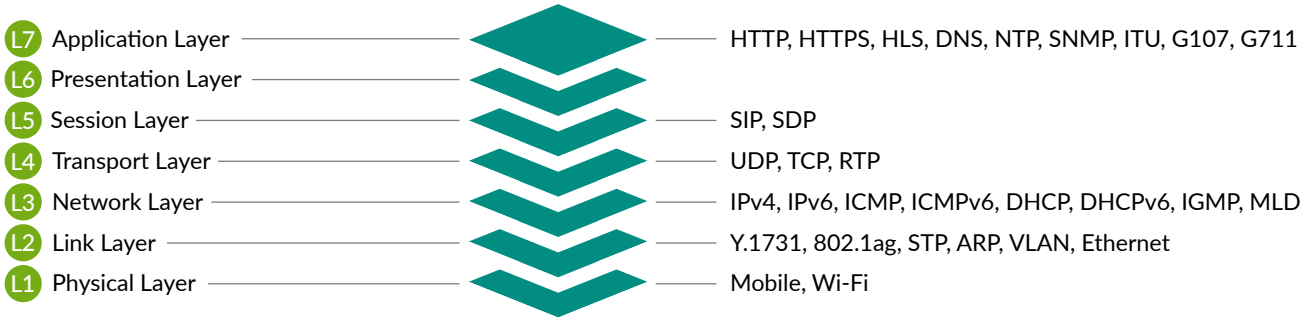


*Figure 6: Supported protocols by OSI layer*

The Control Center can be made available in two ways—hosted in the Amazon AWS public cloud infrastructure or installed on premises or as a private cloud solution. Both deployment options share the same core features, Web portal, and API.

### Test Agents

Test Agents actively generate authentic traffic and analyze detailed, real-time measurements across multiple applications, services, and interfaces. Test Agent capabilities include measurement of network performance (UDP, TCP, Y.1731, TWAMP), IPTV and over-the-top (OTT) video, and Internet (HTTP, Ping, HTML5 Performance Tests), as well as VoIP and Session Initiation Protocol (SIP) telephony, mobile radio, Wi-Fi, and remote packet inspection.

All Test Agents are controlled and updated remotely through the Control Center. The Control Center in turn can be accessed through a Web GUI or through a cloud API.

External OSS and NFV orchestrators easily automate distributed activation tests and quality monitoring through a feature-rich cloud API to the Control Center. Network operations staff access the user-friendly Web interface as a test design environment, as well as for on-demand tests, quality monitoring, and real-time visualizations.

Table 2. Features and Benefits of Test Agents

| Feature | Benefit |
|---|---|
| **Genuinely software-based** | Suitable for both virtualized and traditional networks |
| **Instant remote Test Agent deployment** | No need for field efforts using expensive hardware tools |
| **Traffic generating capabilities** | Activation tests, quality monitoring, and remote troubleshooting from the end-user perspective |
| **Versatile features and tools** | Complete system for assessing end-user experience |
| **Centrally managed** | Consistent interface and back-end for users and orchestrators |

## Product Options

**Hosted**: The Control Center is hosted in the Amazon AWS public cloud infrastructure and managed by Juniper Networks. This solution scales transparently and elastically with the number of Test Agents deployed; there is no need for any involvement from you as a Juniper Networks customer. The server software and the repository of Test Agent software are always kept up to date.

**On Premises**: The Control Center is deployed on premises in your own data center environment, either on bare-metal servers or on existing private cloud infrastructure, and is managed either by your organization or by Juniper Networks as a managed service.

| Hosted Option | On-Premises Option |
|---|---|
| Deployed as a securely hosted SaaS solution in the Amazon AWS public cloud infrastructure | Installed on premises in private cloud infrastructure or private data centers |
| Offers a flexible subscription business model | Offered as licensed software |
| Operated and managed by Juniper Networks as part of the subscription agreement | Operated and managed by Juniper Networks as a service or managed by Juniper customer |
| Scales from single Test Agent deployments to nationwide or multinational rollouts | Starts at deployments of 10+ Test Agents to nationwide or multinational rollouts |
| Subscriptions correspond to one individual tenant account in the hosted, multitenant Control Center | Dedicated multitenant solution with individual dashboards for the service provider and their enterprise customers |
| Frequent updates for Control Center software, as well as for repository of software for all Test Agent types | Update frequency determined by customer for Control Center, as well as for repository of software for all Test Agent types |
| User authentication handled by Control Center | User authentication can optionally be done against an LDAP or TACACS+ server |

# Specifications

## Control Center Interfaces

| Interface | Description |
|---|---|
| Northbound user interface towards operations staff | Browser GUI towards Web portal<br>• Native HTML with JavaScript<br>• HTTPS for secure access to Web portal<br>• Support for all common Web browsers: Chrome, Firefox, Internet Explorer, Opera, and Safari<br>• Mobile browser support<br>• HTTP basic authentication<br>• Multi-user support with different user levels and credentials |
| Northbound API towards OSS and NFV orchestrators | REST<br>• Follows REST API best practices<br>• Web browsable; extensive documentation<br>NETCONF and YANG<br>• Support for service modeling with YANG<br>• Network Configuration Protocol (NETCONF) supported for mapping YANG specifications onto easy-to-use interfaces |
| Southbound interfaces for remote control and configuration towards active Test Agents | Test Agents<br>• Firewall-friendly communication, initiated by Test Agents towards Control Center<br>• Local storage on Test Agent in case Control Center is temporarily unreachable<br>• Secure control protocol using SSL between Control Center and Test Agents |

## Test Agent Types

Test Agents come in two main varieties: Test Agent Software Appliance and Test Agent Application.

## Test Agent Software Appliance

The Test Agent Software Appliance is integrated with an optimized Debian Linux OS. The appliance can be packaged and delivered in a number of ways:

- **Dedicated Test Agent**—Test Agent Software Appliance is downloaded by the customer and installed on customer-provided x86 hardware.
- **Test Agent Virtualized Network Function (TA VNF)**—Test Agent image is downloaded by the customer and run as a virtual machine (VM) on a hypervisor.

These options have identical traffic-generating capabilities and differ only in terms of packet performance, which is determined by available CPU resources and interface speeds.

## Test Agent Application

The Test Agent Application consists of software and can be packaged and delivered in two ways:

- **Test Agent Application**—Consists of software downloaded by the customer and is installed as an application on a Linux machine.
- **Test Agent Cloud-Native Network Function (TA CNF)**—The Test Agent Application can optionally run as a container in any environment that supports it. The containerized application is in a position to approximate very closely the performance of other applications running on the same virtual machine.

## Test Agent Software Appliance—Downloadable Software for Standard x86 Hardware

| | HDD | Bootable USB |
|---|---|---|
| Usage | Permanent installation on physical block storage device (HDD) | Live booting from USB memory stick for temporary transformation of any x86 PC hardware into a Test Agent |
| Delivery format | Delivered as installation ISO image | Delivered as raw disk image |
| RAM requirement | 256 MB minimum; 512 MB recommended | |
| Storage requirement | 1 GB | None; RAM disk used for temporary storage, and image is booted directly from USB device |
| Recommended network interface cards (NICs) | Intel NICs recommended | |
| NIC driver support | Same as supported by Linux Debian | |

### Test Agent Virtual Network Function—Downloadable Software for Hypervisors

Below is a comparison of the various Test Agent virtualized network function (TA VNF) formats.

| | Test Agent VNF Delivery Format | | | | |
|---|---|---|---|---|---|
| | Raw/Qcow2 | Open Virtualization Format (OVF)/Virtual Machine Disk (VMDK) | Amazon Machine Image (AMI) | Virtual Hard Disk (VHD) | Google Cloud Platform (GCP) |
| **Type** | Preinstalled and bootable appliance | | | | |
| **Delivery format** | Raw or Qcow2 disk image | VMDK disk image plus OVF file | AMI | VHD disk image | GCP image |
| **Orchestration support** | OpenStack Heat Orchestration Templates (HOT) using cloud-init | VMware vCloud Director, VMware Integrated Open-Stack (VIO) | AWS CloudFormation templates | Azure ARM templates | Google Deployment Manager |
| **Hypervisor support** | KVM | VMware vSphere | Xen | Azure Hypervisor | Google Cloud Platform |
| **Example platforms** | OpenStack | | | | |
| **Download image size** | 900 MB | 287 MB | 2 GB | 2 GB | 2 GB |
| **Minimum machine type requirement** | Minimum: 1vCPU / 256 MB<br>Recommended: 2vCPU / 4 GB | Minimum: 1vCPU / 256 MB<br>Recommended: 2vCPU / 4 GB | Minimum: t3.nano<br>Recommended: c5.large | Minimum: B1ms<br>Recommended: D2 | Minimum: f1-micro<br>Recommended: n1-standard-2 |
| **RAM and storage requirements** | RAM: 256 MB minimum; 512 MB recommended<br>Storage: 2 GB | | | | |
| **SR-IOV, PCI pass through** | Not required, but could improve accuracy and performance | | | | |
| **NIC driver support** | Same as supported by Linux Debian | Same as supported by Linux Debian and VMware tools | Same as supported by Linux Debian | Same as supported by Linux Debian | Same as supported by Linux Debian |

### Test Agent Application—Linux Application and Cloud-Native Network Function (CNF)

Below is a comparison of the Test Agent Application deployed as a Linux application and the same entity deployed as a container (CNF).

| | Test Agent Application | Test Agent CNF |
|---|---|---|
| **Type** | x86-64 Linux application | x86-64 container |
| **Delivery format** | tar.gz package | Docker Hub or tar.gz package |
| **Orchestration support** | Application arguments | Kubernetes |
| **Hypervisor support** | N/A | Docker |
| **Example platforms** | N/A | AWS, GCP, Azure |
| **Download size** | < 10 MB | < 100 MB |
| **RAM and storage requirements** | RAM: 128 MB<br>Storage: 10 MB | RAM: 128 MB<br>Storage: 100 MB |
| **SR-IOV, PCI pass through** | N/A<br>(uses host OS networking stack) | |
| **NIC driver support** | N/A<br>(uses host OS drivers) | |

# Test Agent Functionality

## General Network Support

| Technology | Test Functionality |
|---|---|
| Transport modes | Bridged Ethernet<br>IEEE 802.1q VLAN<br>IPv4 over Ethernet<br>IPv6 over Ethernet |
| Physical link configuration | Duplex setting (full or half)<br>Speed setting (10 Mbps-10 Gbps)<br>MTU size (64-9000 bytes) |
| Media access control (MAC) addresses | Per physical port or VLAN<br>Factory default<br>User-defined |
| Bridge setup | Bridge physical ports and/or VLANs<br>Multiple bridges (maximum 4 per Test Agent)<br>IP hosts assigned to bridges |
| VLAN setup | Per physical port (maximum 125 per Test Agent)<br>Full VLAN range (1-4095)<br>Priority code point (0-7) |
| IP host setup | Multi-host (maximum 125 per Test Agent), one host per physical port or VLAN<br>Separate routing tables per host<br>DiffServ code point (0–63)<br>Static addressing (gateway, DNS)<br>DHCPv4, DHCPv6, stateless address autoconfiguration (SLAAC)<br>DHCPv4 vendor class<br>Use of IP host for management |
| DHCPv4 server setup | DHCPv4 server for other clients<br>Per physical port or VLAN<br>Network range<br>Network prefix length<br>Gateway and Domain Name System (DNS) |
| Interface status | Per physical port or VLAN<br>Current speed/duplex<br>Current MAC and IP address<br>TX and RX packets<br>TX and RX bytes |

## Supported Standards by OSI Layer

| Technology | Test Functionality |
|---|---|
| L1—Physical Layer (dedicated Test Agents Software Appliance) | IEEE 803.2i: 10BASE-T<br>IEEE 802.3u/x: 100BASE-TX<br>IEEE 802.3ab: 1000BASE-T<br>IEEE 802.3ae: 10GBASE-SR/LR<br>IEEE 802.3ac: 1522 byte "Q-tag"<br>IEEE 802.11g/n/ac: Wi-Fi/Wireless LAN<br>ETSI/3GPP: GPRS/EDGE/UMTS/LTE |
| L2—Link Layer | RFC 826: Address Resolution Protocol (ARP)<br>IEEE 802.1q: VLAN<br>IEEE 802.1p: Protocol for Traffic Prioritization<br>IEEE 802.1ad: QinQ, VLAN Stacking<br>IEEE 802.1ag: Ethernet Loopback<br>RFC 2131: Dynamic Host Configuration Protocol, DHCP<br>RFC 3046: DHCP Relay Agent Information Option<br>ITU-T Y.1731: OAM Functions and Mechanisms for Ethernet-based Networks<br>ITU-T Y.1564: Ethernet Service Activation Test Methodology<br>MEF 6.1.1: Layer 2 Control Protocol Handling |
| L3—Network Layer | RFC 791: IPv4<br>RFC 2460: IPv6<br>RFC 792: ICMP<br>RFC 2236: Internet Group Management Protocol, Version 2<br>RFC 3376: Internet Group Management Protocol, Version 3<br>RFC 5481: Packet Delay Variation Applicability Statement<br>RFC 3393: IP Packet Delay Variation Metric for IP Performance Metrics<br>RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers<br>RFC 2680: One-way Loss Ratio<br>RFC 2679: Minimum One-way Delay<br>RFC 6703: Mean One-way Delay (section 5.2)<br>RFC 5357: A Two-Way Active Measurement Protocol (TWAMP)—Full and Light |
| L4—Transport Layer | RFC 736: User Datagram Protocol (UDP)<br>RFC 793: Transmission Control Protocol (TCP)<br>RFC 3550: RTP: A Transport Protocol for Real-Time Applications |
| L5—Session Layer | RFC 3261: SIP: Session Initiation Protocol<br>RFC 3551: RTP Profile for Audio and Video Conferences with Minimal Control<br>RFC 3266: SDP: Session Description Protocol<br>RFC 3264: An Offer/Answer Model with the Session Description Protocol (SDP)<br>RFC 3515: The Session Initiation Protocol (SIP) Refer Method<br>RFC 3891: The Session Initiation Protocol (SIP) "Replaces" Header<br>RFC 5216: The EAP-TLS Authentication Protocol (Extensible Authentication Protocol—Transport Layer Security)<br>RFC 5281: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)<br>PEAPv0/EAP-MSCHAPv2: Protected EAP |
| L7—Application Layer | ITU-T G.711: Pulse Code Modulation (PCM) of Voice Frequencies<br>RFC 1901, 1908, and 2570: SNMP v2 and v3<br>ITU G.107: The E-model: A Computational Model for Use in Transmission Planning<br>ETSI TR 101 290: Digital Video Broadcasting (DVB); Measurement Guidelines for DVB Systems<br>RFC 6959: Source Address Validation Improvement (SAVI) Threat Scope<br>RFC 7230: Hypertext Transfer Protocol—HTTP/1.1<br>RFC 1305: Network Time Protocol (Version 3)<br>RFC 1034: Domain Name System |

## Internet Performance Measurement

| Technology | Test Functionality |
|---|---|
| General | Request/response-based<br>One-armed (single Test Agent)<br>Distributed (multiple Test Agents) |
| HTTP | HTTP server (URL target)<br>Time between requests<br>Response code validation<br>Response content validation<br>Time to first byte received<br>Page load times<br>Download rates |
| DNS | DNS server<br>Lookup address<br>Time between requests<br>DNS record type response validation (A, AAAA, CNAME, MX)<br>Response time measurement |
| ICMP (Ping) | IP hosts (targets)<br>Time between requests<br>Payload size (64-9000 bytes)<br>DiffServ code point (DSCP) prioritization<br>Time-to-live<br>Hop-by-hop detection of IP hosts |
| HTML5 Performance Tests | Test Agent as HTML5 performance test responder<br>Tests initiated from browsers<br>Test duration<br>TCP port<br>Number of concurrent TCP sessions<br>Access control through IP filters |

## Network Performance Measurement

| Technology | Test Functionality |
|---|---|
| General | Test Agent to Test Agent traffic generation<br>Point-to-point<br>Hub and spoke<br>Custom mesh topologies<br>Destination port (UDP and TCP)<br>Unidirectional or bidirectional<br>Configurable rate (Mbit/s)<br>DSCP and PCP header marking |
| UDP | Unicast or multicast<br>Generated output bandwidth<br>Packet size (64-9000 bytes) |
| VoIP-like UDP | MOS scoring (1-5)<br>20 concurrent calls per Test Agent<br>Codec emulation: G.711, G.723, G.729, GSM-EFR<br>Media transport generation, not signaling |
| Stateful TCP | Number of point-to-point sessions<br>Output rate limitation for each direction |
| Multi-session TCP | Number of point-to-point TCP sessions |
| TCP throughput testing | RFC 6349: Framework for TCP Throughput Testing |
| Quality of Service (QoS) policy profiling | Multi-stream generation in each queue<br>Mix of UDP and TCP to measure queue build-up<br>Profile generated for each traffic stream |
| Y.1731/802.1ag | ITU-T Y.1731 Ethernet Loopback, ETH-LB<br>ITU-T Y.1731 Delay Measurement, ETH-DM<br>ITU-T Y.1731 Synthetic Loss Measurement, ETH-SLM<br>Participating maintenance association end points (MEPs) as input list<br>Maintenance group entity (MEG) level (0-7)<br>Unavailable Seconds (UAS) per ITU-T Y.1563<br>Packet size (64-9018 bytes) |
| TCP throughput testing | RFC 6349: Framework for TCP Throughput Testing |
| QoS policy profiling | Multi-stream generation in each queue<br>Mix of UDP and TCP to measure queue build-up<br>Profile generated for each traffic stream |
| Y.1731/802.1ag | ITU-T Y.1731 Ethernet Loopback, ETH-LB<br>ITU-T Y.1731 Delay Measurement, ETH-DM<br>ITU-T Y.1731 Synthetic Loss Measurement, ETH-SLM<br>Participating MEPs as input list<br>MEG level (0-7)<br>UAS per ITU-T Y.1563<br>Packet size (64-9018 bytes) |
| TWAMP | RFC 5357: Two-way Active Measurement Protocol<br>TWAMP Light (RFC 5357 App. I)<br>UAS per ITU-T Y.1563<br>Packet size (87-9018 bytes)<br>Hardware timestamping |
| UDP loopback | Reflector device configured to loop back UDP packets in hardware<br>Very high throughput achievable |
| BWPing | Bandwidth and response times measured between Test Agent and router/switch<br>Uses Internet Control Message Protocol (ICMP) echo request/reply mechanism<br>Achieves high data throughput |
| Path trace | ICMP and/or UDP echo packets sent with increasing time to live (TTL)<br>Measures delay, jitter, and loss for each hop<br>Continuous detection of network paths |

## IPTV and HTTP Streaming Video

| Technology | Test Functionality |
|---|---|
| General | Request/response-based<br>Emulate single client (one Test Agent)<br>Distributed (multiple Test Agents)<br>Inline with traffic (interception) |
| IPTV Moving Picture Experts Group (MPEG) | Joining of multicast channels<br>Test Agents and input channels selection<br>MPEG transport stream analysis<br>MPEG loss (continuity counter)<br>Peak cell rate (PCR) and real-time polling (RTP) packet jitter<br>Table errors (PAT and PMT)<br>Missing PID detection |
| IPTV MPEG inline | Interception of Internet Group Management Protocol (IGMP) pass through<br>Stream analysis of MPEG transport stream |

| Technology | Test Functionality |
|---|---|
| IGMP channel zapping time | Continuous join and leave cycle<br>Selection of channels to cycle<br>Join and leave delay measurements |
| HTTP video streaming (OTT) | Apple HTTP Live Streaming (HLS)<br>URL input for source of video<br>Detection of buffer underrun<br>Loop feature for static videos |
| IGMP join/leave test | Checks if users can join and receive data on allowed multicast channels (and no others) |
| Multicast group limit test | Checks that a user can only join a specified maximum number of multicast channels |

## VoIP and SIP Telephony

| Technology | Test Functionality |
|---|---|
| General | Hub and spoke<br>Point-to-point<br>SIP account inventory |
| SIP signaling | Registration and un-registration<br>Invite and hang up<br>Cycle length |
| RTP media stream quality | MOS scoring (1-5)<br>Rate<br>Packet loss<br>Packet misorderings<br>Voice codec (G.711 A-law, G.711 μ-law, GSM) |

## Remote Packet Inspection

| Technology | Test Functionality |
|---|---|
| General | Packets intercepted remotely from Test Agents<br>Standard "tcpdump" filters<br>Standard "pcap" files |
| Direct packet capture | Filtered packets forwarded from individual Test Agent to local Wireshark application |
| Packet capture through server | Filtered packets forwarded from group of Test Agents to Control Center for storage and centralized retrieval |

## Transparency

| Technology | Test Functionality |
|---|---|
| General | Packet mangling and network transparency/QoS tests |
| L2 transparency—Ethertypes | Layer 2 transparency for various Ethertypes and logical link control (LLC)/Subnetwork Access Protocol (SNAP) |
| L2 transparency—Custom Ethertype | Checks that specified Ethertype passes through network |
| L2 transparency—VLAN | Verifies transparency for given VLAN tag, VLAN priority (PCP), and DSCP |
| L2 transparency—Custom VLAN | Checks that packets with given VLAN tag and priority (PCP) are not modified by network |
| L2 transparency—Ethernet control protocols | Checks transparency for Link Aggregation Control Protocol (LACP), Extensible Authentication Protocol over LAN (EAPoL), and Multiple VLAN Registration Protocol (MVRP) |
| L2 transparency—IP | Verifies IPv4 header integrity as well as IP multicast, checking that IP packets are not dropped |
| L2 transparency—IPv6 | Verifies IPv6 header integrity |
| L2 transparency—MAC address limit | Checks that number of MAC addresses is between a given minimum and maximum |
| L2 transparency—multicast | Verifies that multicast packets are not dropped (STP and MPLS protocols) |
| DSCP remapping | Verifies expected remapping of DSCP values between two points in a network |
| Layer 4 destination port DSCP remapping | Same as preceding but with specific UDP or TCP destination ports indicated |
| Path MTU discovery | Determines path maximum transmission unit (MTU) between two Test Agents |

## Security

| Technology | Test Functionality |
|---|---|
| General | Tests primarily designed for Layer 3 networks<br>Focused on: man-in-the-middle (MITM) attacks; denial-of-service (DoS) attacks; abuse-tracking of end users<br>Test Agent acting as either customer or ISP |
| DHCP starvation | Checks that a customer can only obtain a limited number of IPv4 addresses |
| Fragmented DHCP packets | Checks that switch drops fragmented DHCP packets before they reach the control plane |
| Fragmented TCP/UDP headers | Checks that switch drops IPv4 and IPv6 packets with fragmented TCP or UDP headers |
| Management protocol scanning | Checks that management protocols are unavailable at customer ports |
| Router redundancy protocol listening | Checks that Virtual Router Redundancy Protocol (VRRP)/Common Address Redundancy Protocol (CARP), Gateway Load-Balancing Protocol (GLBP), and Hot Standby Routing Protocol (HSRP) are unavailable at customer ports |
| Routing protocols | Checks that routing protocols are not available on customer ports |
| Spanning Tree Protocol (STP) | Checks that STP is not available on customer ports |

## Wi-Fi

| Technology | Test Functionality |
|---|---|
| General | Uses Intel Wi-Fi NIC (IEEE 802.11g/n/ac) if available on the host platform<br>Measurement and logging of basic Wi-Fi metrics<br>Network and access point switching capability |
| Wi-Fi switcher | Configuration of MAC address, MTU, SSID, BSSID, type of authentication and cipher<br>802.11n (High Throughput): enable/disable; 40 MHz channels: enable/disable; Miscellaneous Control Subsystem (MCS) indexes allowed<br>802.11ac (Very High Throughput): enable/disable; MCS indexes allowed; maximum number of MIMO spatial streams<br>Frequency bands—2.4 GHz, 5 GHz: enable/disable<br>Short Guard Interval (SGI): on/off<br>Low Density Parity Check (LDPC): on/off |
| Wi-Fi logger | Received signal strength indicator (RSSI)<br>TX bitrate, RX bitrate (theoretical maximum)<br>TX and RX MCS indexes used<br>Guard interval used<br>Number of TX and RX MIMO streams<br>TX retries |

## Ordering Information

Please contact your Juniper Networks sales representative for ordering information.

## About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
**Phone: 888.JUNIPER (888.586.4737)**
**or +1.408.745.2000**
**www.juniper.net**

**APAC and EMEA Headquarters**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
**Phone: +31.0.207.125.700**