

Hawkeye

Release 6.0.7

User Guide

Notices

Copyright Notice

© Keysight Technologies 2016–2025

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly,

Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting us

Keysight headquarters

1400 Fountaingrove Parkway
 Santa Rosa, CA 95403-1738
 Email address: support@keysight.com

Support

Location	Phone number	Local time
<i>Americas</i>		
US, Canada	1-888-829-5558	8h00 – 17h00
Brazil	0800-892-0522	8h00 – 17h00
Mexico	001-888-829-5558	8h00 – 17h00
Other	+1-719-273-6516	8h00 – 17h00
<i>EMEA</i>		
Belgium	0800-18686	8h30 – 17h30
Finland	0800-913-352	8h30 – 17h30
France	0800-917228	8h30 – 17h30
Germany	0800-0824099	8h30 – 17h30
India	1800-18-02552	8h30 – 17h30
Ireland	1800-949245	8h30 – 17h30
Israel	1-809-454975	8h30 – 17h30
Italy	0800-790571	8h30 – 17h30
Luxembourg	0800-25112	8h30 – 17h30
Netherlands	0800-022-9086	8h30 – 17h30

Romania	0213 015 699	8h30 – 17h30
Spain	800-654386	8h30 – 17h30
Sweden	0201-202266	8h30 – 17h30
United Kingdom	0800-0293882	8h30 – 17h30
<i>Asia and Australia</i>		
Australia	1-800-370-558	8h30 – 17h00
China Mainland	800-810-0005	8h30 – 17h30
	400-810-0005	8h30 – 17h30
Hong Kong	800-931-613	9h00 – 18h00
Japan	0120-421-621	9h00 – 17h30
Malaysia	1800-819 092	8h30 – 17h30
South Korea	080-770-0800	8h30 – 17h30
Singapore	800-101-3797	8h30 – 17h30
Taiwan	0800-699-880	9h00 – 18h00
Other	+65 6215 7600	8h30 – 17h30 (Singapore)

Table of Contents

Contacting us	3
What's New in this Release	11
Chapter 1 About this guide	13
Hawkeye overview	14
Key features	14
Hawkeye endpoints	20
Chapter 2 Configure endpoints	21
Hawkeye endpoints definition	22
XRPi	22
XRPi hardware	22
Configure XRPi	25
XR2000	38
XR2000 Hardware	38
Configure XR2000	40
XR3000	56
Initial configuration	56
Setting the password	57
Setting the hostname	58
Configuring networking	58
Connecting to the Hawkeye server	63
Advanced administration	63
Rackmounting	65
Wall mounting	68
XR Docker	70
XR-VM	74
Requirements for XR-VM installation	74

Hardware Requirements for XR-VM	74
Configure XR-VM	75
XR-E1S	76
Install XR-E1S	77
Configure XR-E1S	77
Software Endpoints	79
Chapter 3 IxProbe Element Manager	83
Connect IxProbe to Hawkeye through IxProbe CLI	83
IxProbe Element Manager Dashboard	83
List view	84
Grid view	84
Detailed view	85
How do I...	85
View port statistics	85
Configure IxProbe	86
View audit trail	88
View system information	89
Perform bulk actions on IxProbes	89
Schedule upgrades	91
Chapter 4 Hawkeye User Interface Configuration	93
User Interface Presentation	94
Probes Management	96
Manage users and groups	97
Users and Groups Definitions in Hawkeye	97
Group Management	98
Users Management	100
Test Execution	103
Threshold Management	109
Alarms Management	111
Mesh Management	113
MAP Configuration and Probe Location Configuration	115

Custom dashboard	120
How do I...	120
Hawkeye preferences	126
Configuring Automatic Email Notifications	143
Chapter 5 Hawkeye User Interface Results	145
Main Dashboard	146
Wi-Fi Dashboard	146
Test Results Screens	148
Map Status	152
Hawkeye Reports	152
Paths	159
Outlier	160
Chapter 6 Hawkeye Test Types	163
Test type general description	165
Node to Node	165
Understanding Node to Node Metrics	167
What is Goodput?	172
Testing Throughput Using TCP or UDP	172
Node to Node Test Types	173
TCP Throughput Tests	173
UDP Throughput Tests	183
Network KPI tests	191
QOS Qualification Tests	198
Voice and Video Tests	203
Video Stream	205
Unified Communications	215
Real Time Transactional Applications Tests	223
DSCP (QOS) Settings Explained	239
Details on Class of Service - Different Standards	240
Common Errors - N2N	243
Default Number of Tests per Probe Type (N2N)	246

N2N license cost per Test Types	252
Real Services	255
Licensing	256
Continuous	256
Advanced	261
Path Discovery	293
Real Service Endpoint Support Matrix	298
Replicating Tests Across Multiple Endpoints	302
Test Types Reporting Wi-Fi Statistics	302
Supported Protocols and Standards	308
Supported Voice over IP Codecs	311
Chapter 7 Outlier detection	313
How do I...	313
Configure Auto Learn Threshold	313
Configure Auto Learn Threshold Global	314
Configure Outlier	314
Quantization and Fudge Factors	315
Chapter 8 Server and Probe Communications	317
Server and Probe Communications Overview	318
Hawkeye Ports for Automatic Endpoints	319
Hawkeye Scenarios for Endpoints	321
Debugging Routing Issues	326
Troubleshoot Connectivity between Endpoints	326
Chapter 9 System Optimization	333
Hawkeye Services	334
Manage Configuration Database	335
Report Generation	337
Parameters Effecting Performance	337
Example of optimization of a running system	339
FPM tuning	340
Chapter 10 Security	343

Secure Access to Hawkeye Server	344
Hawkeye User Authentication	347
Change Passwords	350
Security Audit Logging of Users	350
Hawkeye Server SSL customization	350
Chapter 11 Advanced Administration Guide	353
MariaDB Database Management	354
Hawkeye Configuration Database Structure	354
Elasticsearch Management	355
OSS (Operations Support System) Integration	356
Backup and restore Hawkeye databases	357
Probe Management - Probe Busy	360
Hawkeye Folder Structure	362
Set up e-mails with Hawkeye server	362
SNMP Configuration and Verification	364
SNMP Traps	364
How to use SNMP Traps	364
Verify Hawkeye Server MIBs file can be interpreted by the User's SNMP server	365
Configure Hawkeye Server to send SNMP trap to a specific SNMP server	365
Configure your SNMP server to receive Hawkeye server originated SNMP traps	365
Enable SNMP traps to be triggered for endpoint scheduled tests	366
Verify SNMP trap successfully received and decoded by SNMP server	366
Advanced Troubleshooting – Debug SNMP packet routing issues	366
Rest API	367
REST examples	371
Server upgrade	378
Configure Time Zone and NTP	383
Configure Time Zone	383
Configure NTP Client	383
Configure Hawkeye as NTP Server	384
Configure UI Time Zone	385

Chapter 12 Server CLI Commands	387
Chapter 13 Troubleshooting	393
LDAP	393
Index	395

What's New in this Release

For detailed information on the new features and updates for Hawkeye and its dependent components that are implemented in the current release, see *Hawkeye Release Notes*.

This page intentionally left blank.

*CHAPTER 1***About this guide**

The Hawkeye user guide covers the installation and configuration of Hawkeye endpoints and how to use and manage Hawkeye.

This chapter contains the following topics:

Hawkeye overview	14
Key features	14
Hawkeye endpoints	20

Hawkeye overview

In today's highly competitive environment, the following activities are important to a company's survival:

- Delivering innovative services such as Voice over IP (VoIP)
- Maintaining unified communications (for example, Skype for Business)
- Migrating business services to cloud
- Streaming videos

The following factors can compromise a company's network performance and brand reputation:

- Bottlenecks in network
- Latency
- Wireless network issues
- Other hard-to-locate network issues

Network managers and operators need a simple, yet reliable way to continuously verify the performance of their networks for hassle-free application delivery.

The key benefits of Hawkeye are as follows:

- Quickly and effectively validate network performance
- Isolate problems and proactively detect issues by running scheduled verification tests on any site, by using wireline or wireless connections

Hawkeye simulates application traffic and sends key performance metrics to a central console for fast action. To do this, Hawkeye uses a combination of hardware and software agents called performance endpoints. These performance endpoints provide end users perspective of the remote site on network performance. These endpoints empower network managers with proactive ways to detect, diagnose, and fix issues. Measurements range from network quality to user experience and wireless network monitoring. Thus, it enables administrators to improve the overall network up-time and to detect network performance issues before they impact end users.

Hawkeye tests are easy to deploy and use, which helps your company to efficiently assess networks and applications.

Key features

Following are the key features of Hawkeye:

- Uses a web-based platform for multi-user access, test scheduling, data storage, and real-time analysis.
- Deploys endpoints with turnkey hardware or software endpoints.
- Verifies virtual infrastructure with software and VM endpoints.
- Installs the endpoints automatically within complex network topologies that include network address translation (NAT) and firewalls.
- Verifies user experience, monitor and diagnose wireless networks with inspect features.

- Continuously injects real-time traffic into the network as per schedules between nodes or in a mesh.
- Conducts distributed tests with on-premises or off-premises servers, that is, cloud servers.
- Verifies fixes that are available in your network in real-time with Pass/Fail status.
- Finds network or application faults quicker with interval testing throughout the day, week, and month.
- Tracks services and network trends proactively based on time-of-day and day-of-week of services.
- Registers Hawkeye Express online and creates an account to your server.
- Deploys Hawkeye on-premise web server in central locations such as NOC and data center.
- Strategically deploys the software and hardware endpoints to reach any network location at lowest cost. Network locations can be the following:
 - Customer premises
 - Mobile devices (wireless network or cellular)
 - Remote sites and head offices
 - Network aggregation points (PEs)
 - Core network, Multiprotocol Label Switching (MPLS) routers
 - Data centers
 - Virtual machines and servers
 - Cloud locations such as Amazon and Microsoft Azure

Plan and design your active test scenarios

You can do the following to plan and design your active test scenarios using Hawkeye:

- Define test topology with node-to-node or mesh with hub and spoke.
- Build a large topology test (full mesh).

Test types selection among pre-calibrated tests in Hawkeye library

Hawkeye supports a variety of service level agreements (SLA) and quality of experience (QoE) objectives, that include the following tests:

- For both Hawkeye Express and Hawkeye:
 - Speed test from site-to-site with the advanced configuration on traffic profiling
 - Bandwidth availability or verification with TCP-based testing
 - IP network SLA verification (one-way delay, jitter, loss)
 - Unified communications tests (Skype for Business), which is Microsoft Certified
 - Voice over IP calls (G711, G729) with MOS score
 - Ping (ICMP) and path discovery to any interface on the web
 - User experience downloading web pages
 - DNS response time

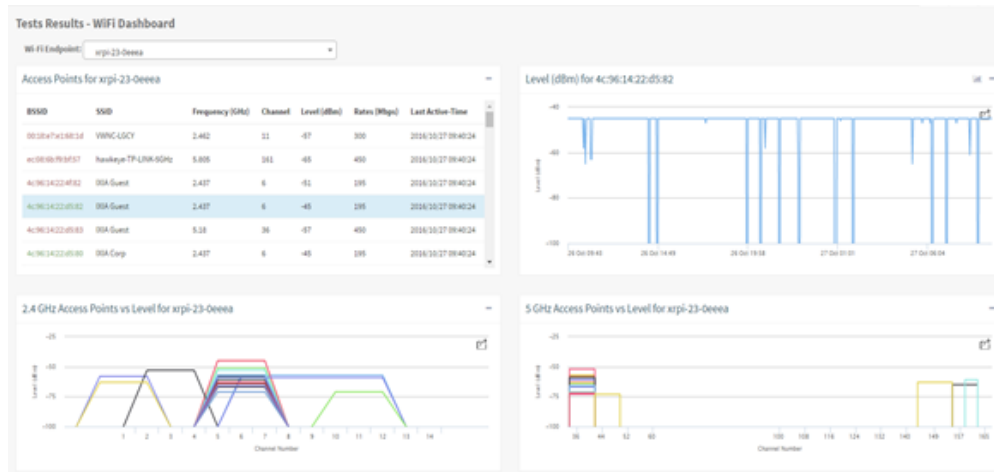
- For advanced test types and metrics on Hawkeye:
 - Advanced bandwidth availability or verification with bit blasting or TCP-based testing
 - Class of service (COS) implementation validation with oversubscription scenarios
 - IP network SLA verification (one-way delay, jitter, loss) with COS verification
 - Real-time streaming verification:
 - Mean opinion score (MOS) for voice
 - Media delivery index (MDI) for video streaming
 - Server response time for transactional applications emulating user profile
 - Unified communications tests (Skype for Business), which is Microsoft Certified, volume calls verification
 - Voice over IP calls (G711, G729) with MOS score, volume calls verification
 - Access to any HTTP/HTTPS servers by using one arm test to any URL
 - Netflix, YouTube, and any Dash/Adaptive streaming test
 - Video streaming
 - Multicast video
 - TCP, UDP echo tests
 - Quality of Experience for email, torrent, YouTube, Dropbox
 - Remote destination port opening verification
 - Wireless network advanced metrics

Monitor distributed wireless networks from the end-user perspective

Perform the following steps to monitor distributed wireless networks from the end-user perspective.

1. Connect XRPI to a wireless network in key locations and software agents in devices for ad-hoc verifications.
2. Collect wireless network's signal strength information while running Hawkeye tests.
3. Prove your wireless network connectivity to different SSIDs with recurrent connectivity tests. Diagnose any issues connecting to the wireless network and quickly identify issues, such as authentication, DHCP, and Layer 3 connectivity.
4. Collect and display the wireless network coverage dashboards and understand wireless network environment.

5. Build floor plans with the real-time wireless network coverage.



Create target thresholds for different tests

Thresholds are the baseline to decide if tests are passing or failing. You can configure target thresholds for different tests by using Hawkeye.

- Adjust applications, test variables, and thresholds based on trial data to match expectations of the network and its performance.
- Decide whether the test is passing or failing based on thresholds.
- Set up correct thresholds to understand the test results and make sure that the right level of information is in the database.
- Pre-configure the default test thresholds in the system.

Leverage Path Discovery for troubleshooting

Path discovery helps to provide visibility into network topology from a location with Hawkeye endpoint to any remote location. Path discovery leverages the Hawkeye test execution framework to allow historical data collection and perform analysis in real-time or with retrospective views. Following are the advantages of Hawkeye Path Discovery:

- Advanced topology discovery from Ixia endpoints to any remote location.
- Hop-by-hop discovery.
- Path discovered based on specific application settings
- Powerful and intuitive result display
- Quick troubleshooting tools that identify nodes with loss or long delay

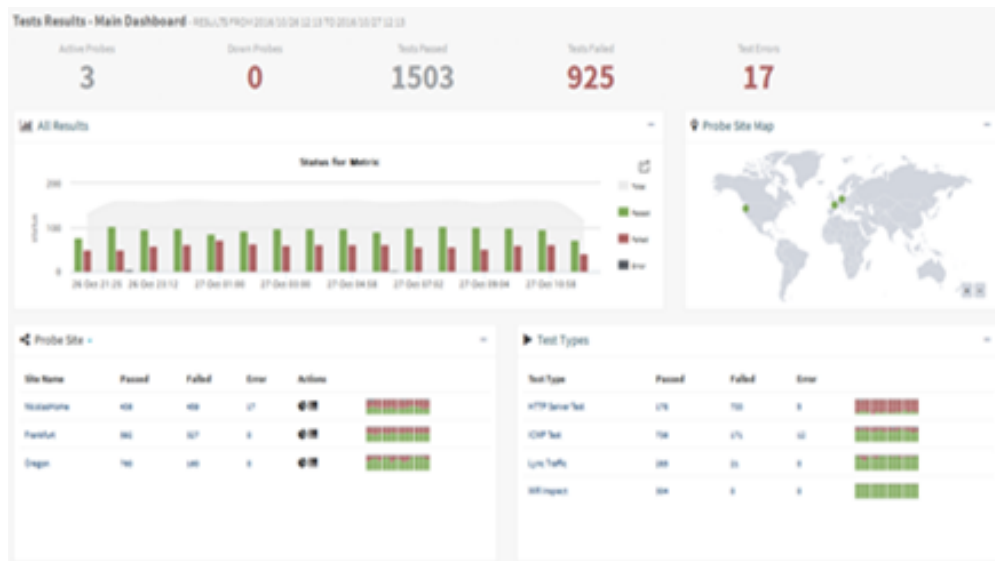
- Geolocalization on each identified public node



Analyze results

Hawkeye helps you to analyze test results with the following features:

- Use different result levels and granularity to get quick and efficient results and understanding.
- Ensure that team members can access the data required with simple Pass or Fail criteria or detailed test reports.
- See results in real-time in the geographic dashboard.
- Run your test and view single instance results or group of test results.
- Quickly identify problematic links.
- View specific tests and understand results.
- Run trend reports on historical data and analyze network behaviors.
- Export and send reports through email to share results between teams.



Monitor Pass or Fail for trouble spots

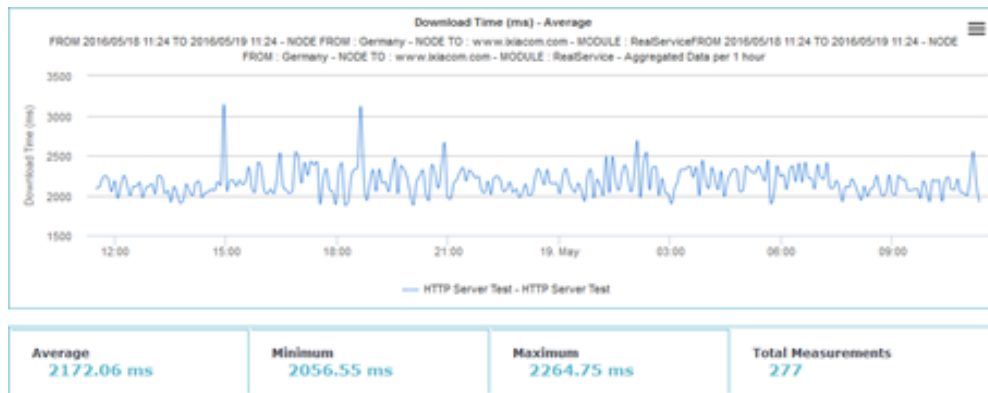
Hawkeye allows you to set the following on troubled spots to get notified for test status:

- Alarms on critical paths
- Notification email, SNMP traps, and other customized notifications

Run reports

Hawkeye allows you to generate an array of reports, which helps you to monitor the performance of your network. You can do the following:

- Create reports and dashboards from the reporting engine, based on the results stored in the database.
- Schedule daily automatic reports to follow critical networks.
- Receive automatic emails with comprehensive reports.



Hawkeye endpoints

The following table describes the Hawkeye endpoints:

	XR3000	XRPi	Virtual Endpoints	Android	iOS	Windows	Linux	XR-E1S	IxProbe
			XR-VM 						
Network Monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application and Web Monitoring	✓	✓	✓					✓	✓
Wireless Network Monitoring	✓	✓							
Specifications									
Hardware	✓	✓						✓	✓
Software			OVA, KVM, Docker, Public cloud 1 CPU, 1 GB RAM	✓	✓	✓	✓		

CHAPTER 2

Configure endpoints

This chapter describes how to configure Hawkeye Endpoints.

In this chapter:

Hawkeye endpoints definition	22
XRPi	22
XRPi hardware	22
Configure XRPi	25
XR2000	38
XR2000 Hardware	38
Configure XR2000	40
XR3000	56
Initial configuration	56
Setting the password	57
Setting the hostname	58
Configuring networking	58
Connecting to the Hawkeye server	63
Advanced administration	63
Rackmounting	65
Wall mounting	68
XR Docker	70
XR-VM	74
Requirements for XR-VM installation	74
Hardware Requirements for XR-VM	74
Configure XR-VM	75
XR-E1S	76
Install XR-E1S	77
Configure XR-E1S	77
Software Endpoints	79

Hawkeye endpoints definition

An endpoint is called a probe and represents a device inserted at a key juncture in a network for monitoring or collecting performance data about network activity. The test traffic generated conforms to applicable standards. For example, voice traffic contains generated data that conforms to selected codecs with correct packet sizes and packet timings. The Hawkeye endpoint for corporate security generates its test data. Hawkeye does not monitor or analyze corporate private transmitted data. The following Hawkeye endpoints are available:

- Keysight Technologies hardware endpoints: XR3000, XR-E1S, IxProbe, XRPi, and xr2000
- XR software endpoints: XR-VM, XR Docker, PI4 Image, and XR Cloud
- Software endpoints: IOS EP, Android EP, Linux EP, and Windows EP

Hawkeye supports different software endpoints for various platforms. You can download these endpoints from the Keysight Technologies, Inc. web site mentioned in the section on software endpoints.

NOTE

The Real Services testing is only available with XR2000, XR2000 VM (Linux Software), XR Docker, and XRPi endpoints. Use XRPi to perform or monitor wireless network testing.

XRPi

The XRPi is a low-profile ultra-small form factor unit. It is ideal for use as an endpoint. It contains an ultra-low voltage CPU and an integrated Ethernet port. It does not contain any fans.

The optional wireless network device supports both 2.4 and 5 MHz. The wireless network device also supports the latest state 802.11ac with 80 MHz.



XRPi hardware

Package contents

XRPi ships with the following components:

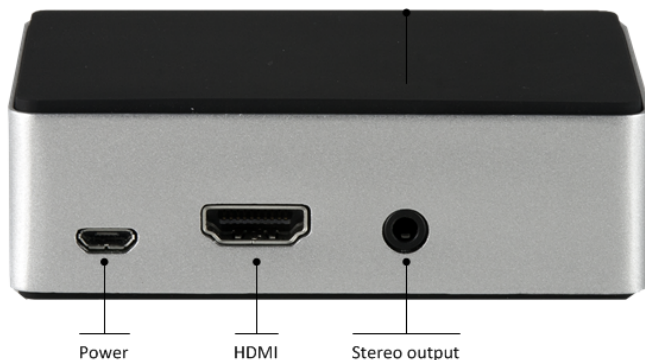
- XRPi unit
- Dual-voltage (110/220) AC power adapter
- Keysight wireless network device
- Non-powered 2.0 USB hub
- HDMI-to-DVI cable
- Quick start guide

Ethernet and USB ports



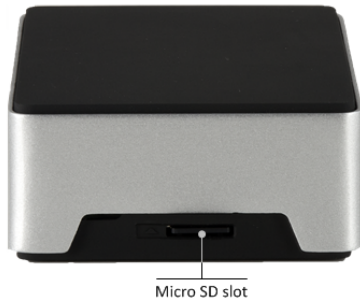
Component	Description
Ethernet port	Use these ports to connect the XRPi to other Ethernet devices.
	LAN LEDs
	Green: Connection speed
	On 100 Mbps
	Off 10 Mbps
	Yellow: Activity
	On Port is active
	Blinking Port is sending or receiving traffic
USB ports	USB 2.0 ports. Keyboards, mice, USB 2.0 hub, and the wireless network device are the only supported accessories that can be plugged into these ports.

Power and HDMI ports



Component	Description
Power port	Micro-USB power port. Connect the supplied AC power adapter to this port.
HDMI	HDMI 1.4 video output port. Connect the supplied HDMI cable to this port.
Stereo	3.5 mm stereo output port (disabled).

Micro SD slot



Component	Description
Micro SD slot	Micro SD card slot. A micro SD card contains the Hawkeye operating system and application. The micro SD card is the only permanent storage on Hawkeye.

Insert the micro SD card

To insert the micro SD card, position the micro SD card with the contacts facing upwards and insert the card into the slot until you hear a click.

Remove the micro SD card

To remove the micro SD card, press the card inwards with a fingernail until you hear a click, and then withdraw the card from the slot.



System information

Current Draw	~ 650 mA, (3.0 W)
Temperature (ambient)	Operating: 0°C ~ 70°C Storage: -20°C ~ 70°C

Humidity (RH), ambient	5 ~ 95 percent, non condensing
Dimensions (WxHxD)	92 mm x 29 mm x 67 mm 3.63" x 1.13" x 2.63"
Weight	100 g
Approvals & Compliance	CE Emission, FCC Class A, RoHS

Configure XRPI

You can connect the device through HDMI and keyboard by using a USB port.



Sign in the XRPI by using the following default credentials:

- Username: root
- Password: Ixia!123

Default configuration (as shipped from factory)

Physical port	Logical port	Address
LAN1	eth0	DHCP

Configure port

This section explains the steps to configure DHCP IP and static IP.

IP configuration for eth0

The default configuration for eth0 is IPv4 DHCP to configure IPv6 or Static IPv4 Please follow the instructions below.

IPv4 using static IP only

In file /etc/network/interfaces add

```
iface eth0 inet static
address 192.168.x.x
gateway 192.168.1.1
netmask 255.255.255.1
network 192.168.1.0
broadcast 192.168.1.255
```

IPv6 using DHCP and disable IPv4 on eth0.

In file /etc/network/interfaces add

```
iface eth0 inet6 dhcp
```

and remove

```
iface eth0 inet dhcp
```

IPv4 using static IP and IPv6 using DHCP on eth0.

In file /etc/network/interfaces add

```
iface eth0 inet6 dhcp
iface eth0 inet static
address 192.168.x.x
gateway 192.168.1.1
netmask 255.255.255.1
network 192.168.1.0
broadcast 192.168.1.255
```

IPv4 using DHCP and IPv6 using static IP on eth0.

In file /etc/network/interfaces add

```
iface eth0 inet dhcp
iface eth0 inet6 static
address 2001:1800:1234:22::3fd/64
gateway 2001:1800:1234:22::1
```

Configure a DNS server

In file /etc/resolv.conf add

nameserver 8.8.8.8	# Google's public DNS server
nameserver 2606:4700:4700::1001	# public IPv6 DNS server

Reboot the XRPi for changes to take effect.

```
# reboot
```

Check the IP address locally and testing connectivity (DHCP or static)

1. Access the XRPi's console and use the following command to check the XRPi's IP address:
`ifconfig eth0`
2. Run the following command to test connectivity:
`ip route`
Look for: `default via [gateway IP]`. Ensure that `ping [gateway IP]` succeeds.
3. Run the following command to test that the XRPi can reach the internet and that DNS resolution works:

```
ping www.ixiacom.com
```

The ping should succeed and not time out.

If either the connectivity or name resolution fails, check the static IP information that you entered and confirm that the DHCP server is available.

NOTE

For XRPi wireless device, when setting up static IP addresses and connecting both wlan0 and eth0 interface, XRPi automatic routing scripts that ensure proper communications with the server will not turn on. We recommend to use DHCP configuration for this scenario.

4. The default host-name for the XRPI is `xrpi2-<last 5 digit of MAC address>`. The MAC address is on the label at the bottom of the XRPI.

XRPI Upgrade

Register with Hawkeye server

We recommend you to configure XRPI with the Hawkeye server as automatic endpoint.

If XRPI is registered to the Hawkeye server, you can perform the upgrades automatically. If XRPI is registered to the Hawkeye Server 1.0 or registered as a manual endpoint, you must upgrade the endpoint by using `probeConfigure`. We recommend you to use this upgrade strategy for Hawkeye users.

To update automatically, do the following:

1. Connect to the XRPI with SSH.
2. Type the following command to start the script: `probeConfigure`.
3. When the script prompts you, enter the following:
 - A name for the probe. You can use letters, numbers and hyphens (`_`) in the name. This option will set the host name and the name as displayed into Hawkeye. You can edit the name on the Hawkeye GUI.
 - The host name or IP address of the Hawkeye server (public IP, if in cloud).

NOTE The name cannot contain spaces.

4. When the script ends, XRPI will automatically try to register.

Upgrade XRPI without Hawkeye Server

To upgrade XRPI from internet, do one of the following steps:

- When the XRPI has internet connectivity, connect to XRPI with SSH and run the following commands:

```
cd /tmp
wget https://ixiapublic.s3.amazonaws.com/hawkeye/xrpi_upgrade.tar.gz
tar zxvf xrpi_upgrade.tar.gz
cd ix_upgrade
./ixia_chariotprobe_install.sh
cd ..
rm -rf ix_upgrade
rm -rf xrpi_upgrade.tar.gz
```

- If the XRPI does not have internet connectivity, copy the file at the `https://ixiapublic.s3.amazonaws.com/hawkeye/xrpi_upgrade.tar.gz` location. Then FTP (or equivalent, such as `scp`) the file to the XRPI in the `/tmp` folder. Then run the procedure:

```
tar zxvf xrpi_upgrade.tar.gz
cd ix_upgrade
./ixia_chariotprobe_install.sh
cd ..
rm -rf ix_upgrade
rm -rf xrpi_upgrade.tar.gz
```

NOTE A reboot after upgrade is necessary.

Secure XRPI2 ports

Follow the instructions in this section to secure and configure XRPI2 ports.

Ports opening requirements for Ixia endpoints

The ports that you must open for INBAND are:

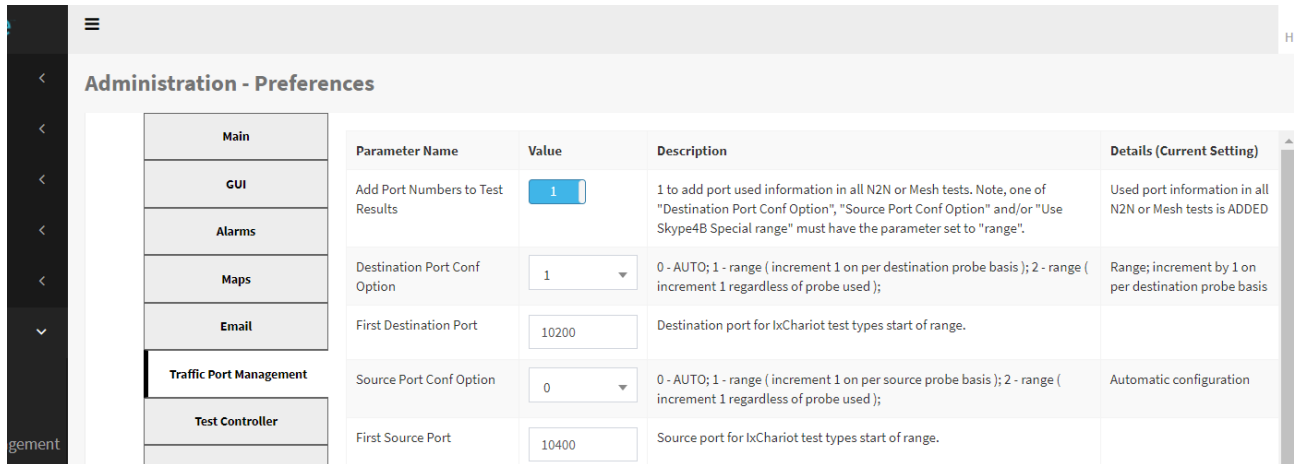
- TCP port 22: This is required for manual remote management. Hawkeye server does not need these ports. You can protect this port by access list.
- TCP/UDP ports 10115-10116. This is required for control between endpoints.
- TCP/UDP ports TEST RANGE: You must define this range in Hawkeye server (see preferences below).

We recommend to let any OUTBAND ports be opened for Real Service tests.

Configure endpoints to use specific range of ports to test traffic

On the Hawkeye Server, under the **System Preferences > Traffic Port Management**, you can configure the ports for Node to Node traffic tests.

Each test executed on the endpoint will increment this range. Hence, it is necessary to open a range on the XRPI that can allow up to the maximum number of simultaneous tests that can go to a single endpoint. For XRPI, a recyclable range of 200 ports is enough.



Parameter Name	Value	Description	Details (Current Setting)
Add Port Numbers to Test Results	1	1 to add port used information in all N2N or Mesh tests. Note, one of "Destination Port Conf Option", "Source Port Conf Option" and/or "Use Skype4B Special range" must have the parameter set to "range".	Used port information in all N2N or Mesh tests is ADDED
Destination Port Conf Option	1	0 - AUTO; 1 - range (increment 1 on per destination probe basis); 2 - range (increment 1 regardless of probe used);	Range; increment by 1 on per destination probe basis
First Destination Port	10200	Destination port for IxChariot test types start of range.	
Source Port Conf Option	0	0 - AUTO; 1 - range (increment 1 on per source probe basis); 2 - range (increment 1 regardless of probe used);	Automatic configuration
First Source Port	10400	Source port for IxChariot test types start of range.	

Configure XRPI endpoints firewall

To activate firewall on XRPI, do the following:

1. SSH as root on the XRPI device.
2. Create and edit new file with vi or nano text editor.

```
# nano /etc/init.d/firewall
```

3. Add and adapt the following in the table for ports openings:

```
#!/bin/sh
### BEGIN INIT INFO
# Provides: firewall rules
# Required-Start: $remote_fs $syslog
```



```

# Required-Stop: $remote_fs $syslog
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: Start daemon at boot time
# Description: Enable service provided by daemon.
### END INIT INFO
# Remove rules
iptables -F
iptables -X
# Block everything by default
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
# Keep established connections
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
# Authorize loopback (127.0.0.1)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# SSH (22)
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
# endpoint management (10115:10116)
iptables -A INPUT -p tcp --dport 10115:10116 -j ACCEPT
iptables -A INPUT -p udp --dport 10115:10116 -j ACCEPT
# endpoint traffic (need to be adapted to console configuration)
iptables -A INPUT -p tcp --dport 50000:50500 -j ACCEPT
iptables -A INPUT -p udp --dport 50000:50500 -j ACCEPT
# ICMP (Ping)
iptables -A INPUT -p icmp -j ACCEPT
# Limit denial or service
iptables -A FORWARD -p tcp --syn -m limit --limit 1/second -j ACCEPT
iptables -A FORWARD -p udp -m limit --limit 1/second -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/second -j ACCEPT
# protects port scans
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j
ACCEPT
# Drop XMAS / NULL scans
iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH FIN,URG,PSH -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

```

4. Save the file and make it executable.

```
# chmod +x /etc/init.d/firewall
```

5. Start the firewall.

```
# ./etc/init.d/firewall
```

We recommend you to make firewall load automatically at boot.

```
# update-rc.d firewall defaults
```

Enable wireless network interface

You can enable the wireless network interface on XRPI2. Before you enable the wireless network interface on the XRPI2, ensure that you have the following:

- Wireless dongle provided by Keysight.
- Network connection for XRPI eth0 (LAN) interface.
- The XRPI has image with version 2.0.9062115 or later. To see the XRPI version, use the `xrpi2_version` command after you have SSH or use **Probe Management**.
- For 2.2 onwards releases, XRPI supports static IP address being used for eth0 but DHCP must be used for wireless network interface (WLAN0). You must configuring the static IP address for eth0, which is used for Hawkeye management. The automatic wireless network scripts configures the WLAN0 interface routes.
 - Default routes for traffic will be over wireless interface (wlan0), if it is turned on. If, however, eth0 and wlan0 interface are on different subnetworks for Mesh tests, turn on the **Set test IP that matches default gateway** parameter on the **Administration > Preferences > Advanced Options** tab, so that for mesh tests, traffic will be made on the interface that has default gateway defined. When wlan0 is defined, default gateway is configured in the routing tables to be on wlan0.
 - We recommended you not to configure the XRPI with just the wireless network interface, as eth0 is used for Hawkeye management and it is a more reliable interface.
 - The wlan0 subnet must be different to eth0 subnet for XRPI routing scripts to correctly set up routes for DHCP.

To turn on the wireless network interface on XRPI, do the following:

1. Connect the network cable to the XRPI ethernet port.
2. Connect AC power supply using micro USB power connector.
3. Use a software tool like Putty or Bitwise to connect using SSH to the XRPI eth0 interface.

NOTE

The default username is **root** and password is **Ixia!123**.

4. Connect the Ixia wireless device dongle to any available USB port on XRPI device. The wireless interface (wlan0) is automatically configured on XRPI when you connect the dongle.

```

Linux xrpi-08914 4.1.20-v7+ #40 SMP Mon May 9 15:57:26 EDT 2016 armv7l
IXIA Raspberry PI image
This image is provided by Ixia
The exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Last login: Mon Oct  3 20:30:51 2016 from 192.168.83.138
root@xrpi-08914:~# xrpi2_version
2.0.9129825
root@xrpi-08914:~# ifconfig
eth0      Link encap:Ethernet  HWaddr b8:27:eb:20:89:14
          inet addr:192.168.82.22  Bcast:192.168.82.255  Mask:255.255.255.0
          inet6 addr: fe80::ba27:ebff:fe20:8914/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:244 errors:0 dropped:0 overruns:0 frame:0
          TX packets:203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40377 (39.4 KiB)  TX bytes:30216 (29.5 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr 74:da:38:73:4f:39
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@xrpi-08914:~#

```

5. Run the Linux **ifconfig** command (see the below example) to confirm the interface wlan0 is present.

NOTE

If you want to use wireless network for **Wi-Fi Inspect** and **Wi-Fi connect**, you can skip the steps above.

Route for Eth0 and Wlan0

Reboot

When eth0 (LAN) and wlan0 (Wi-Fi) are both used, XRPI will have sequential configuration for network stacks that are described below:

- The eth0 interface is brought up by system and runs dhcp query to obtains def GW, NTP server, DHCP lease, NIS servers, DNS servers, DHCP IP on LAN interface.
- A static route is configured to Hawkeye server through LAN interface to make sure the connectivity to Hawkeye server will remain through LAN interface.
- wlan0 interface is brought up by the system to connect to the access point. DHCP runs first, then the custom XRPI scripts run. It reconfigures and overwrites the routing tables, specifically the global default route (default GW for DHCP) to switch to wlan0. Then, the default routes and network routes are set in the global tables and the interface table. If eth0 and wlan0 are on different subnets, all routes to the subnet are unmodified. If they are on the same subnet, then this may cause routing issues as this is not a supported configuration.

Node to Node tests

Interface to be used for traffic is specified as part of test creation on Hawkeye server.

Mesh and real services tests

- If eth0 and wlan0 are on the same subnet, this may cause routing issues. This is not a supported configuration.
- If eth0 and wlan0 are on different subnets, (network routes apply) so if destination IP for test is on subnet for eth0, traffic will go on eth0.
- If destination IP for test is on the subnet for wlan0, traffic will go on wlan0.

Wireless network connectivity lost

- If XRPI receives disconnect from AP or a DHCP release, XRPI will attempt to reconnect by using wpa_default.cfg, as long as DHCP lease has not expired.
- If XRPI receives no message/event for lost connectivity (eg AP loses power), XRPI will attempt to reconnect every 10 seconds.

NOTE

Rebooting triggers re-establishment of wlan0.

Connect to wireless network

You can connect to wireless network using one of the following:

- By using **Wi-Fi Connect** of Hawkeye Server GUI.
- By using Real Service wireless network connect test.
- By using a script (wifiConnect) to connect to specific SSID.

NOTE

The double quote symbol is not supported in the password. It is advised that if manually editing the wpa_default.cfg file not to use the double quote symbol for comments as it is used by the parser to denote parameters.

Use Hawkeye server GUI option for Wi-Fi Connect

The Hawkeye server supports the ability to configure the wireless network interface for XRPI, assuming eth0 is present. After XRPI is configured as an automatic endpoint on the Hawkeye server in the **Probe Management > Probe Management Automatic**, if the you drill down on a specific XRPI, there is a pop-up for **Wi-Fi Configure**, which allows you to enter details for the AP. When **connect** is selected, XRPI uses these details to connect to the AP. If successful, it saves the changes on XRPI in the **wpa_default.cfg** file.

Use Real Service Wi-Fi Connect test

The Real Service Wi-Fi Connect test is explained in the *XR2000 User Guide > Real services* section for the Wi-Fi Connect test type. When the test is run, the XRPI receives commands to directly configure the wireless network device. XRPI releases wlan0 connection (routes updated), then attempts to connect to the AP defined for the Wi-Fi Connect test. The connection details from the test are temporary and are not saved in a file on the XRPI. If the connection is successful, routes are updated for wlan0 and results are sent to Hawkeye Server. After the test is finished, if Wi-Fi Connect test parameter **reset Interface** is set to **yes**, wlan0 is released and wireless network reestablishment occurs to the AP defined in wpa_default.cfg (if file exists). If Wi-Fi Connect test parameter **reset Interface** is set to **no**, wlan0 will remain with temporary test configuration until XRPI is restarted. The ethernet port must be active for the management connection to the Hawkeye Server to report results, as the test resets the wlan0 connection.

Use script to connect to specific SSID

The XRPI has a custom wireless network connection script that can be used to connect to an access point (SSID). The script is located in /home/ixia directory and is named wifiConnect.py:

```
# cd /home/ixia
# wifiConnect
```

The script scans for available AP's in range, then prompt for the selection of a SSID/BSSID. You can then enter authentication parameters. If the wifiConnect script runs with the **-D** option to save the connection as default, it saves in the directory /etc/wpa_supplicant as wpa_default.cfg if only the connection is successful. If the **-D** option is not used with the wifiConnect script command, it prompts if you want to save settings as default. If an AP has a configuration that is not addressed by the wifiConnect script, you have to manually edit the parameters in the wpa_default.cfg file.

There are several options that can be used with the wifiConnect command:

- To list out all options with a brief description:

```
# wifiConnect -h
```

- To connect then save the AP connection details as default:

```
# wifiConnect -D
```

- To use a pre-existing AP configuration file:

```
# wifiConnect --config /etc/wpa_supplicant/wifi_ixia_guest.cfg
```

Disable wireless interface

To disable wireless interface, do the following:

1. Go to XRPI (ssh) and physically renaming the XRPI WIFI configuration file (/etc/wpa_supplicant/wpa_default.cfg) to another name or delete the file.
2. Restart XRPI or bring down the wireless interface with the command:

```
Ifdown wlan0
```

Configure custom wireless network

Hawkeye Server supports the use of wireless network custom parameters (defined by `wpa_supplicant`). The specific parameter, however, must be supported by the `wpa_supplicant` and the physical wireless network device.

When you perform a wireless network connect to an AP, following steps occur:

1. The configuration including custom wireless network configuration is saved into the `wpa_default.cfg` file on the XRPI.
2. The `wpa_supplicant`, which is an IEEE 802.1 cross platform compliant application (third party Linux app), reads the configuration from `wpa_default.cfg` and sends information to the wireless network driver specific to the wireless network device. After you configure the wireless network device, the `wpa_supplicant` negotiates connection with the AP and radius server for authentication.

IMPORTANT

Hawkeye can only take custom wireless network parameters and store them in the `wpa_default.cfg` file to be read by the Linux `wpa_supplicant` application. For your custom wireless network parameters to be successful, the version of `wpa_supplicant` must support the parameters and the wireless network driver must also support the custom parameter. Refer online to all parameters supported by the `wpa_supplicant`. Contact Keysight Customer support if you need confirmation that a specific parameter is implemented or supported. We recommend to use the minimum amount of configuration in the `wpa_default` file (eg. key management, user, password, SSID).

Troubleshoot wireless network issues

This section provides you information with scenarios to troubleshoot the wireless network issues.

1. Confirm hardware and drivers are okay for wireless network:

- a. Confirm wireless network device is plugged into XRPi USB port and has been initialized by checking the LED on the **Edimax** labeled wireless network device. A blue flash from the LED indicates the device is working.
 - b. Run the following Linux command to confirm wireless network device detected in USB port. After detecting the device, the name of the device that is **Edimax** appears in the list of devices.

```
# lsusb -t | grep Edimax
```
 - c. Confirm that the driver for **Edimax** device is running, using the following command:

```
# lsmod | grep 8812au
```
- Confirm WLAN0 interface for wireless network is operational:
 - a. To confirm if there is an entry and the wlan0 interface is operational, use the following command:

```
# "ifconfig wlan0"
```
 - b. To check the status of WLAN, use the following command:

```
# ip link show wlan0
```
 - c. To bring up the Wi-Fi interface, use the following command:

```
# ip link set wlan0 up
```
 - d. To check the log files for time stamp for wireless network connectivity and release events, use the following command:

```
# cat /var/log/Ixia
```
 - Check if the wireless network interface is connected to an AP by using the following command:

```
# iw wlan0 link
```
 - Confirm if the XRPi Wi-Fi can see all AP in range using the following command:

```
# iw wlan0 scan
```
 - Confirm the IP assigned to WLAN0, using the following command:

```
# ifconfig wlan0
```
 - After an IP is assigned to wlan0, confirm all routes including the default route is using wlan0 with the following command:

```
# route -n
```
 - If an XRPi wireless network endpoint is moved from one location to another, the IP addresses for wlan0 and eth0 changes. After the XRPi Wi-Fi endpoint is located in its new location, use the following commands in the given sequence to optimize the routes:


```
# route -n
# ip route flush table main
# rm -rf /etc/wpa_supplicant/wpa_default.cfg
# wlan0 down
# wlan0 up
# route -n
# ifconfig
```
 - Schedule the real service test **Wi-Fi Inspect** on the Hawkeye server at an interval of five or ten minutes for one or two hours to find problems with different AP. View results in the **Wi-Fi**

Dashboard. The results show the stability of each AP signal strength over the period. Graphical representation of the results, channels, and signal strength of each selected AP issues of all AP is available, which helps you to view the overlapping interference:

- Different wireless network devices report signal strength at different layers in the wireless network stack, so sometimes there can be differences when comparing.
- The Edimax device considers a weak signal to be below -65 dBm. Packets can become corrupted and lost at this weak signal strength. The Edimax device may have difficulty connecting to an AP with a very weak signal strength of -70 dB.
- The wireless network scan may have issues detecting and reporting older AP if they do not provide primary channel information and/or frequency.

9. If connection to an AP is unsuccessful, perform the following steps to troubleshoot:

- a. Perform a Wi-FiConnect test from the XRPI CLI and enable debug logs using one of the following commands, to see message sequences and reason codes.

```
# wifiConnect --debug=6
# wifiConnect --debug=6 2>&1 |tee /tmp/myLog.txt
```

NOTE

Set debug flag to **7** for most detailed logs, which include messaging and state changes. Second command saves trace to a file.

- b. Perform a detailed wireless network scan to find other AP using the same channel as the one previously attempting to connect to. The noise interference for an AP is affected by the relative signal strength of other AP's using the same channel and the signal strength of those AP. The bandwidth used by an AP usually spans the channel number above and below the reported channel number. The following command will perform a detailed wireless network scan and save results to a file:

```
# /home/ixia/wifiScan.py -d 4 -u 2>&1 |tee /tmp/myScan.log
```

10. Fails to connect or drop from specific BSSID. If you specify BSSID with wifiConnect command or test the connection may drop or lose. A disconnect from an AP (BSSID) may be due to a local generation event or remote generation event. A locally generated event for disconnect can be due to XRPI wireless network inability to see the beacon or keep it alive from its connected AP (BSSID). Keysight recommends you to use different signal channels for each AP (BSSID) of an SSID with multiple AP. It is possible that an AP for the same SSID, but different BSSID, may have a stronger signal and drown out the beacon of the weaker BSSID when using the same signal channel.

The connection can also drop due to the remote generation of events. The Radius server may realize that the XRPI Wi-Fi is connected to an AP (BSSID) but an AP (BSSID) belonging to the same SSID (i.e. Corporate Wi-Fi) may have a stronger signal. The Radius server will often inform the currently connected AP to send a disconnect and optionally perform a handover to a different stronger signal strength AP (BSSID).

11. You can manually adjust routes. The following code snippet is for reference. We suggest you to first check if the default route is missing.

```
# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 0.0.0.0 0.0.0.0 U 0 0 0 wlan0
172.16.0.76 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
```


The above output shows the missing route.

```
# ifdown wlan0; ifup wlan0
```

Then, verify the routes with

```
# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 0.0.0.0 0.0.0.0 U 0 0 0 wlan0
172.16.0.0 0.0.0.0 255.255.255.128 U 0 0 0 wlan0
172.16.0.76 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
```

Finally, confirm the additional route for wlan0 is present and routes are as expected.

NOTE

The microSD card cannot be moved from one XRPi to another as the identity from the first XRPi will be used for the second XRPi.

XR2000

The XR2000 is a low-profile small form factor unit ideal for use as an endpoint. It contains the following components:

- An ultra-low voltage CPU
- Six integrated ethernet ports

NOTE

One of the ethernet ports is PXE-enabled, which allows you to run remote diagnostics and reboot.

It does not contain any fans.



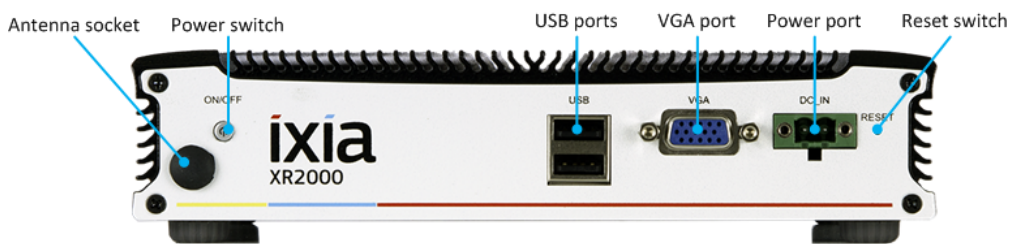
XR2000 Hardware

Package contents

The XR2000 ships with the following components:

- XR2000 unit
- Dual-voltage (110/220) AC power adapter
- *Quick Start Guide*

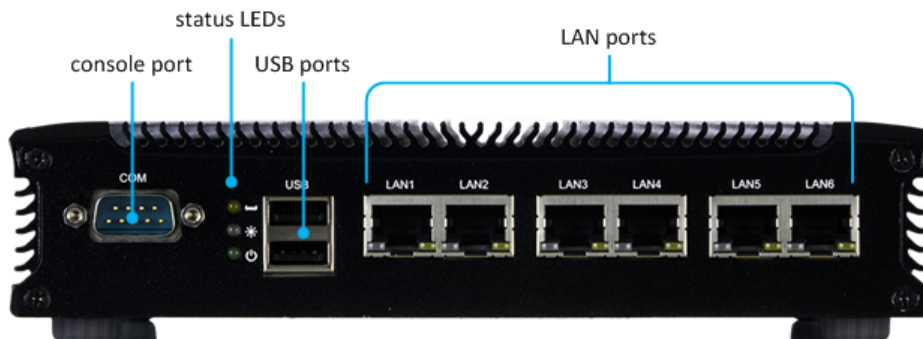
Front panel



Component	Description
Antenna socket	Not supported
Power switch / LED	Green indicates that the system is powered on. Red indicates that the system is in standby mode.

USB ports	Not supported
VGA port	Connect this port to a monitor or other display device. The Hawkeye supports QXGA resolution (2048 x 1536 at 75 Hz).
24V DC power socket	Use with the supplied 24V DC power adapter.
Reset switch	Not supported

Rear panel



Component	Description
Console Port (DB-9)	<p>Use this port to connect a suitable rollover cable (Yost cable or Cisco console cable) to configure the Hawkeye, or for diagnostics.</p> <p>Default terminal configuration parameters are 115200 baud, 8 data bits, no parity, 1 stop bit , no flow control.</p> <p>Internally this port is assigned as COM1.</p>
HDD/Status/Power LEDs	<ul style="list-style-type: none"> • HDD: Indicates that the Hawkeye's storage media is functioning normally. At boot time, the LED is on steadily. During data access to or from storage, it blinks. Otherwise, it is off. • Status: Green indicates that the Hawkeye is operating normally. Amber indicates a hardware fault. • Power: On indicates that the system is powered on. Off indicates that the system is powered off.
USB 2.0 ports	<p>You can connect USB devices such as keyboards to the USB ports.</p> <p>Top: USB0, bottom: USB1</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>NOTE You should only connect USB devices that have been qualified by Ixia for use with the XR2000. For the list of qualified products, contact your Ixia representative or support@ixiacom.com.</p> </div>
10/100/1000Mbps Ethernet LAN ports	<p>Use these ports to connect the Hawkeye to other ethernet devices.</p> <p>From left to right: LAN1-LAN6</p>

	LAN1 has Preboot Execution Environment (PXE) capability, so if you access the Hawkeye through this port, you can boot it independently of the installed operating system.	
	LAN LEDs	
	Left: Connection speed	
	Green	100 Mbps
	Orange	1000 Mbps
	Off	10 Mbps
	Right: Activity	
	On	port is active
	Blinking	port is sending or receiving traffic

System information

Temperature (ambient)	Operating: 0°C ~ 40°C Storage: -20°C ~ 70°C
Humidity (RH), ambient	5 ~ 95 percent, non condensing
Dimensions (WxHxD)	200 mm x 42 mm x 144 mm 7.9" x 1.65" x 5.67"
Weight	1.2 KG
Approvals & Compliance	CE Emission, FCC Class A, RoHS

Configure XR2000

There are four phases to configure and set up XR2000:

- Connect to XR2000
- First-time setup, in which you have to configure an IP address on the XR2000 so that you can access it over a network.
- Web setup, in which you set the XR2000 basic boot-up and runtime configuration. For this phase, you use a web browser to access the XR2000 over your network.
- Register XR2000 with Hawkeye server.

Connect to Hawkeye

For a new XR2000, you need to connect to the XR2000, and then configure its IP addresses so that you can access it over your network.

After you can access it over the network, you can use a web browser to perform more in-depth setup using the web setup. You need to connect directly to the XR2000 to set the IP address. You can do it in the following ways:

- Connect a monitor to the VGA port and a keyboard to the USB port. See, [First time setup through VGA and USB](#).
- Use a console cable to connect a laptop to the console port. See, [First time setup through the console port](#).
- Use an ethernet cable to connect a laptop to one of the LAN ports. See, [First time setup over ethernet](#).

NOTE

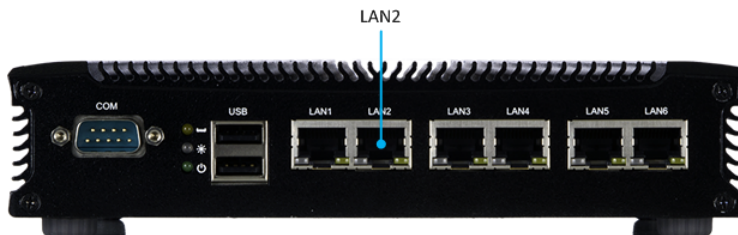
XR2000 supports multiple ethernet ports. Default routes for traffic will be over eth0. If each interface is, however, on a different subnetwork, go to **Preferences > Advanced Options > Set test IP that matches default gateway** and enable the option for Mesh tests a parameter so that when mesh tests are made, traffic will be on the interface that has default gateway defined. On the command line on the XR2000 use the `route -n` command to see which interface has the defined default gateway.

First time setup over ethernet

In the first time setup, you connect to the XR2000, and run a script to configure its name (the probe name). You will need a terminal-type application such as PuTTY.

To perform the first-time setup over ethernet:

1. Make sure that the XR2000 is powered off.
2. Connect one end of an ethernet cable to a computer, and the other end to the LAN2 port on the XR2000.



As shipped from the factory, the XR2000 is configured as follows:

Physical port	Logical port	Address
LAN1	eth0	192.168.1.10 / 255.255.255.0
LAN2	eth1	DHCP

3. On the computer, set its IP address so that it is on the same subnet (192.168.1.xxx) as the XR2000. For example, you can set it to **192.168.1.1**.
4. Power on the XR2000. At this point, you can do either of two things:
 - Exit the initial setup and move on to the web setup.
 - Run the setup script to configure the permanent IP addressing on the XR2000.

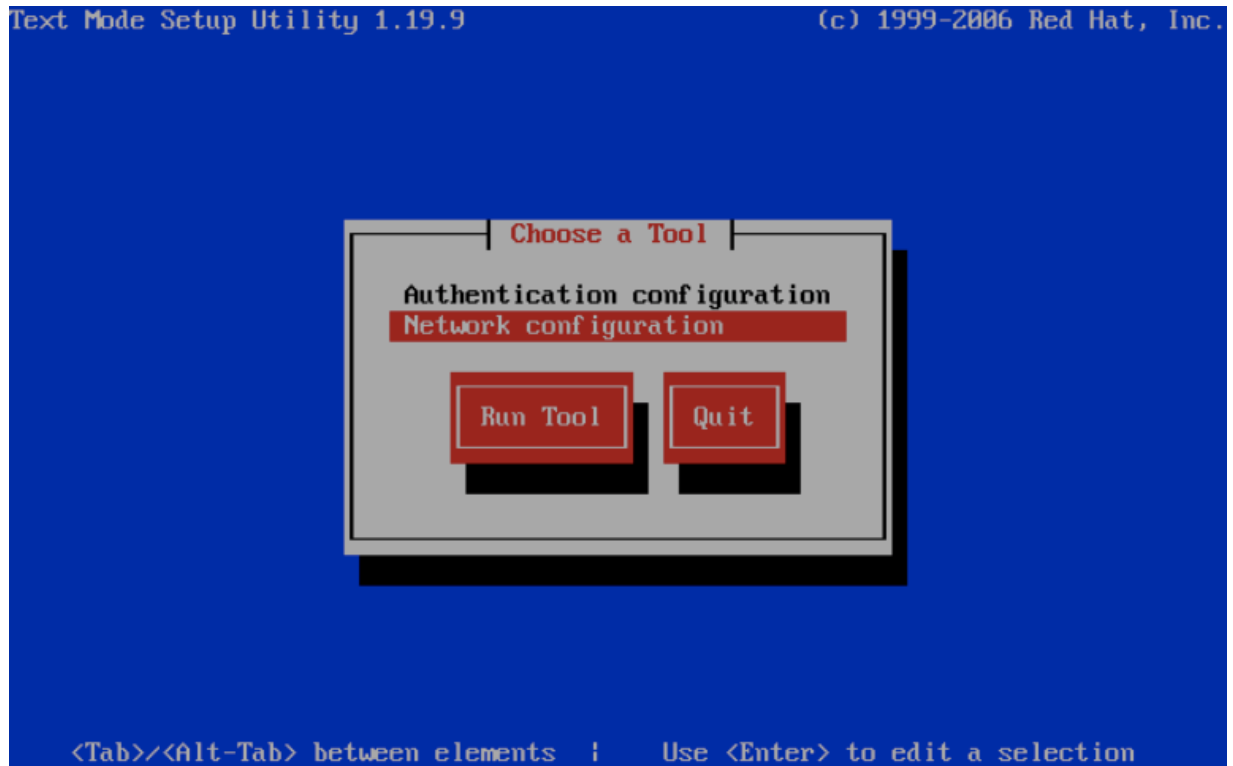
Running the setup scripts

The setup script allows you to quickly configure the IP addressing on the LAN ports. To run the setup script, do the following:

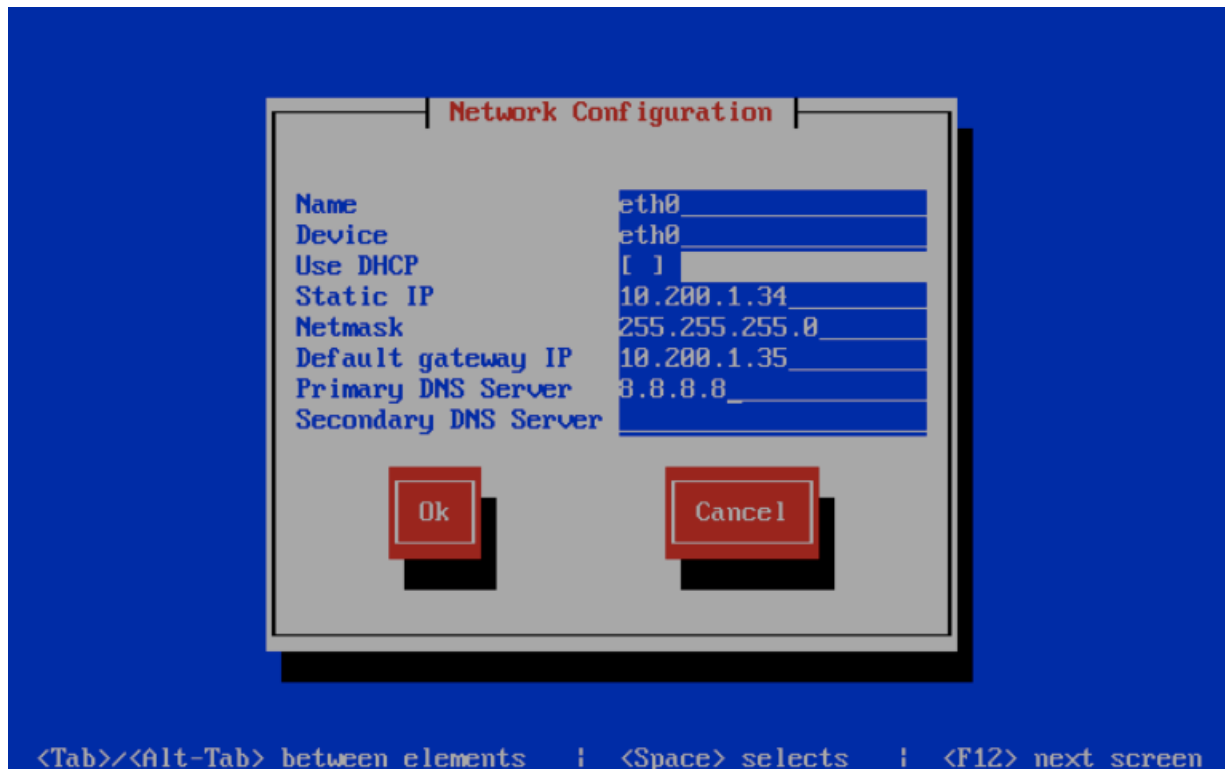
1. Connect to the XR2000.
2. Type the following command to start the script:

```
setup
```

The **Choose a Tool** window is shown.



3. Select **Network configuration**, then choose **Run Tool**.
4. Select **Device configuration**, and then the interface (eth0 or eth1) that you want to configure. The interface's configuration is displayed.



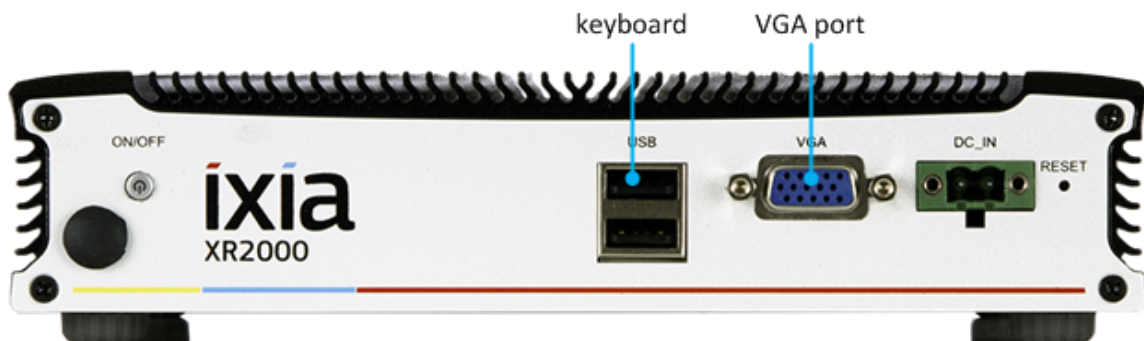
5. Configure the interface settings, then choose **OK** to save the changes.
6. When the script ends, type exit to sign off.

If you want to register the XR2000 with a Hawkeye server, continue with [Register with a Hawkeye Server](#).

First time setup through VGA and USB

To perform first-time setup through VGA and USB, do the following:

1. Connect a monitor to the VGA port, and a keyboard to one of the USB ports.

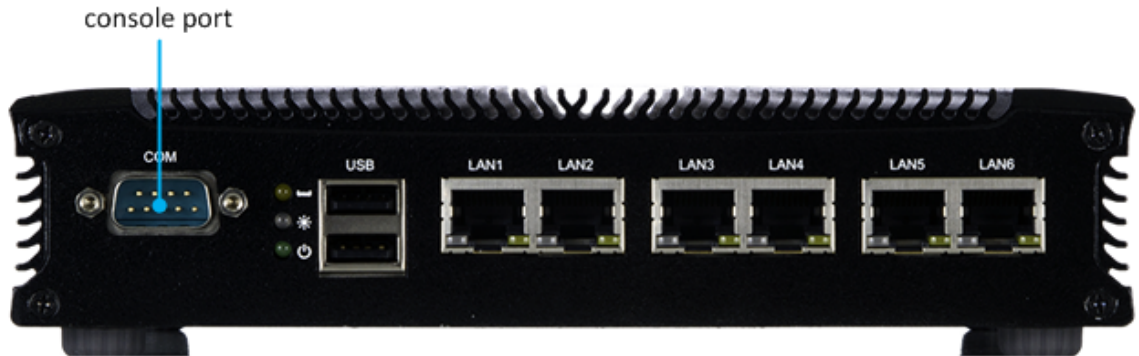


2. Power on the XR2000.
A console window is displayed.
3. Now that you have connected to the XR2000, continue with the setup script.

First time setup through the console port

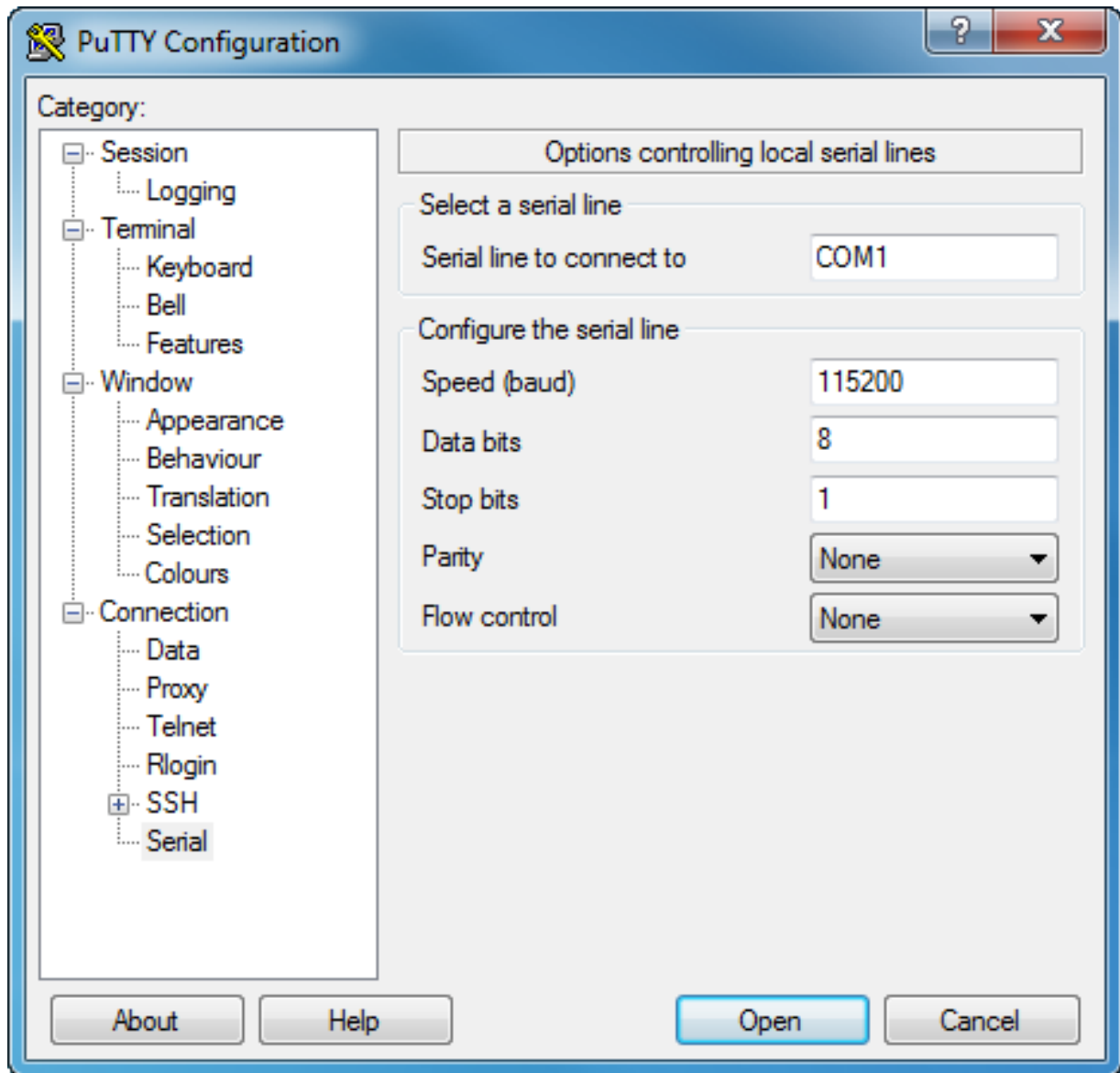
To perform first-time setup through the console port:

1. Connect a rollover cable or RJ-45 to DB-9 female (Cisco console cable) to the XR2000's console port.



2. Power on the XR2000.
3. On the computer, start a terminal application (such as PuTTY or minicom), and establish a serial connection to the XR2000:

Parameter	Value
Speed	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	None



When a successful connection is established, a terminal window is displayed.

4. Now that you have connected to the XR2000, continue with the setup script.

Source-based routing

When using multiple interfaces on the XR2000, it is impossible to configure multiple default gateways because all the interfaces share the same routing table. To customize the interface routing, you can either configure static routes to remote hosts, or use source based routing. Source-based routing allows each interface (physical and logical) to have its own routing table, including default routes.

To configure source-based routing, you use a text editor such as `vi` to edit script files stored on the XR2000. Each logical interface or VLAN ID must have its own script file. Store the scripts in the following folder:

```
/etc/sysconfig/network-scripts
```

Name the scripts according to the logical interface or VLAN ID that they control. For example, to configure `eth0`, you edit the `ifcfg-eth0` script. If a script file for the interface (or combination of VLAN ID and interface) does not already exist, you must create it in the editor.

To configure source-based routing, complete the following steps:

1. Connect to XR2000 by using one of the first time setup methods, and open a console window.
2. Start a text editor, such as `vi`.
3. Set the path to the `/etc/sysconfig/network-scripts` folder, and open the script for the interface that you want to configure.

Scripts are named according to the interfaces that they configure by using the following naming convention:

`ifcfg-<logical_interface>.<vlanId>`

Examples:

- Logical interface: To configure the logical interface `eth0`, edit `ifcfg-eth0`.
- VLAN: To configure the logical interface `eth0`, edit `ifcfg-eth0.25`.

If there is no script file for the interface (or combination of VLAN ID and interface), use the editor to create it.

4. The table below describes the parameters available for the scripts. You can also refer to the examples in this section for examples of how to configure scripts for specific configurations.

Parameter	Description
<code>BOOTPROTO=</code>	Boot-time protocol used to obtain an address for the interface: <code>dhcp</code> = DHCP <code>none</code> = No protocol <code>static</code> = Use static address information configured in this script file Example: <code>BOOTPROTO=dhcp</code>
<code>BROADCAST=</code>	Broadcast IP address Example: <code>BROADCAST=192.168.1.255</code>
<code>DEFROUTE=</code>	Always set <code>DEFROUTE</code> to <code>no</code> , so that the default route in the default routing table will not be used. Example: <code>DEFROUTE=no</code>
<code>DEVICE=</code>	Logical interface that the script configures: Logical interface: <code>ethx</code> Example: <code>DEVICE=eth0</code> VLAN interface: <code>ethx.vlanId</code> Example: <code>DEVICE=eth0.25</code>
<code>GATEWAY=</code>	Always set this value to null to exclude the default gateway from the default routing table. Example: <code>GATEWAY=""</code>

HWADDR=	MAC address of the card Example: <code>HWADDR=4C:02:89:00:F3:90</code>
IPADDR=	IP address of the interface (static IP addressing only) Example: <code>HWADDR=4C:02:89:00:F3:90</code>
IPV6INIT=	Enable IPv6 addressing on the interface. Example: <code>IPV6INIT=no</code>
MACADDR=	Specify a value for this parameter only if you want to spoof a MAC address. Example: <code>MACADDR=4C:02:89:00:F3:26</code>
NETMASK=	Network mask for IP address (static IP addressing only) Example: <code>NETMASK=255.255.255.0</code>
NETWORK=	Network address Example: <code>NETWORK=192.168.1.0</code>
NM_ CONTROLLED=	Allow or deny changes from the web interface Example: <code>NM_CONTROLLED=yes</code>
ONBOOT=	Activate the interface at boot time Example: <code>ONBOOT=yes</code>
TYPE=	Interface type Example: <code>TYPE=Ethernet</code>
VLAN=	Enable VLAN routing on the interface Example: <code>TYPE=Ethernet</code>

- After configuring and saving the script file, you need to create separate routing tables for each logical interface that need specific default gateways.

To do this, edit the `/etc/iproute2/route_tables` file, and add as many tables as you need for your configuration. For each new table, you need a table identifier and a table name.

NOTE

You can use any name you want for the tables, but when using VLANs, we recommend you to use the VLAN ID and part of the table name as the table identifier. See the example below, where VLAN 25, 26 and 27 were defined over `eth0`.

Example:

```
# cat route_tables
#
# reserved values
#
255 local
254 main
253 default
0 unspec
```

```
#
# local
#
#1 inr.ruhep
25 vlan25table
26 vlan26table
27 vlan27table
```

6. After you create the tables, you need to add the routes and rules for each table/logical interface. To do this, you create two files in the `etc/sysconfig/network-scripts` folder for each table/logical interface: `route-ethx` and `rule-ethx`.

For example, assume the following:

- VLANs 25, 26 and 27 were created on top of `eth0`.
- The VLAN IPs are: 10.25.0.2, 10.26.0.2, and 10.27.0.2.
- The IPs' corresponding gateways are: 10.25.0.1, 10.26.0.1, and 10.27.0.1.

Under these conditions, the following files must be created:

```
/etc/sysconfig/network-scripts/route-eth0.25
/etc/sysconfig/network-scripts/route-eth0.26
/etc/sysconfig/network-scripts/route-eth0.27
/etc/sysconfig/network-scripts/rule-eth0.25
/etc/sysconfig/network-scripts/rule-eth0.26
/etc/sysconfig/network-scripts/rule-eth0.27
```

The content of `/etc/sysconfig/network-scripts/route-eth0.25` would be:

```
default table vlan25table via 10.25.0.1
```

while the content of `/etc/sysconfig/network-scripts/rule-eth0.25` would be:

```
from 10.25.0.2 table vlan25table
```

The `route-eth0.26`, `route-eth0.27`, `rule-eth0.26`, and `rule-eth0.27` files should have similar content.

7. When you have finished, restart the network service using the `service network restart` command.

Important pointers on using source based routing

- When source-based routing is configured and you want to test the connectivity with a destination, you must use the `-I` switch to specify the source IP that you want to use. For example, to test connectivity from interface IP 10.25.0.2 to destination IP 8.8.8.8, use: `ping 8.8.8.8 -I 10.25.0.2`. If 8.8.8.8 is reachable from the 10.25.0.2 interface, the ping should work. A simple `ping 8.8.8.8` command will not work, even if you have internet connectivity.
- In some cases, you may need to add a default route for the entire system. In this case, you need to add a default route to the default routing table. To add a default route for the entire system, configure the `GATEWAY` parameter in one of the `ifcfg-ethx` files (if the interface uses a static IP address), or configure `DEFROUTE=yes` if the interface uses DHCP. Also, you can add routes under default routing table, using normal commands, in which you do not need to specify the name of the table.

A PPPoE connection uses the predefined default routing table and will automatically add a default route for the system.

- To display the routes corresponding to a specific table, use the following command `ip route show table <table_name>`.
- To display the routing rules created on the system, use the `ip rule` command. Make sure that there are no duplicate entries for a table.
- Inside the specific routing tables, add as many supplementary routes as you need.
- We recommend source based routing only when multiple gateways are required.
- For routing to specific destinations, use static routes instead.
- If a probe has multiple interfaces, in the Hawkeye GUI you need to add the probe multiple times, using various names, but with the same serial number. Management and test addresses must be configured in various ways, in order to match your testing requirements.

DHCP Example

The following example shows how to configure interface `eth0` for DHCP (script file `ifcfg-eth0`).

Parameter	Description
<code>BOOTPROTO=dhcp</code>	Enable DHCP
<code>HWADDR=4C:02:89:00:F3:90</code>	Replace the MAC value with the actual MAC address of the card.
<code>MACADDR=4C:02:89:00:F3:26</code>	Include this line only if you want to have a spoofed MAC address.
<code>NM_CONTROLLED=yes</code>	Set to <code>no</code> if you do not want to allow changes from the web interface.
<code>TYPE=Ethernet</code>	Set the interface type to ethernet.
<code>IPV6INIT=no</code>	Set to IPv4.
<code>DEVICE=eth0</code>	Interface <code>eth0</code>
<code>DEFROUTE=no</code>	<code>DEFROUTE</code> must be <code>no</code> to keep the default route out of the default routing table.
<code>ONBOOT=yes</code>	Applies on start up.

Static IP Example

The following example shows how to configure interface `eth0` with a static IP address (script file `ifcfg-eth0`).

Parameter	Description
<code>BOOTPROTO=static</code>	Enables static IP address.
<code>HWADDR=4C:02:89:00:F3:90</code>	Replace the MAC value with the actual MAC address of the card.

MACADDR=4C:02:89:00:F3:26	Include this line only if you want to have a spoofed MAC address.
NM_CONTROLLED=yes	Set to no, if you do not want to allow changes from the web interface.
TYPE=Ethernet	Set the interface type to ethernet.
IPV6INIT=no	Set to IPv4
DEVICE=eth0	Interface eth0
IPADDR=192.168.1.10	Set to the required IP address (IPv4)
NETMASK=255.255.255.0	Set to the required Netmask.
BROADCAST=192.168.1.255	
NETWORK=192.168.1.0	
GATEWAY=""	Set this parameter to null to keep the default gateway out of the default routing table.
ONBOOT=yes	Applies on start up

VLAN and DHCP Example

The following example shows how to configure VLAN ID 25 on logical interface eth0 for DHCP (script file ifcfg-eth0.25).

Parameter	Description
BOOTPROTO=dhcp	Enables DHCP
HWADDR=4C:02:89:00:F3:90	Replace the MAC value with the actual MAC address of the card.
MACADDR=4C:02:89:00:F3:26	Include this line only if you want to have a spoof MAC address.
NM_CONTROLLED=yes	Set to no if you do not want to allow changes from the web interface.
TYPE=Ethernet	Set the interface type to ethernet.
IPV6INIT=no	Set to IPv4
DEVICE=eth0.25	Set the VLAN ID to 25
DEFROUTE=no	DEFROUTE must be no to keep the default route out of the default routing table.
VLAN=yes	Enables VLAN
ONBOOT=yes	Applies at start up

VLAN with no IP Address Example

The following example shows how to configure a VLAN (ID 25) with no IP address to create a PPPoE connection on top (script file ifcfg-eth0.25).

Parameter	Description
BOOTPROTO=none	Sets no IP address
HWADDR=4C:02:89:00:F3:90	Replace the MAC value with the actual MAC address of the card.
MACADDR=4C:02:89:00:F3:26	Include this line only if you want to have a spoof MAC address.
NM_CONTROLLED=yes	Set to no if you do not want to allow changes from the web interface.
TYPE=Ethernet	Set the interface type to ethernet.
IPV6INIT=no	Set to IPv4
DEVICE=eth0.25	Set the VLAN ID to 25
VLAN=yes	Enables VLAN
ONBOOT=yes	Applies at start up

VLAN with Static IP Example

The following example shows how to configure VLAN ID 25 on eth0 with a static IP address (script file ifcfg-eth0.25).

Parameter	Description
<code>BOOTPROTO=static</code>	Enables the static IP address.
<code>HWADDR=4C:02:89:00:F3:90</code>	Replace the MAC value with the actual MAC address of the card.
<code>MACADDR=4C:02:89:00:F3:26</code>	Include this line only if you want to have a spoof MAC address.
<code>NM_CONTROLLED=yes</code>	Set to <code>no</code> if you do not want to allow changes from the web interface.
<code>TYPE=Ethernet</code>	Set the interface type to ethernet.
<code>IPV6INIT=no</code>	Set to IPv4
<code>DEVICE=eth0.25</code>	Set the VLAN ID to 25
<code>IPADDR=192.168.1.10</code>	Set to the required IP address (IPv4).
<code>NETMASK=255.255.255.0</code>	Set to the required netmask.
<code>BROADCAST=192.168.1.255</code>	
<code>NETWORK=192.168.1.0</code>	
<code>GATEWAY=""</code>	Set this parameter to null to keep the default gateway out of the default routing table.

Register with Hawkeye server

Automatic endpoint

Keysight includes a script that allows XR2000 to automatically register itself with an Hawkeye server. If you do not want to do this, you can move on to the web setup. Later you can run the script or use the web interface to configure auto-registration.

To automatically register with Hawkeye server, do the following:

1. Connect to XR2000.
2. Type the following command to start the script:

```
xr2000_configure
```
3. When the script prompts you, enter the following:
 - A name for the probe. You can use letters, numbers, and hyphens (-) in the name. The name will be used by Hawkeye to set the hostname, and it is displayed as the probe name.

- The host name or IP address of the Hawkeye server (public IP if in cloud).

NOTE The name cannot contain spaces.

4. If you want to configure the advanced features of XR2000, continue with the web setup process.

Upgrade XR2000

Following instructions are valid for XR2000 and XR2000_vm probes.

Overview of XR2000 upgrade

XR2000 needs the following upgrades:

- Update operating system so that security levels are maintained.
- Update Ixia software on the endpoint for manual probes.
- Apply Ixia software patch.

Following instructions are valid for XR2000 and XR2000_vm endpoints.

NOTE Any XR2000 upgrade to latest Hawkeye server release, where the XR2000 is on a version prior to 9.x, we recommend to first update the operating system and then perform manual upgrade.

Register with Hawkeye Server

When an automatic endpoint is connected to the Hawkeye server, Hawkeye server will automatically upgrade the endpoint to the required software version. You can confirm this from the Hawkeye server web UI in the **Auto Probe Management** page. Select the endpoint, to display the details of the endpoint including the version.

Upgrade XR2000 from internet without Hawkeye server

To upgrade manual endpoints from internet, do the following:

1. When the XR2000 has internet connectivity, connect to XR2000 with SSH.
2. Run:

```
cd /tmp
wget https://ixiapublic.s3.amazonaws.com/hawkeye/xr2000_upgrade.tar.gz
tar zxvf xr2000_upgrade.tar.gz
cd xr2000_upgrade
./ixia_chariotprobe_install.sh
cd ..
rm -rf xr2000_upgrade
rm -rf xr2000_upgrade.tar.gz
```

3. If the XR2000 does not have internet connectivity copy the file at the https://ixiapublic.s3.amazonaws.com/hawkeye/xr2000_upgrade.tar.gz location, copy on USB drive to XR2000 and place in /tmp folder. Then run the procedure:

```
tar zxvf xr2000_upgrade.tar.gz
cd xr2000_upgrade
./ixia_chariotprobe_install.sh
cd ..
```

```
rm -rf xr2000_upgrade
rm -rf xr2000_upgrade.tar.gz
```

NOTE

A reboot after upgrade is necessary.

Upgrade operating system

You must be connected to internet to upgrade operating system. You cannot upgrade operating system without accessing public servers.

IMPORTANT

Do not upgrade your operating system. The packages are constantly being upgraded and may not function with a specific version of the Hawkeye Server. If the operating system upgrade is required, please contact Keysight Customer Support for assistance as it is preferred to update only required packages.

1. To perform upgrade, sign in as root and type in:

```
yum update -y
yum clean all
```

2. To keep compatibility with the bittorrent test type in Hawkeye, the following library needs to be downgraded after yum upgrade:

```
yum downgrade libtorrent -y
```

Linux Quick Reference

This section lists some standard Linux commands that you may find helpful with the XR2000.

NOTE

After capturing data, you can use the web interface remote tools **Upload** and **Download** to load the .enc file and open it with Wireshark on a windows PC.

Command	Descriptions
netstat	Displays generic network statistics of the host. If you include the <code>-an</code> and <code>-rn</code> arguments, <code>netstat</code> displays the routing table and the application ports open on the XR2000, as well as their respective output. With no arguments, <code>netstat</code> displays the active connections and the used sockets.
passwd	Changes the password for the current user.
route	Displays routing table information.
ifconfig	Displays the IP address and netmask associated with each Ethernet port. Also displays details/counts of packets/bytes of traffic on each port.
route	Displays the routing table information.
tcpdump	Displays the packets on an interface. To use for a specific interface: <code>tcpdump -i eth0</code>

	To use with no ssh port:	<code>tcpdump -i eth0 not port 22</code>
	To export the command output to a file:	<code>tcpdump -i eth0 not port 22 -w /tmp/mycapture.enc</code>

XR3000

This section provides information about XR3000.

Initial configuration

This section describes the initial configuration of the Hawkeye.

First time log in

There are three methods you can use to log in and access the Hawkeye:

Console:	Directly through the console port, using the supplied Micro-USB cable
DHCP:	By allowing the Hawkeye to obtain a DHCP address
Static:	From a static IP address on the host PC

Each method is described below.

Logging in through the console:

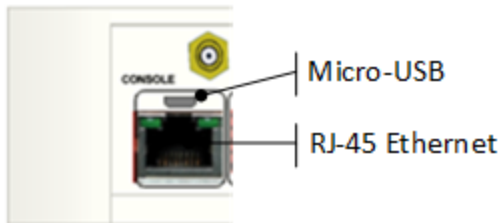
NOTE

If you want to use the Micro-USB connector on the console port, you may need to install a virtual COM port (VCP driver) on the host PC. Many modern operating systems already have a native driver for the console port. If yours does not, you can download a VCP driver from the following location:

<http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

For Windows host PCs, download the Universal Windows Driver version of the VCP driver installer.

1. Connect a console cable from the host PC to the Hawkeye console port.



2. On the host PC, open a PC terminal emulator session for the console port.
3. Configure the terminal settings as follows:

Baud rate	115200
Data	8 bit
Parity	None
Stop	1 bit
Flow control	None

4. Insert the AC line cord into the input connector of the desktop power supply.
5. Plug desktop power supply output connector into unit 12 VDC input jack.
The unit will automatically power up -- you do not need to press the power button.
During the boot process, various messages will display on the serial console while the bootloader and Linux come up.
6. At the Linux prompt, log in using the following credentials:

User name	ksuser
Password	keysight

Logging in through a DHCP address:

1. Connect an Ethernet cable from a switch to port 1 on the Hawkeye.
2. Insert the AC line cord into input connector of the desktop power supply.
3. Plug the desktop power supply output connector into unit 12 VDC input jack.
The unit will automatically power up -- you do not need to press the power button.
4. Check your DHCP server for the IP address issued to the Hawkeye.
The default hostname is xr3k-XXXX where the XXXX is the last 4 digits of the serial number
5. Open an SSH session to the Hawkeye IP address.
6. At the Linux prompt, log in using the following credentials:

User name	ksuser
Password	keysight

Logging in through a static address:

1. Connect an Ethernet cable from the host PC to port 1 on the Hawkeye.
2. On the host PC, configure the PC with a static IP address on the Ethernet interface in the 192.168.0.0/24 subnet.
3. Insert the AC line cord into the input connector of the desktop power supply.
4. Plug the desktop power supply output connector into the Hawkeye 12 VDC input jack.
The unit will automatically power up -- you do not need to press the power button.
5. SSH to the Hawkeye default IP address: 192.168.0.10.
6. At the Linux prompt, log in using the following credentials:

User name	ksuser
Password	keysight

Setting the password

You can use the `passwd` command to change the password for the username that you are logged in as.
The default password for both usernames is `keysight`.

```
ksuser@xr3k-0015:~$ passwd
Changing password for ksuser.
Current password:
New password:
Retype new password:
```

Setting the hostname

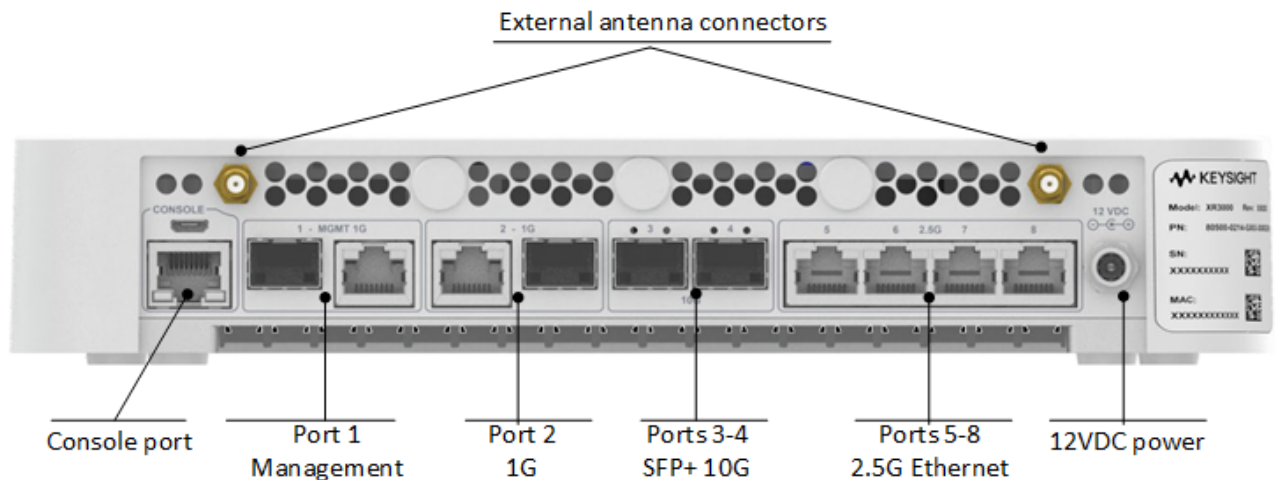
The default hostname is `xr3k-XXXX` where the `XXXX` is the last 4 digits of the unit's serial number.

You can use the `changeHostname` command to change the hostname:

```
ksuser@xr3k-0015:~$ changeHostname <new_hostname>
```

Configuring networking

The Hawkeye supports 1Gbps, 2.5 Gbps, 10Gbps and Wifi-6 interfaces.



Configuring wired networking

The section describes how to configuring the wired interfaces.

1. To configure the interfaces, run the `interfaceConfigure` script.
2. At the prompt, select the interface you want to configure.

```
# ksuser@xr3k-0015:~$ interfaceConfigure
1 : p01_1g (enp2s0f1)
2 : p02_1g (enp2s0f0)
...
8 : p08_25g (enp7s0)
e : EXIT
Please select an interface to configure: 1
Chosen interface is: enp2s0f1
```

3. Configure the address method on the interface.

```
Interface chosen: enp2s0f1
1 : IPv4 Only
2 : IPv6 Only
3 : Both IPv4 and IPv6
e : EXIT
Config interface as: 1
```

4. Optionally, configure the MTU on the interface.

```
Would you like to configure the IPv4 MTU size on this interface? (y/N):
```

5. Configure the address source on the interface.

```
Interface enp2s0f1 currently configured for dhcp IPv4.

1 : dhcp
2 : static
e : EXIT
Config enp2s0f1 interface as: 1
```

6. After the final prompt, the script applies your configuration.

```
Restartng the netplan configurations.
Stopping
Done
```

You can use the `ip a` command to verify the interface configuration.

Run the script again for each interface you want to configure.

Configuring wireless networking

1. Run the `wifiConnect` command to scan for available APs and configure the Wifi-6 interface.

```
ksuser@xr3k-0010: ~$ wifiConnect
running wifiConnect for interface wlp17s0
```

2. Select the access point SSID that you want to use.

```
Quick scanning for Access Points...
0: <HIDDEN> 6e:d7:9a:82:85:e6 (x1)
...
12: Hawkeye (x4)
13: Hawkeye-B's LAN (x1)
14: Hawkeye-ENT (x4)
15: Hawkeye-EnGenius-5GHz (x1)
...
r: RESCAN
Please select an access point SSID: 14
```

3. Select the Desired BSSID.

```
Chosen ssid: Hawkeye-ENT
0 : 34:8a:12:94:04:01 -- Channel= 11, signal level=-79 dBm
```

```

1: 34:8a:12:93:94:c1 -- Channel= 1, signal level=-79 dBm
2: 34:8a:12:94:04:11 -- Channel= 36, signal level=-85 dBm
3: 34:8a:12:93:94:d1 -- Channel= 36, signal level=-89 dBm
a: ANY
Please select an access point BSSID: a
selected bssid: ANY (using 0: 34:8a:12:94:04:01 for parameters)

```

4. Enter the username and password or pre-shared key to complete the configuration.

```

Selected AP params:
SSID=Hawkeye-ENT
BSSID=34:8a:12:94:04:01
Primary Channel: 11
Signal Strength: -79 dBm
Max Data Rate: 144.4 Mbps
RSN version: 1
Group Cipher: CCMP
Pairwise Ciphers: [ CCMP ]
Auth Suites: [ IEEE-802.1X|PMK/RSN|PMK ]

Generating configuration...
Enter Username: devtester
Enter Password: *****
Configuring connection...
Connecting...

```

Utilizing interfaceConfigure command to setup your XR3000

This section covers the steps to configure XR3000 by using the `interfaceConfigure` command. The initial questions, which you must answer each time you run the `interfaceConfigure` command are discussed in this section. This section also explains the following use cases:

- IPv4 DHCP (Dynamic Host Configuration Protocol) interface with custom MTU
- IPv4 Static interface with default MTU

Initial questions when you run the interfaceConfigure command

The Hawkeye Server Interface is the local interface you must use to communicate with the Hawkeye Server. This interface will be configured with a static route to the server.

```

The Hawkeye Server Interface is p01_1g(enp2s0f1), would you like to change it? (y/N): y
1 : p01_1g (enp2s0f1)
2 : p02_1g (enp2s0f0)
3 : p03_10g (enp3s0f0)
4 : p04_10g (enp3s0f1)
5 : p05_25g (enp4s0)
6 : p06_25g (enp5s0)
7 : p07_25g (enp6s0)
8 : p08_25g (enp7s0)
9 : wifi (wlp17s0)

```

Select the interface to the Hawkeye Server.

The next question prompts you to select an interface to configure or enter `e` to exit the script if you only wanted to change the Hawkeye Server interface.


```

1 : p01_1g (enp2s0f1)
2 : p02_1g (enp2s0f0)
3 : p03_10g (enp3s0f0)
4 : p04_10g (enp3s0f1)
5 : p05_25g (enp4s0)
6 : p06_25g (enp5s0)
7 : p07_25g (enp6s0)
8 : p08_25g (enp7s0)
9 : wifi (wlp17s0)
e : EXIT

```

Select an interface to configure: 4

USE CASE 1: Configure an interface as IPv4 DHCP with custom MTU

1. When prompted to select if the previously chosen interface should be configured for IPv4, IPv6, or both, select one of the following:

```

Chosen interface is: p04_10g (enp3s0f1)
1 : IPv4 Only
2 : IPv6 Only
3 : Both IPv4 and IPv6
e : EXIT
Config interface as: 1

```

2. Now configure the Custom MTU size to 7500.

```

Would you like to configure the IPv4 MTU size on this interface? (y/N): y
Enter new IPv4 MTU (9000): 7500
Good MTU size entered: 7500

```

3. The system will tell you if the interface is currently configured as DHCP or Static and prompt you for what you would like to make it now. In this case, you should select 1 to continue utilizing DHCP addressing.

```

Interface enp3s0f1 is currently configured for dhcp IPv4.
1 : dhcp
2 : static
e : EXIT
Config enp3s0f1 interface as: 1

```

4. Next, you will be asked about using the interface under configuration as the default route for the system. you select no, system will show with the current interface that holds the default route and will prompt you to confirm it to continue.

```

Would you like p04_10g(enp3s0f1) to be the default route interface for IPv4? (Y/n): n
The current DEFAULT route interface is p01_1g(enp2s0f1)
Would you like p01_1g(enp2s0f1) to continue to be the default route? (Y/n): y

```

5. Lastly, you must confirm if you want to configure any other interfaces before exiting the script.

```

Would you like to configure another interface? (Y/n): n

```

USE CASE 2: Configure an interface as IPv4 Static with default MTU

1. In the next prompt, you must select if the previously chosen interface should be configured for IPv4, IPv6 or Both.

```

Chosen interface is: p05_25g (enp4s0)

```

```

1 : IPv4 Only
2 : IPv6 Only
3 : Both IPv4 and IPv6
e : EXIT
Config interface as: 1

```

2. To utilize the default MTU size of 1500 you must answer (N) in the following question.

```

Would you like to configure the IPv4 MTU size on this interface? (y/N): N

```

3. The system will tell you if the interface is currently configured as DHCP or Static and prompt you for what you would like to make it now. In this case, 2 is selected to configure the interface for STATIC addressing.

```

Interface enp4s0 currently configured for dhcp IPv4.

```

```

1 : dhcp
2 : static
e : EXIT
Config enp4s0 interface as: 2
Enter static IPv4 address: 192.168.172.85
Good IPv4 Address entered: 192.168.172.85
Enter Netmask (255.255.255.0):
Good Netmask entered: 255.255.255.0

```

4. After configuring the IP address and Netmask for your static network config, specify if you want to enter a gateway (next hop address) for this network. This will be used to create any needed static routes and to configure a system default route.

```

Would you like to enter an IPv4 gateway (next hop address)? (Y/n):y
Enter IPv4 gateway (next hop address): 192.168.172.1

```

5. Next, add search domains. These will be used when looking up non FQDN host names.

```

No Search Domains for interface enp4s0
Would you like to enter a Search Domain? (y/N): y
Enter new Search Domain: mycompany.com
Would you like to enter another Search Domain? (y/N): y
Enter new Search Domain: it.mycompany.com
Would you like to enter another Search Domain? (y/N):
1 : mycompany.com
2 : it.mycompany.com
n : No
Would you like to order your Search Domains (Select number of first Domain or n for No):
n

```

6. Add DNS servers.

```

No DNS servers for interface enp4s0
Would you like to enter an IPv4 DNS server? (y/N): y
Enter IPv4 DNS server (8.8.8.8): 1.1.1.1
Would you like to enter another IPv4 DNS server? (y/N): n

```

7. Finally, you can make the current interface as the default route for the entire system.

```

Would you like p05_25g(enp4s0) to be the default route interface for IPv4? (Y/n): y
Lastly, you are asked if you want to configure any other interfaces before exiting the script.
Would you like to configure another interface? (Y/n): n

```

Connecting to the Hawkeye server

Use the `probeConfigure` command to connect the Hawkeye to the Hawkeye server that will control it.

1. Execute the `probeConfigure` command.

```
ksuser@xr3k-0015:~$ probeConfigure
```
2. Press Enter to skip the Probe/Host Name prompt.

```
Probe/Host Name (xr3k-0001):
```
3. Specify the hostname of the Hawkeye server:

```
Hawkeye Server (hawkeye-server):<hawkeye_server_hostname>
```
4. Choose whether to require the Hawkeye server to supply valid SSL certificates to the Hawkeye:

```
Require valid server certificates? (y/N):
```

By default, a Hawkeye server uses a self-signed SSL certificate.

- If the Hawkeye server is still using the default self-signed certificate, enter `n` (no).
- If the default certificate has been replaced with a valid certificate from a Certificate Authority (CA), enter `y` (yes). The Hawkeye will require a valid certificate from the server to connect to it.

Once the `probeConfigure` is complete, the Hawkeye connects to the Hawkeye server. If any updates are available from the server, the Hawkeye downloads and applies them. The Hawkeye may restart after the updates.

At this point, the Hawkeye is ready for use. You can use the Probes page on the Hawkeye server to confirm that the Hawkeye is connected to it.

Advanced administration

Advanced networking

The Hawkeye supports a single interface with a default route and additional interfaces with only a route for their subnets. If you need to use advanced routing, you can enable an admin account that allows you to use Linux networking commands to create more a complex routing configuration.

IMPORTANT Any changes you make using the admin user account will not be supported by Keysight. If you use the admin account to change the system configuration and then experience routing and connectivity issues, Keysight Support will ask you to re-image the Hawkeye to return it to its factory default settings and before performing any further troubleshooting.

To enable the admin user account:

1. Run the `enable_ksadmin` command as `ksuser` (see [CLI commands on the next page](#)).
 The Hawkeye prompts you to acknowledge that this account will allow you to make unsupported changes.
2. Acknowledge the prompt.

3. The admin user account is created with the following credentials:

User name	ksadmin
Password	keysight

Logging in under this account will grant you admin rights to the Hawkeye.

CLI commands

The Hawkeye supports the following commands:

Command	Options	Description
probeStatus	-v	Check the status of the Hawkeye. The -v (verbose) option shows output including status of individual components of the total system.
collectLogs	-a	Collect all the open log files and snapshots of the probe's configuration.
probeReboot		Reboot the Hawkeye.
probeShutdown		Turn off the Hawkeye. The device will need to be power cycled to restart.
systemInformation		Display the serial number, UUID, BIOS vendor, and BIOS version.
ksTcpdump	all tcpdump options	ksusers tcpdump.
changeHostname <NewHostName>		Change the hostname of the Hawkeye.
linkstat	-v	Show the status of the Ethernet link.
interfaceConfigure		Configure the Ethernet interfaces on the Hawkeye.
wifiConnect		Configure the wireless interface.
wifiScan		Scans for all available wireless networks and presents a list of SSIDs, BSSIDs, and other available information about those APs.
enable_ksadmin		Enables the ksadmin account which can be used when unsupported routing configurations are required.

		<div data-bbox="695 212 878 258">IMPORTANT</div> Any changes you make using the admin user account will not be supported by Keysight. If you use the admin account to change the system configuration and then experience routing and connectivity issues, Keysight Support will ask you to re-image the Hawkeye to return it to its factory default settings and before performing any further troubleshooting.
--	--	---

Rackmounting

The rackmounting kit is optional.

The rackmount kit contains the following items:

Qty	Description
1	Rack Bracket Assembly
2	Cables, USB3-A to Micro USB3-B
4	Screws, M4 x 30mm Socket Head
6	Cable Ties, 99mm
3	Cable Ties, 300mm

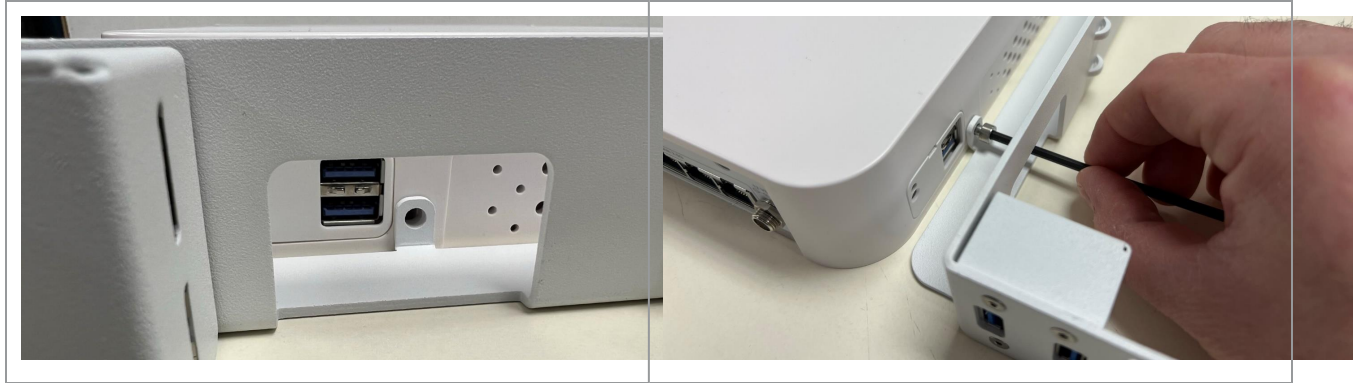
1. Insert the Hawkeye

Insert the Hawkeye into the rackmount bracket, oriented as shown.



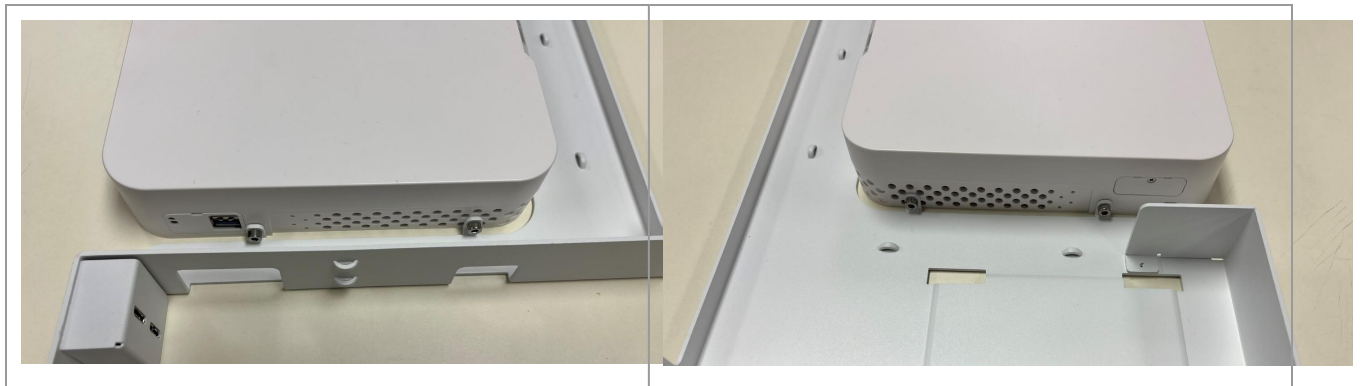
2. Align the mounting holes

Align the mounting holes in the Hawkeye system with the holes located in the tabs on the rackmount bracket. Insert a screw into one of the mounting holes and snug. Do not overtighten.



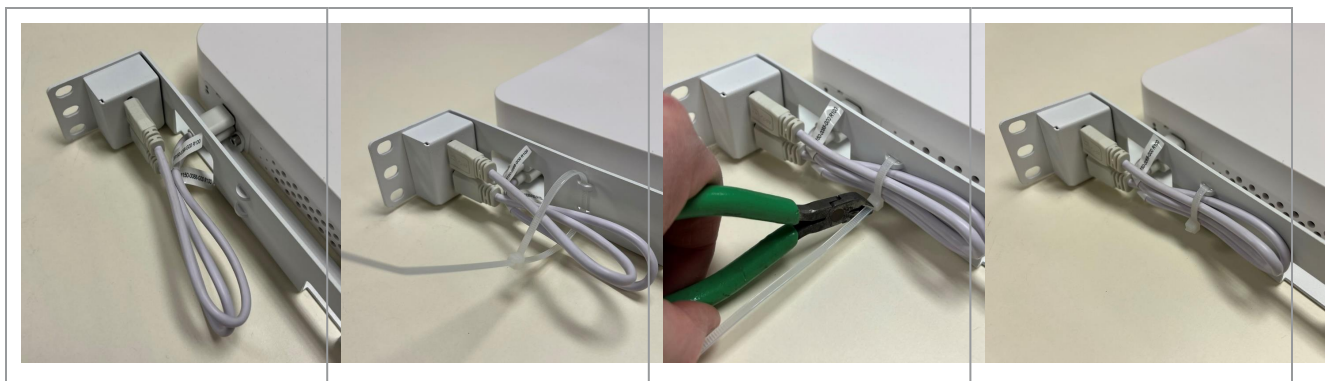
3. Insert remaining screws

Insert the remaining screws into the mounting holes and snug. Do not overtighten.



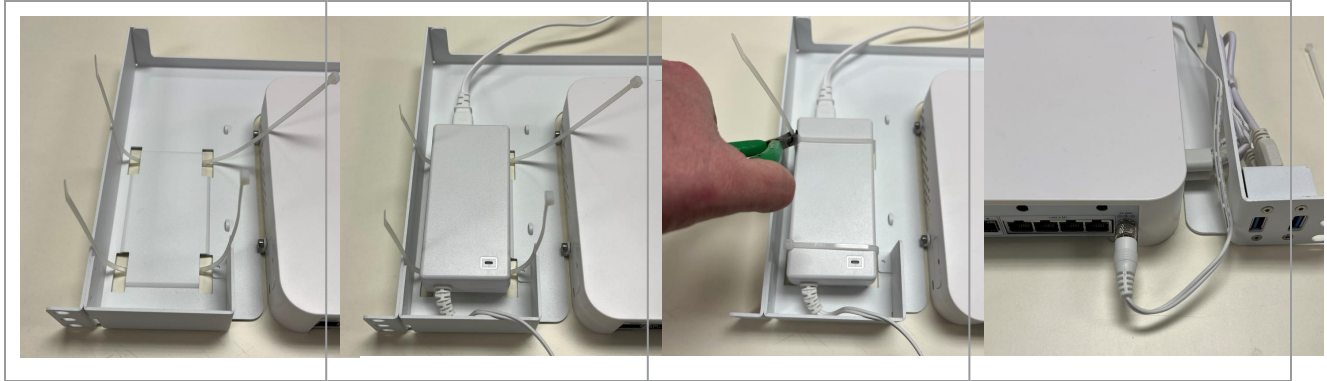
4. Install the USB cables

Install the USB cables between the USB 3.0 Micro B connections on the rackmount bracket and the USB 3.0 Type A connections on the Hawkeye system. Secure the cables in place with a 300mm cable tie passed through the cable tie mounts on the rackmount bracket and snip off the excess.



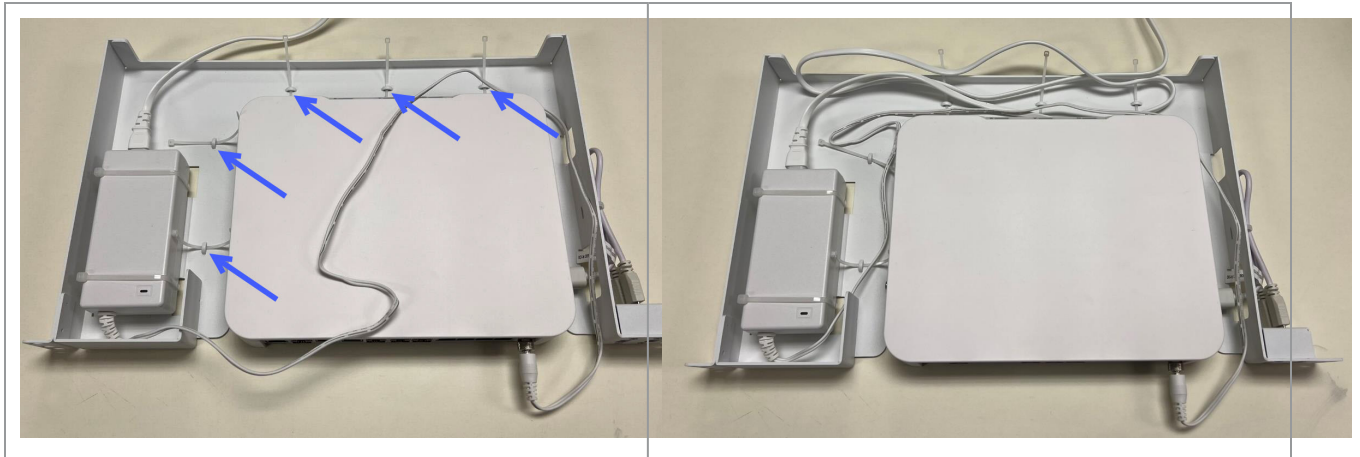
5. Install the power supply

Route two 300mm cable ties underneath the PSU standoff on the rackmount bracket. Place the PSU on the standoff with the cables oriented as shown. Secure the PSU to the rackmount bracket with the cable ties and snip off the excess. Screw power cable into the Hawkeye.



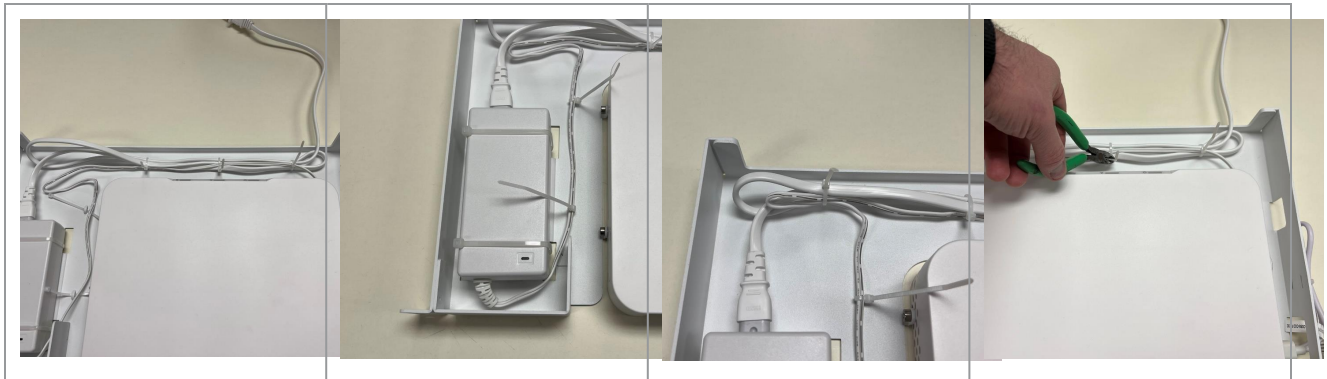
6. Insert cable ties

Route five 99mm cable ties through the cable tie mounts on the rackmount bracket where shown. Bundle the PSU cables and route them around the rackmount bracket as shown.



7. Secure the PSU cables

Secure the PSU cables with the cable ties. If necessary, bundle any excess cable slack and secure with the remaining 99mm cable tie. Snip off the excess.



Wall mounting

The wall mounting kit is optional.



1. Attach the mounts

Attach the mounts to the Hawkeye.



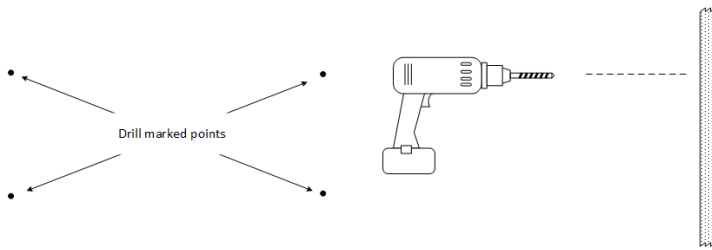
2. Mark the mounts

Position the Hawkeye on the wall where you want to mount it and mark the location of the mounting holes on the wall.



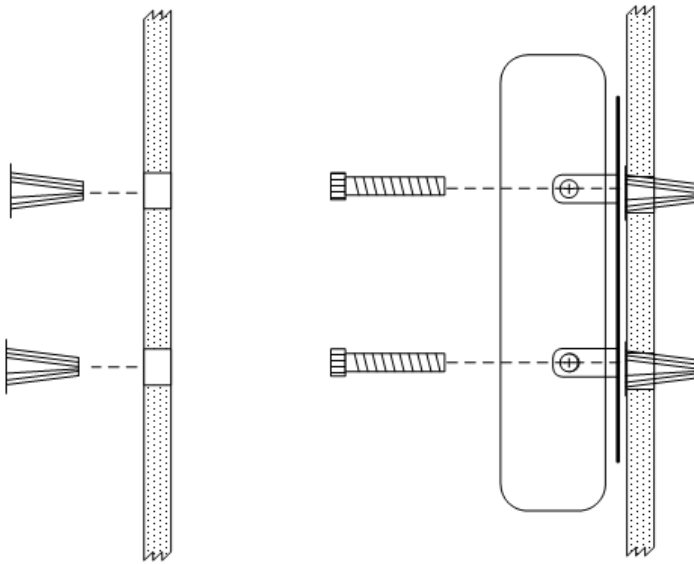
3. Drill the holes

Drill the holes for the mounts.



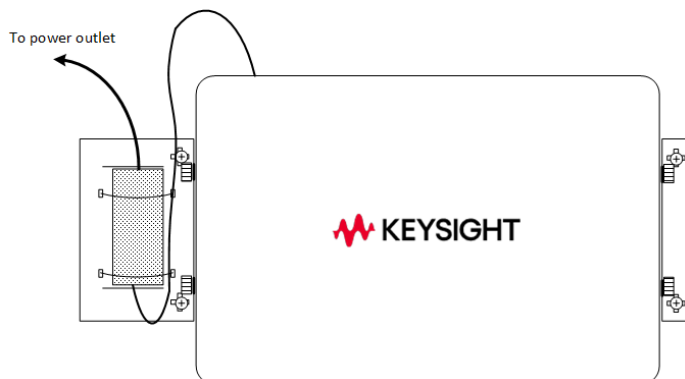
4. Insert the wall anchors

Insert the wall anchors into the drilled holes. Position the Hawkeye on wall and screw the mounts to the wall anchors.



5. Attach the power supply

Attach the power supply to the wall mount bracket with the supplied cable ties. Plug the input power cord into wall socket and the output power cord into the Power socket on the Hawkeye.



XR Docker

The XR Docker image is a docker image, which you can install as a Hawkeye endpoint. You can install the XR Docker image on a platform as an application that is capable of the following:

- Running Node to Node, Mesh, and a limited subset of Real service tests
- Performing scheduled restarts from the Hawkeye Server.

The XR Docker registers as an automatic endpoint to Hawkeye Server.

Hawkeye Server can restart probes on a timed basis. You can restart the probe from **Probe Management**. When the restart is triggered for the XR Docker, IxChariot and RealServiceManager restarted. These are the two main processes on the XR docker that manage tests. Host VM is not impacted, so routes are not re-initialized.

Base platform requirements

- Linux x86 64 bit OS
- 1 Gb RAM
- 1Gb hard drive

Installation

Complete the following steps to create an XR Docker endpoint where internet connectivity is available for base platform to run the XR Docker (endpoint) and only one IP is being used for the base platform. You can install only one XR Docker container on a single base platform.

Contact Keysight Customer support for more advanced installations of XR Docker, such as, multiple IP (multiple subnetworks) support and unavailability of internet connection for Linux base system to obtain the XR docker image.

- We assume you are familiar with Docker environment before attempting XR Docker installation.
- Contact Keysight Customer support to install XR Docker on a host computer without internet connection.
- For some base platform Linux OS such as Ubuntu, the docker package is referenced as docker.io.

Installation steps

1. Install the Docker library and Docker application on the endpoint (Linux) base platform.
2. Transfer the XR Docker install script, located on the Hawkeye Server Web GUI download endpoints web page, to the base platform.
3. Run the install script to simulate a Hawkeye endpoint. You may have to change permissions on the file.


```
# chmod +x install_xr_docker.sh
```
4. The XR Docker endpoint automatically registers with the Hawkeye Server as part of the start up process and registers using the IP of the host platform.

Example of installation of XR Docker onto Debian 12 platform

1. Log (ssh) on as root on XR Docker host platform.
2. Ensure latest libraries and packages are installed for Debian.

```
# sudo apt update
# sudo apt upgrade
```

3. Install Docker package and start application.

```
# sudo apt install docker.io
# sudo systemctl start docker
```

4. The Docker application on the host computer will not survive a reboot by default. We recommend you consider the following command to configure the Docker application to be persistent and remain functional on rebooting the host computer.

```
# sudo systemctl enable docker
```

NOTE

It is your responsibility to apply a restart policy for the XR Docker to restart following a host computer reboot.

5. Transfer the XR Docker image for Hawkeye (located on Hawkeye server - software download web page) to the Debian platform. We recommend you perform this from /tmp directory.
6. Run install script to activate the XR Docker container and create an XR Docker endpoint.

```
# sudo ./install_xr_docker.sh
```

NOTE

You will be prompted to specify the endpoint name and the IP of the Hawkeye Server. The XR Docker endpoint will register with the Hawkeye Server and perform any necessary software upgrade from the server.

7. Confirm XR Docker container (Endpoint) is successfully running with the below command and verify on Hawkeye Server – Probe Management web GUI.

```
# sudo docker ps
```

Sample output

Container ID	Image	Command	Created	Status	Ports	Names
54f755a4ccb9	xr_docker_x86_64:latest	/startup.sh	7 minutes ago	Up 7 minutes	XR-Docker-MC1	

Log files on the XR Docker container can also be accessed for debugging purposes if directed by Keysight customer support.

Recover XR Docker after power failure

1. SSH to the XR_Docker host machine.

```
# docker ps
```

If no entries are found, this means XR-docker is not running and you must recover XR Docker.

2. Confirm the host machine was previously used as an XR-Docker by running the below command to confirm there is an image loaded and it is the correct version.

```
# docker images
```

- Find directory where the XR-Docker installation files were stored by using the find command:

```
# cd /
# find . -name install_xr_docker.sh
# cd <install directory for XR-Docker installation from find command above>
```

- Run the installation script again for XR-Docker.

```
# ./install_xr_docker.sh
```

- Provide the XR-Docker hostname as seen by Hawkeye Server in Probe Management.
- Provide the Hawkeye Server IP.
- Confirm in **Probe Management** on the Hawkeye Server that the new XR-Docker name appears and is in a green working status.

Change endpoint name/Hawkeye server of XR Docker

After installing XR Docker, if you want to change its endpoint name and registered Hawkeye Server, you must stop and restart XR Docker to enter the new endpoint name or the new Hawkeye Server IP. Complete the following steps to do this:

- Log (ssh) onto XR Docker host computer.
- Re-run XR Docker from the directory previously transferred to (ex. /tmp) to set new endpoint name and new Hawkeye Server IP.

```
# ./install_xr_docker.sh
```

- Confirm XR Docker registered on Hawkeye Server – Probe Management web GUI.

Remove or uninstall XR Docker

To remove XR Docker from the host platform, use the following commands:

- Log (ssh) onto XR Docker host computer.
- Run `docker ps` command to get the container name of your current XR Docker.

```
# docker ps
```

Sample output

Container ID	Image	Command	Created	Status	Ports	Names
54f755a4ccb9	xr_docker_ x86_ 64:latest	/startup.sh	7 minutes ago	Up 7 minutes	XR- Docker- MC1	

- Stop the XR docker container.
`docker stop <container ID>`
- Remove docker container from the system.
`docker rm <container ID>`

- Find the image file name.

```
# docker images
```

Sample output:

Repository	Tag	Image ID	Created
xr_docker_x86_64	latest	6c209f438d3b	6 hours ago

- Remove the docker image from the host platform.

```
# docker rmi <image ID>
```

- Remove the install script and image tar from the platform (from the directory you transferred the install script to – recommended/tmp):

```
# rm -rf xr_docker_x86_64.tar install_xr_docker.sh
```

XR Docker debug tips

- You can access the log files on the XR Docker container for debugging if directed by Keysight customer support. The XR Docker container can be accessed with a Linux bash shell with the following command:

```
# docker exec -it <containerid/container name> bash
```

 After you access the container, the following common XR commands are available:

```
# probeVersion
```
- The XR Docker runs as a container on a host computer so the IP routing and port restrictions of the host computer apply. If tests are failing due to connectivity reasons, as seen in Hawkeye test results, check the firewall and iptables settings of the host computer.
- If the XR Docker is flagged as **Private** in **Probe Management** but it is expected to be **Public**, check firewall settings of the host computer.
- If certain real service tests fail or show error on an XR-Docker endpoint but are successful for other endpoints in your network, it can indicate host machine for XR Docker has ports blocked. To identify the issue quickly, run real service test 'traceroute' or to use Linux nmap command from the XR-Docker container. Refer to [Routing and Ports management](#) for more information.
- If multiple XR Docker endpoints are required to be created for the user, a shortcut of downloading and using a local copy of the XR Docker image can be employed as follows:
 - The first installation of an XR Docker endpoint will result in the XR Docker image (.tar) file being downloaded onto a host computer. This TAR file can be copied to the next host computer. Load the XR docker image and then run the install script as follows:

```
# docker load -i <xr docker tar image>
```

 Then run

```
# ./install_xr_docker.sh
```
- Log files on the XR Docker container can also be accessed for debugging purposes if directed by Keysight customer support. Contact Keysight customer support for detailed instructions.
- To clean up unnecessary XR docker image:

```
# docker ps
# docker stop <cntrID>
# docker rm <cntrID>
```

```
# docker images
# docker rmi -f <imageID>
```

8. If the base platform is Ubuntu or similar, it may require commands to be preceded by 'sudo' to execute commands with root access.
9. The XR Docker endpoint may fail to show all test results when it is in a large mesh. Specifically, when the XR Docker endpoint is the hub in a hub and spoke mesh. The reason is the Linux host (often a VM) must route messages to the Docker process, which then routes messages to the docker container. These time delays can sometimes cause incomplete results to be gathered from all endpoints before the XR Docker must report all mesh tests results to the Hawkeye Server. Keysight recommends to use a physical XR endpoint for a large hub mesh.
10. Tests running with the XR docker probe, may have higher latencies, delays, and round trip times than other probe types. This is expected as packets are routed from host physical interface (to optional VM), through docker container, the docker container running as the probe. Other probes do not have this overhead of additional routing and waiting for processing due to layers.
11. If HTTPS tests Error with reason "HTTP SERVER DNS RESOLUTION FAILED", you will need to update /etc/resolv.conf on the host machine to reference a nameserver that can locate the URL in the test. An example line to add to /etc/resolv.conf would be:nameserver 8.8.8.8.

XR-VM

The XR-VM is a Debian 12 based virtual probe delivered as both an OVA or Qcow2. It is the replacement for the XR2000-VM to provide a more secure system for the future. The XR-VM is supported in the same virtual environments as the Hawkeye Server.

Requirements for XR-VM installation

VMware solution

Following are the software requirements for delivering XR-VM as an OVA image, which is hosted within a virtualization (VMware) solution.

- VMware ESXi 7.0 or higher (qualified with 7.0u3)

The XR-VM virtual image requires 64-bit support from the host operating system or from the specific hypervisor. The CPU virtualization instructions, such as, Intel VT-x and AMD-V must be supported and enabled.

KVM/OpenStack solution

You can install XR-VM probe on a Linux system running Debian 12 or equivalent with KVM. You can install XR-VM probe in OpenStack using version Liberty or higher. The XR-VM virtual image is a 64-bit system.

Hardware Requirements for XR-VM

Minimum Requirements 1vCPU and 2GB RAM.

Configure XR-VM

Following the successful deployment of the provided OVA or QCOW2 image in your Virtualization environment. The following steps will be needed to be taken to connect to your Hawkeye Server

- Login to XR-VM
- Change default Password
- Configure IP Address
- Configure Hostname
- Connect to Hawkeye Server

Login to XR-VM

After deployment use your virtualization system's console solution to access the CLI. The default login for XR-VM is username: `ksuser` and password: `keysight`.

Change Default Password

The default login is `ksuser/keysight`.

If admin access is required, `ksuser` can install an admin (user name: `ksadmin`) account with `sudo` access through the `enable_ksadmin` command.

You can use the `passwd` command to change the password for the user account you are logged in.

The default password for both the accounts is `keysight`.

```
ksuser@xrvvm-0015:~$ passwd
Changing password for ksuser.
Current password:
New password:
Retype new password:
```

Configure IP Address

By default the network interface is configured as DHCP. You can check your assigned IP address using the `ip a` command and checking the IP assigned to `eth0`.

To modify the interface configuration to support IPv4 or IPv6 (DHCP/Static) use the `interfaceConfigure` command:

```
#interfaceConfigure
Only found one interface: eth0
1 : IPv4 Only
2 : IPv6 Only
3 : Both IPv4 and IPv6
e : EXIT
Config interface as: 3
The current DEFROUTE interface is eth0
Would you like eth0 to continue to be the IPv4 default route? (Y/n):
Would you like to configure the IPv4 MTU size on this interface? (y/N):
Interface eth0 currently configured for dhcp.
1 : dhcp
2 : static
```

```

e : EXIT
Config IPv4 interface as: 1
Would you like eth0 to be the IPv6 default route? (y/N): y
Would you like to configure the IPv6 MTU size on this interface? (y/N):
Interface eth0 currently configured as static.
IPv6 Address: 2690:11bf:ac36:c080::b:8008
1 : dhcp
2 : static
e : EXIT
Config IPv6 interface as: 2
Enter static IPv6 address (2690:11bf:ac36:c080::b:8008): 2690:11bf:ac36:c080::b:4004
Would you like to enter an IPv6 default gateway? (Y/n):
Enter IPv6 Gateway (2690:11bf:ac36:c080::b:1):
Current DNS servers (Maximum 3):
8.8.8.8
8.8.4.4
Would you like to delete any current DNS servers? (y/N):
Would you like to enter an IPv4 DNS server? (y/N):
Would you like to enter an IPv6 DNS server? (y/N):
0 : 8.8.8.8
1 : 8.8.4.4
n : No
Would you like to order your DNS Servers (Select number of first DNS Server or n for
No): n
#

```

Changes are applied when the script is completed, and you can verify changes with the “ip a” command

Configure Hostname

To configure the hostname for you XR-VM please use the changeHostname command.

```
# changeHostname <NewHostname>
```

For you new hostname to take effect you will have to reboot the system using the reboot command.

Connect to Hawkeye Server

After your system is configured with access to the network you can now point it to your Hawkeye 4.1 or later Server using the probeConfigure command

```

# probeConfigure
Probe/Host Name (XR-VM):
Hawkeye Server (hawkeye-server):<HawkeyeServerName_IP>

```

XR-E1S

The XR-E1S is a CentOS 7 based probe derived from the Vision E1S. It is the replacement for the Vision E1S to provide the following:

- More performance for the endpoint
- Less restrictions on routing
- Full root access without the packet broker functions

Install XR-E1S

To install the XR-E1S, do the following:

1. Log in to the Vision E1S as user `ksuser`.

NOTE

Do not change the interface configuration before running `install_xr_e1s`. The interface configuration is not maintained between modes.

2. Run the XR-E1S installation script `install_xr_e1s` from the command line. The system auto installs and reboots to the new image when the installation is complete. If your Vision E1S does not have the command `install_xr_e1s`, contact Keysight support before proceeding.

Configure XR-E1S

To configure the XR-E1S, do the following:

1. Sign in to the XR-E1S. After deployment, use your serial connection or ssh to the XR-E1S to access the CLI. Default credential is user name: `root` and password: `keysight`.
2. Change the default password. Use the `passwd` command to change the password for root.

```
#passwd
Changing password for user root.
Changing password for root.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
#
```

3. Connect to the Hawkeye server. After your system is configured with access to the network, you can point it to your Hawkeye server 5.2 or later by using the `probeConfigure` command.

NOTE

The `probeConfigure` command will set the Linux host name.

```
# probeConfigure
Probe/Host Name (xr-e1s):
Hawkeye Server (hawkeye-server):<HawkeyeServerName_IP>
```

XR-E1S CLI commands

The XR-E1S probe supports the following CLI commands:

Command	Options	Description
<code>probeStatus</code>	<code>-v</code>	Checks the Status of the XR-E1S system. <code>-v</code> option shows verbose output including status of individual components of the total system.
<code>collectLogs</code>	<code>-a</code>	Collects all the open log files.

probeVersion		Shows version of the XR-E1S probe.
probeConfigure		Configures the probe name and Hawkeye server.
systemInformation		Shows system information: Serial Number, UUID, BIOS Vender, BIOS Version.
switch_mode		Toggles between Vision E1s (PacketBroker Mode) and XR-E1S (Endpoint Mode).

Software Endpoints

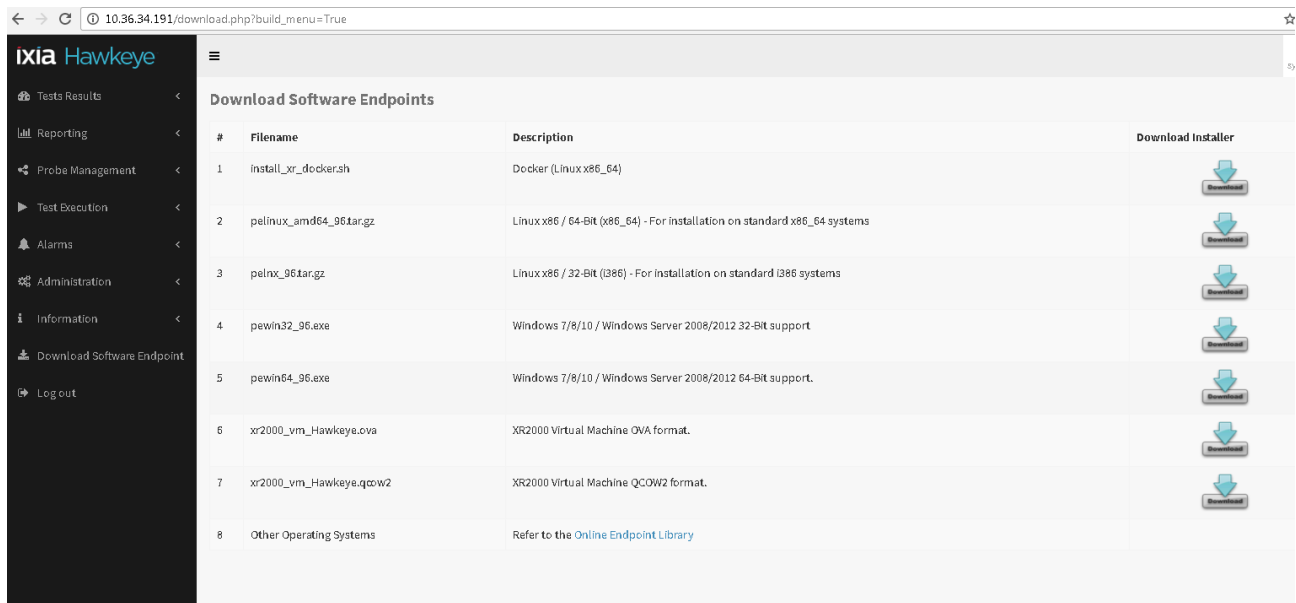
Software endpoints offer the user the ability to use any hardware platform as a Hawkeye endpoint but with the limitation of not being able to run Real Service tests. The XR2000 VM is an exception to this rule.

Different flavors of probes or endpoints can be downloaded from the Hawkeye server software download page or from the link (Online Endpoint Library) provided at the bottom of that page. Some endpoints such as android, iPhone, and Mac IOS, require additional configuration outlined in the Performance Endpoint user guide found from the Online Endpoint Library page.

NOTE

The endpoints available on the Ixia web page are for the most part fully compatible with Hawkeye, but some specific versions may not be completely tested with the current Hawkeye server. We recommend you to download the endpoints from Hawkeye server directly to ensure 100% tested compatibility and stability with the current Hawkeye version.

You can also download from the Hawkeye server directly:



#	Filename	Description	Download installer
1	install_xr_docker.sh	Docker (Linux x86_64)	
2	pelinux_amd64_96.tar.gz	Linux x86 / 64-Bit (x86_64) - For installation on standard x86_64 systems	
3	pelinx_96.tar.gz	Linux x86 / 32-Bit (i386) - For installation on standard i386 systems	
4	pewin32_96.exe	Windows 7/8/10 / Windows Server 2008/2012 32-Bit support	
5	pewin64_96.exe	Windows 7/8/10 / Windows Server 2008/2012 64-Bit support.	
6	xr2000_vm_Hawkeye.ova	XR2000 Virtual Machine OVA format.	
7	xr2000_vm_Hawkeye.qcow2	XR2000 Virtual Machine QCOW2 format.	
8	Other Operating Systems	Refer to the Online Endpoint Library	

Mobile phone endpoints

Android and iOS software endpoints can be found on the respective app stores. Look for the key word IXIA in the application search engine. The application is Hawkeye Endpoint or Ixia Performance Endpoint.

Install software endpoints

For most software endpoints (Windows, Android, and iOS), the installation is very straight forward with a few steps.

The important step is the registration server configuration: the URL or IP address (public) of the Hawkeye server must be filled in for automatic endpoint creation and management.

Install Raspberry Pi endpoints

The following steps need to be performed to create a Raspberry Pi Software Endpoint:

1. On Hawkeye Server UI, select web page for **Download Software Endpoint** to obtain Raspberry PI SW endpoint as a tar file.
2. Copy endpoint tar file to the XRPI and store in `/tmp` directory.
3. Create directory structure for Raspberry Pi

```
# copy pelinux_rasp_pi_2_96.tar to /home/
# tar -xvf pelinux_rasp_pi_96.tar
# cd temp
# cp * /usr/local/Ixia/.
```

4. Obtain the file `/usr/local/Ixia/endpoint.ini` from either a working XRPI or Hawkeye Customer Support and copy to `/usr/local/Ixia/endpoint.ini`
5. Edit (nano) `/usr/local/Ixia/endpoint.ini` and define IP for Hawkeye Server
6. Edit (nano) `/etc/hostnames` to define name for probe.
7. Add entry to `/etc/hosts` for Hawkeye server IP
8. Edit (nano) `/etc/rc.local` and add the following at the end:
`(sleep 10 && /usr/local/Ixia/endpoint 1>>/var/local/endpoint.console 2>&1)&`
9. Reboot Raspberry PI.

```
# reboot
```

NOTE

After reboot to activate wireless network, routes will be wrong. Change the default route to bring it on wlan0.

If you want to enable the Wi-Fi interface use the following steps:

1. Enable Raspberry Pi WIFI

```
# sudo raspi-config
Enable WIFI interface WLAN0
# nano /etc/network/interfaces and add
auto lo
iface lo inet loopback

auto eth0
allow-hotplug eth0
iface eth0 inet dhcp

auto wlan0
iface wlan0 inet dhcp
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

2. Create file to configure WIFI

```
# nano /etc/wpa_supplicant/wpa_supplicant.conf
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
network={
ssid="hawkeye-TP-LINK-1"
```

```
key_mgmt=WPA-EAP
priority=1
auth_alg=OPEN
eap=PEAP
phase2="auth-MSCHAPV2"
identity="testuser"
password="testpw"
}
```

You are responsible for configuring Raspberry Pi firewalls to open required ports.

This page intentionally left blank.

CHAPTER 3

IxProbe Element Manager

Hawkeye provides an element management system for the IxProbe device. Hawkeye provides a unified front-end interface to manage all IxProbes from a single location.

Connect IxProbe to Hawkeye through IxProbe CLI

To connect IxProbe to Hawkeye through IxProbe CLI, use the `set hawkeye` commands to configure Hawkeye.

Syntax

```
set hawkeye endpoint <enabled|disabled>
set hawkeye server <string>
add device ntp server ip <string> state enabled
```

Arguments

Argument	Description
endpoint <enabled/disabled>	Enter <code>enabled</code> to enable the Hawkeye endpoint and <code>disabled</code> to disable it.
server <string>	Enter the Hawkeye server IP address.
NTP server <string>	Enter the IP address of the NTP Server (Recommended the Hawkeye Server)

Example

```
IxProbe > set hawkeye
endpoint Hawkeye endpoint status
server Hawkeye server IP address
IxProbe > set hawkeye endpoint
disabled
enabled
IxProbe > set hawkeye server <ServerIP>
IxProbe > set hawkeye endpoint enabled
IxProbe > show hawkeye endpoint
enabled
IxProbe > add device ntp server ip <NTPServerIP> state enabled
```

NOTE

For IxProbe installation instructions and descriptions of its functionality, see the *IxProbe User Guide*, available on the Ixia Support web page.

IxProbe Element Manager Dashboard

IxProbe Element Manager dashboard has the following views:

- List View
- Grid View
- Detailed View

List view

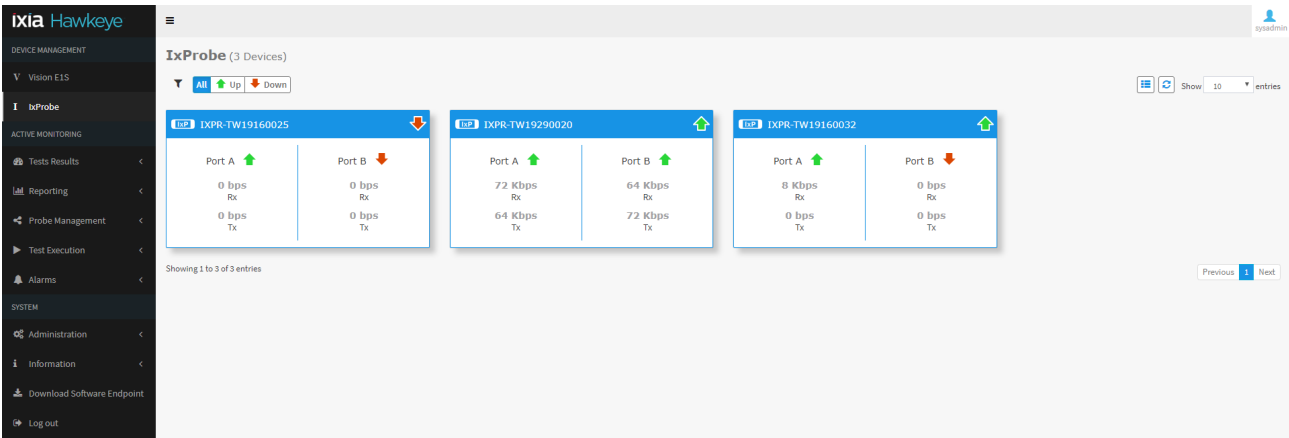
From the list view, you can see the **Status** of the IxProbes connection to the element manager, indicated by red or green status arrows in the **Status** column. You can also view the port status as well as TX and RX rates for each of the two front ports of the IxProbe. From this list view, you can perform bulk configuration actions (see [Perform Bulk Actions on IxProbes](#)) or open individual IxProbe windows to see detailed statistics, additional configuration parameters, system information, and audit trail for each device.

Status	ID	Name	Port A Rx	Port A Tx	Port B Rx	Port B Tx
↓	2	IXPR-TW19160025	0 bps	0 bps	0 bps	0 bps
↑	4	IXPR-TW19290020	72 Kbps	56 Kbps	56 Kbps	72 Kbps
↑	3	IXPR-TW19160032	40 Kbps	80 Kbps	0 bps	0 bps

Grid view

In the list view, select  to view the IxProbes in grids. From grid view, select **Detailed view** in the corresponding IxProbe box to view the detailed information of the individual IxProbes.

Status	ID	Name	Port A Rx	Port A Tx	Port B Rx	Port B Tx
↓	2	IXPR-TW19160025	0 bps	0 bps	0 bps	0 bps
↑	4	IXPR-TW19290020	0 bps	0 bps	0 bps	0 bps
↑	3	IXPR-TW19160032	16 Kbps	0 bps	0 bps	8 Kbps



Detailed view

Select the (+) in **List view** or select any IxProbe device in **Grid view** to view the details for the selected IxProbe. From the detailed view, you can do the following:

- View port statistics
- Make additional configuration changes
- Review audit trail
- View system information

How do I...

This section covers the tasks that you can perform on IxProbe Element Manager:

View port statistics	85
Configure IxProbe	86
View audit trail	88
View system information	89
Perform bulk actions on IxProbes	89
Schedule upgrades	91

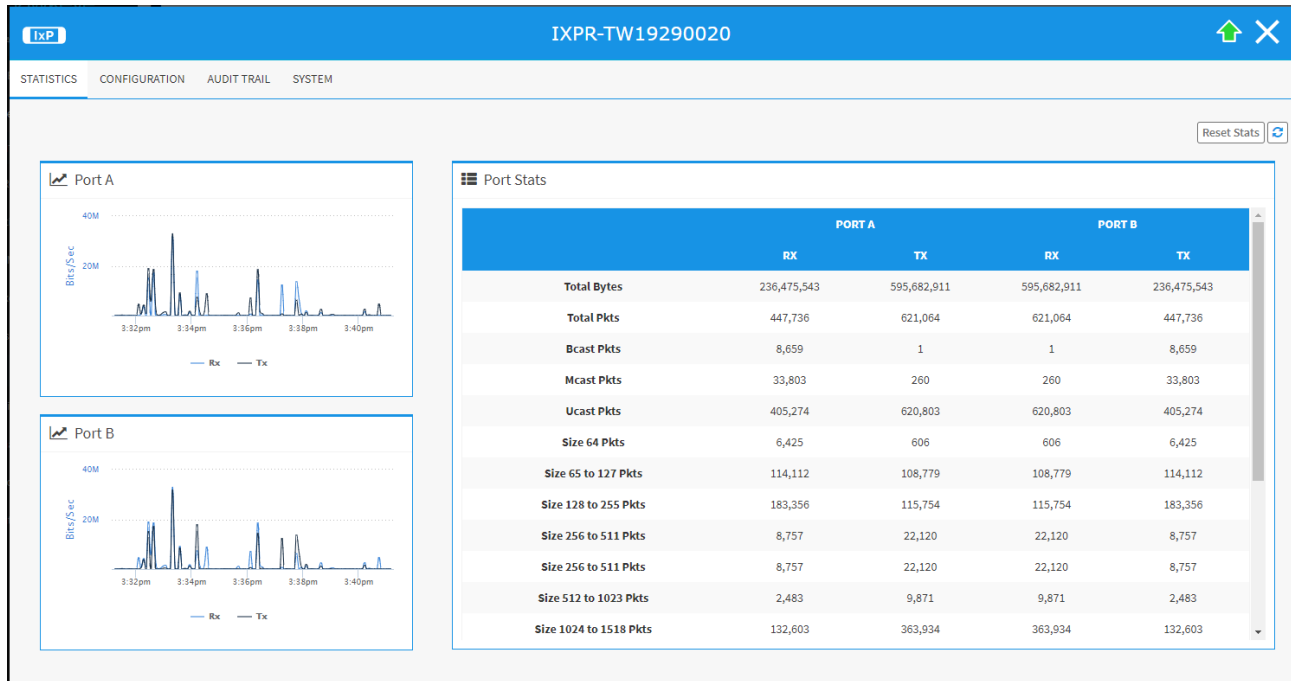
View port statistics

To view port statistics, do the following:

1. On the **Statistics** tab, view the graph for both ports showing the TX and RX rates for each port over the last 10 minutes.
2. View the **Port Stats** table to see the cumulative statistics since the last boot of IxProbe or the last reset.
3. Select **Reset Stats** to clear the statistics on the IxProbe.

NOTE

Reset Stats sets all the statistics to 0 on the IxProbe. Because of the polling interval, all 0s do not appear in the detailed view, but your statistics decrease to what has occurred during the last interval indicating a successful reset of the statistics on the probe.



Configure IxProbe

On the **Configuration** tab, you can see the following configurations of the IxProbes:

Configuration	Definition
Port Stats	Shows the following current port status: <ul style="list-style-type: none"> Up/Down indicated by arrows Speed DUPLEX ALDF Status
Device Information	Shows you the serial number of your IxProbe along with its model and software version.
Rate Stats	Shows the current TX and RX Rates per port for the last polling interval. If your IxProbe is using Inline Management Mode/Inline Adoption Mode (IMM/IAM), your IxProbe will only interact with IP Addresses that are in a Trusted Subnet.
Trusted Subnets	Shows the configured trusted subnets. If your IxProbe is using Inline Management Mode/Inline Adoption Mode (IMM/IAM), your IxProbe will only interact with IP Addresses that are in a Trusted Subnet.
Trap Destination	Lists the IP of configured SNMP Trap receivers.

List	
Network	<p>Shows the current network management mode and its associated mode and IP information. The IxProbe can be in one of three management modes with various network modes for each:</p> <ul style="list-style-type: none"> • IMM (Inline Management Mode) • OOB (Out Of Band management mode) • IMM & OOB <div style="background-color: #cccccc; padding: 5px; display: inline-block;">NOTE</div> When IMM is configured, the Element Manager (Hawkeye IP) must be reachable through the IMM interface.
Hawkeye Server	Shows the currently configured Hawkeye server.
DNS Servers	Configure DNS servers to be used IF probe is configured for Network Static mode.

IXP
IXPR-TW19160023 ↑ ×

STATISTICS CONFIGURATION AUDIT TRAIL SYSTEM

Port Status
Edit

Port A ↑
 1000 Mbps
Speed
full
Duplex

Port B ↓
 NA Mbps
Speed
NA
Duplex

enabled
ALFD ⓘ

Device Information
Edit

Name: IXPR-TW19160023

Contact: James Marshal Hendrix

Location: Redmon Washington

Software Version: 3.0.1576

Device Type: IxProbe

Model: IXPR-CU3 IxProbe Copper

Serial Number: IXPR-TW19160023

Host Name: IXPR-TW19160023

Rate Stats
Sync

Port A
 56 Kbps
Rx
0 bps
Tx

Port B
 0 bps
Rx
0 bps
Tx

Trusted Subnets ⓘ
+ Add

Enabled for IMM

No Trusted Subnets configured.

Trap Destination List ⓘ
+ Add

No SNMP Trap Destinations configured.

Network

IMM ⓘ

Mode: IAM ⓘ

IP: 0.0.0.0

MAC: 00:1b:0e:12:e1:a7

OOB ⓘ

Mode: DHCP

IP: 10.36.42.228

Prefix: 23

MAC: 00:1b:0e:12:e1:a8

GW: 10.36.42.1

Hawkeye Server
Edit

Server IP: 10.36.34.162 ⓘ

Outgoing Interface: System Default ⓘ

DNS Servers ⓘ
Edit

Server 1: 8.8.8.8

Server 2: 0.0.0.0

To configure the IxProbes, do the following:

1. Select **Edit** on the **Port Stats** tile to do the following:
 - Force duplex.
 - Disable Auto negotiation.
 - Disable Asymmetric Link Fault Detect (ALFD) status.
2. Select **Edit** on the **Device Information** tile to do the following:
 - Set **Name**.
 - Set **Contact**.
 - Set **Location**.

NOTE

You can view the information from both the element manager and the IxProbe CLI under device info.

3. Select **Add** on the **Trusted Subnets** tile to add an additional Trusted subnet.
4. Select the trash can next to a subnet to remove that subnet from the list.
5. Select **Add** on the **Trap Destination List** tile to add new IPs to the list.
6. Select the trash can next to an IP to remove that IP from the list.
7. Select **Edit** on the **Hawkeye Server** tile to change the Hawkeye Server IP address. If the IxProbe uses Inline Management Mode/Inline Adoption Mode (IMM/IAM), ensure the IP is part of a trusted subnet.

NOTE

This tab is updated as changes are made through either Bulk Actions or from this page. Changes to the configuration by using the IxProbe CLI or standalone web page are not automatically populated to this tab. To get the latest full running configuration from the IxProbe, select **Sync**.

8. Select **Edit** on the DNS Servers tile to add DNS servers to use if the IxProbe is configured for static mode.

View audit trail

The **Audit Trail** tab shows you a list of actions that have been taken on the IxProbe. The **Status** column indicates if the action has completed successfully. It also provides you with the Element Manager User's login ID, source IP, and the date when the change was attempted.

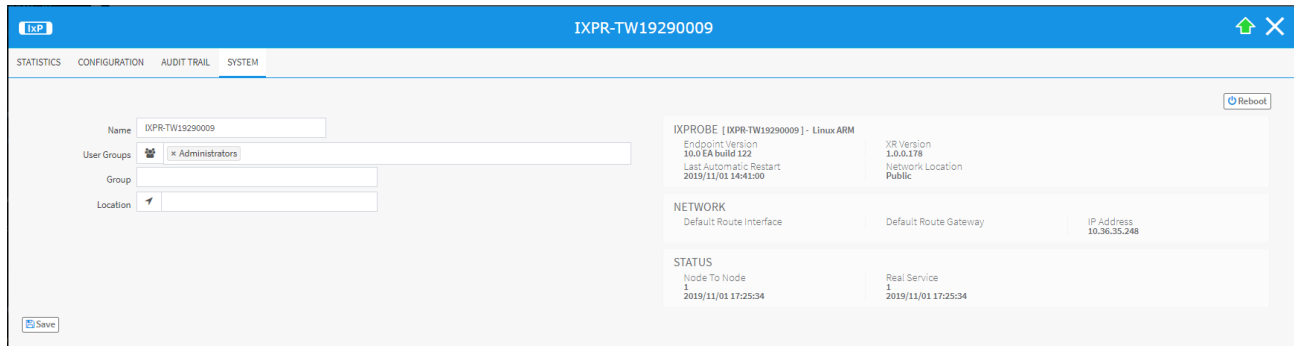
IXPR-TW19290009						
STATISTICS CONFIGURATION AUDIT TRAIL SYSTEM						
Change	Status	Message	Login	Source IP	Date	
Update Stats Reset : stats reset requested	✓		sysadmin	10.64.32.88	2019/11/01 17:30:59	
Add Trap Destination : ip-172.17.150.5	✓		sysadmin	10.64.32.88	2019/11/01 17:30:58	
Add Trap Destination : ip-172.17.192.250	✓		sysadmin	10.64.32.88	2019/11/01 17:30:22	
Add Trusted Subnet : ip-172.17.0.0/prefix-16	✓		sysadmin	10.64.32.88	2019/11/01 17:30:11	
Add Trap Destination : ip-192.168.200.245	✓		sysadmin	10.64.32.88	2019/11/01 17:29:03	
Add Trusted Subnet : ip-192.168.200.0/prefix-24	✓		sysadmin	10.64.32.88	2019/11/01 17:28:53	
Add Trap Destination : ip-192.168.200.85	✓		sysadmin	10.64.32.88	2019/11/01 17:28:53	
Update Device Info : contact=Thomas Eddison,location=Eddison New Jersey,name=Toms LAB	✓		sysadmin	10.64.32.88	2019/11/01 17:28:05	

Showing 1 to 8 of 8 entries

Previous 1 Next

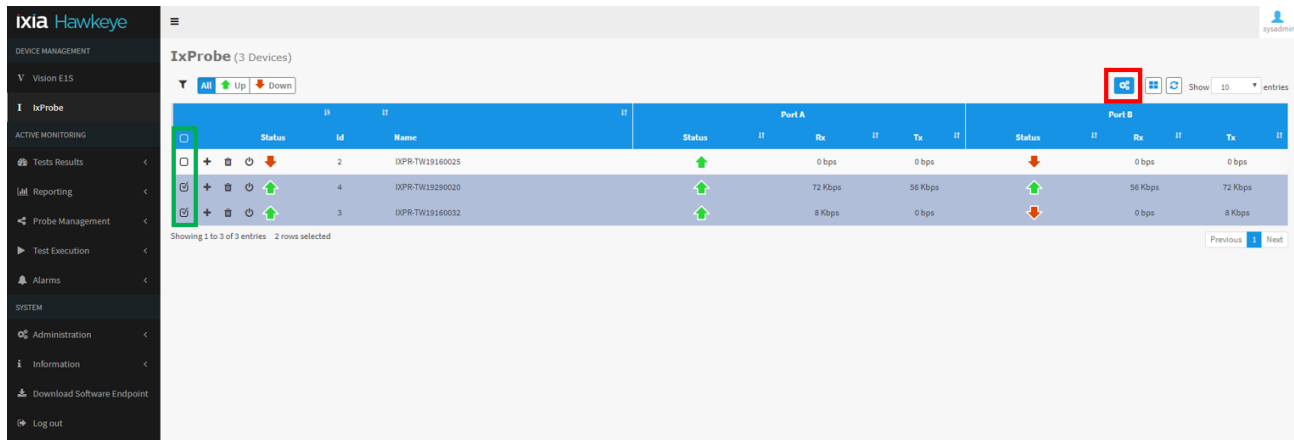
View system information

On the **System** tab, you can find the running versions of the IxProbes core software (XR version) and its Active Monitoring Software (Endpoint Version) along with some network information and status of the Active Monitoring Services. In this tab, you can also change the element managers device name specific its location and add or remove it from a User Group.

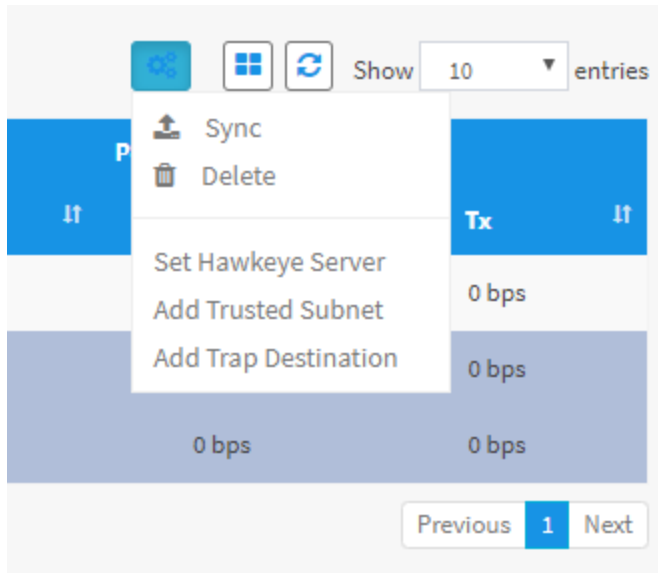


Perform bulk actions on IxProbes

From the IxProbe Element Manager dashboard in list view bulk configuration changes can be made to any or all of the IxProbes that currently appear in the list. To start the bulk configuration process, select individual probes by selecting the check box in the first column. Select all the probes in the current list view if you want to perform bulk actions.



After you have selected the IxProbes on which you want to perform bulk actions, select  to perform one of the available tasks.

**NOTE**

is visible after you select at least one IxProbe for bulk action.

Sync

The **Sync** action retrieves the current running configuration of the selected IxProbe . This is used to get configuration updates that may have been made through the IxProbe CLI or an IxProbe's standalone web UI.

Delete

The **Delete** action removes the selected IxProbes from the Element Manager Database. This is used to remove stored data about IxProbes that are no longer being managed by Hawkeye.

Set Hawkeye server

The set Hawkeye server actions allow you to pass a new Hawkeye server IP down to the selected IxProbes. This is used to migrate IxProbes from one Hawkeye Element Manager Server to another.

Set Hawkeye Server
X

Hawkeye Serveri

Save

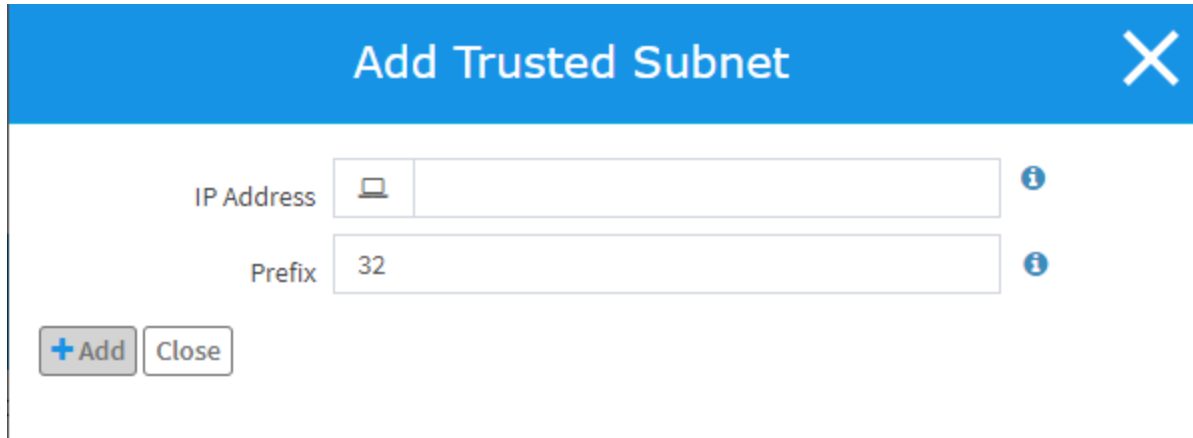
Cancel

NOTE

If any of the selected Probes are in IP Adoption Mode (IMM/IAM), the new Hawkeye server IP must be added to the Trusted Subnet List before performing the **Set Hawkeye Server** bulk action.

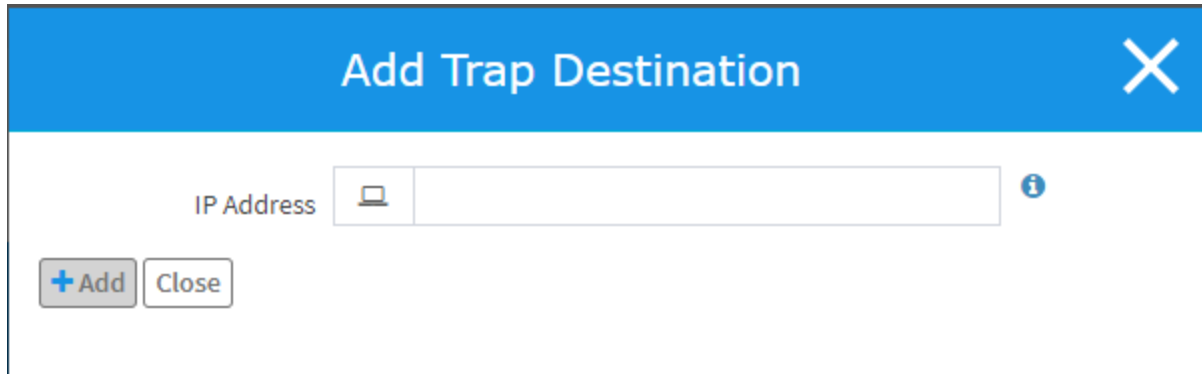
Add Trusted Subnet

Add Trusted Subnet adds the supplied IP address and Subnet Mask (prefix) combination to the selected IxProbes.



Add Trap Destination

Adds the supplied IP address as an SNMP Trap Destination on the selected IxProbes.



Schedule upgrades

Automatic upgrades of IxProbe are turned off by default. If you want to upgrade the IxProbes, you must complete one of the following:

- Turn on automatic upgrade
- Schedule upgrade of a IxProbe

Turn on automatic upgrade

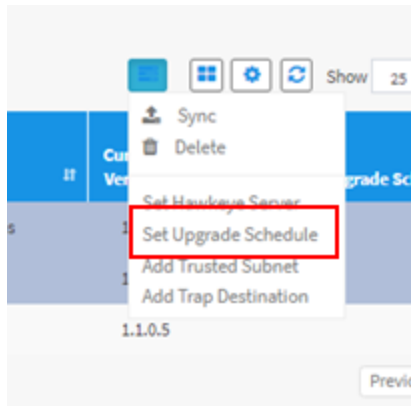
To turn on automatic upgrade of all IxProbes, complete the following steps:

1. From the **IxProbe Element Manager** dashboard in list view select .
2. Select **Settings** to open the **IxProbe Settings** pop up.
3. In the **IxProbe Settings** pop up, from the Auto Upgrade drop-down list, select **Enabled** and select **Save**.

Schedule upgrade of a IxProbe

To schedule upgrade of a IxProbe, complete the following steps:

1. From the **IxProbe Element Manager** dashboard in list view select .
2. Select **Settings** to open the **IxProbe Settings** pop up.
3. In the **IxProbe Settings** pop up, from the Auto Upgrade drop-down list, select **Scheduled** and select **Save**.
4. Go to **IxProbe Element Manager** dashboard and select the IxProbes for which you want to schedule the upgrades.
5. Select  and select **Set Upgrade Schedule** from the drop-down list to open the **Set Upgrade Schedule** pop up.



6. In the **Set Upgrade Schedule** pop up, complete the following step:
 - a. In the **Upgrade Schedule** option, select **On** to turn on the upgrade schedule.
 - b. In the **Scheduled Date** box, set the date and time for the schedule and select **Save**.

NOTE

Date must be in YYYY/MM/DD format.

CHAPTER 4

Hawkeye User Interface Configuration

This section explains the details of the Hawkeye application configuration.

In this chapter:

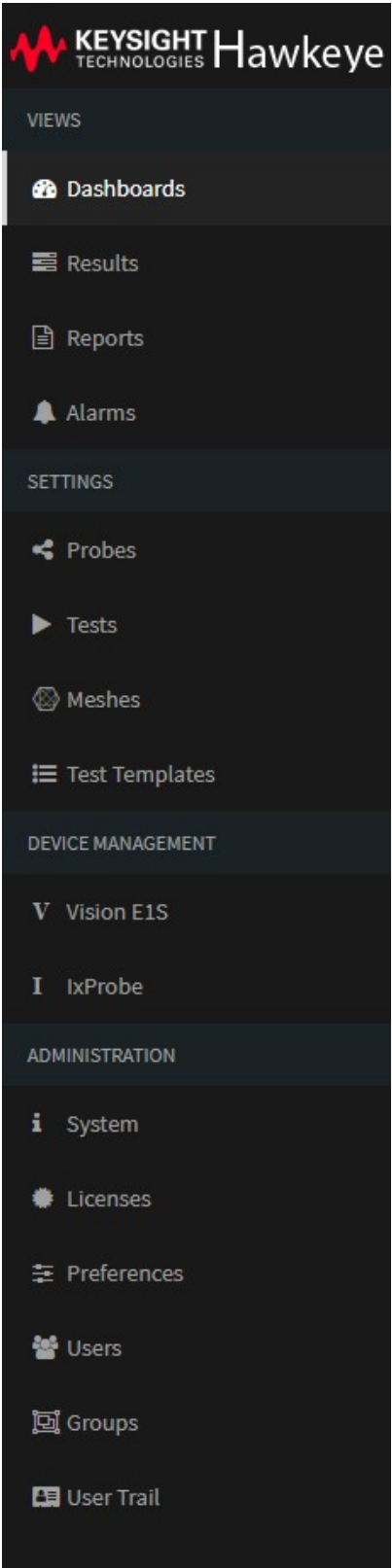
- User Interface Presentation 94**
- Probes Management 96**
- Manage users and groups 97**
 - Users and Groups Definitions in Hawkeye 97
 - Group Management 98
 - Users Management 100
- Test Execution 103**
- Threshold Management 109**
- Alarms Management 111**
- Mesh Management 113**
- MAP Configuration and Probe Location Configuration 115**
- Custom dashboard 120**
 - How do I... 120
- Hawkeye preferences 126**
- Configuring Automatic Email Notifications 143**

User Interface Presentation

The left pane of the window allows you to select the various modules of Hawkeye.

The modules of Hawkeye are restricted by user privileges. You need to have access rights to view the different modules.

This panel is the main menu of the application, which allows you to browse through the different sub menus of the application.



On the same bar, info about the current login account is present: who is logged in and last login info.

The central panel changes the appearance according to the options enabled in the main menu.

The panel located on the bottom of the page shows options typically reserved for user input and actions.

NOTE

It is possible to move the gray bar (vertical only) so that the panels sizes can be expanded or reduced.

Probes Management

This section explains how to add a new probe entry, manage existing probes (aka endpoints), check the probes health, and configure the probes to be displayed on the live map.

Edit a Probe



Select the  icon to edit an existing probe entry.

You need to have access to probe to be able to edit the probe.

The information about the probe will be available in the window below. They can be edited and select **Update probe** to save new information.

NOTE

The probe name can be changed but any existing test results will still be stored into test history with OLD probe name. 2 probes with the same name will be also showed in test history as same "entity" with no way to distinguish them.

View Probe Advanced Information



Select the  icon to edit an existing probe and view the following information: active schedules which the probe is participating to, and meshes for which probe is belonging.

Endpoint in Public or Private mode

Probes that are defined can be public or private depending on the where they are connecting to the network topology in relation to the Hawkeye Server.

The location is automatically determined by Hawkeye server first time the probe is registering.

The determination is based on the ability of the Hawkeye server to open a new connection to the probe.

Typically, if the probe is behind a NAT, the probe will be seen as a private probe.

Private/public mode is very important as it will define Hawkeye endpoints strategies to bypass NAT/FW rules (see Firewall Test_UseCases).

There are cases where forcing a probe detected as private to public will be needed (or the other way around). Understanding where the probe is compared to the location of the other probe and Hawkeye server is important.

Remove an Endpoint

There are many ways to remove an endpoint from Hawkeye.

The endpoint needs to be first removed from any existing mesh and any active test execution schedule before deleting. If you attempt to delete the endpoint by clicking the  icon, without removing the endpoint from all active scheduled tests it will automatically re-register with the Hawkeye server and will appear in the list of probes again.

In probe management, when an endpoint is edited **is Active** check box becomes available. If this box is unselected the probe will no longer be available for running tests and will not count against the active license count for probes. The endpoint connectivity status green or red will remain the same.

For a software endpoint, the install script can be run again and the endpoint software can be uninstalled. Following this, the endpoint in Probe Management will show as red. The endpoint can then be deleted from **Probe Management**.

For an XR endpoint (that is, XRPi/XR2000 VM, XR Cloud, XR Docker) the endpoint is continuously (once every 4 to 5 seconds) sending an "I am here" message to the Hawkeye Server, so just deleting the endpoint from Hawkeye Server will only work for 4 to 5 seconds. You need to first disconnect the endpoint from the Hawkeye Server either by physically disconnecting the endpoint or by connecting a ssh session to the endpoint and running the "probeConfigure" command and entering "0.0.0.0" as the Hawkeye Server IP. This will stop the endpoint from communicating with the Hawkeye Server and the endpoint will turn red shortly afterwards in **Probe Management**. At which point the endpoint can be deleted from **Probe Management**.

Manage users and groups

This section covers users and groups management. The system administrator / administrators group sees all tests, all probes and all system configuration. Other Users can be defined as part of a group hierarchy and only allowed to run certain test types and use certain probes. The users and groups would only be able to see test results for this limited set. This offers a level of security in that a group of users could be limited in their view of the Corporate network. These restrictions can also be extended to maps, test templates, custom dashboards.

Users and Groups Definitions in Hawkeye

Hawkeye application supports different users and groups of users. The user level and group appurtenance will allow to decide which sets or results the user shall be able to see.

Users and Groups Rules

- Each Hawkeye user belongs to a group of users.
- Each Hawkeye user has one user role.
- System Administrators can only be part of the Administrators group.

There are five user roles associated with Hawkeye:

User Role	User/Groups	Test Templates	Probes	Maps	Tests	Results	User Trail
System Administrator	F/C	F/C	F/C	F/C	F/C	F/C	F/C
Group Administrator	L/C	X	L/C	V	X	X	V

User	N/A	X	V	V	X	X	V
System Viewer	N/A	N/A	N/A	V/A	N/A	V/A	N/A
Group Viewer	N/A	N/A	N/A	V	N/A	V	N/A

- F/C = Full Control
- V/A = View Across all Groups
- X= Execute what is Assigned to Group
- L/C = Limited Control of assets assigned to Group
- V= View what is Assigned to Group

Group Management

Hawkeye implements a group hierarchy that includes implied control of the assets of the child group by the parent group. This ensures the parent group maintains the same level of asset control as its children. This should ease configuration by allowing you to assign probes, test templates, maps, test types to the child group that requires the access and the parent group will also get this access without additional steps.

Creating a Group

1. Log into the Hawkeye application as an Admin level user (System or Group Admin).
2. Select **Groups** from the side bar and then select **+Add**.

The screenshot shows the 'Groups' management interface in Hawkeye. A modal window titled 'Group' is open, allowing the creation of a new group. The form includes fields for 'Name', 'Description', and a 'Parent Group' dropdown menu currently set to 'None'. Below these fields are tabs for 'TEST TYPES', 'USERS', and 'PROBES'. The 'TEST TYPES' tab is active, displaying two columns: 'Available:' and 'Selected:'. The 'Available:' column contains a search bar and a list of test types including 'Network KPI bidirectional', 'Network KPI', 'TCP Throughput from->to N streams', 'TCP Throughput from->to 1 stream', 'TCP Throughput to->from 1 stream', 'TCP Throughput to->from N streams', 'TCP Throughput bidirectional', 'UDP Throughput from->to', 'UDP Throughput to->from', 'UDP Throughput bidirectional', and 'HTTP Server Test'. The 'Selected:' column is currently empty. A 'Save' button is located at the bottom left of the modal.

3. Enter the **Group Name**. Enter a description if any. If this is going to be a child group select the parent group.

NOTE

User with the role, Group Administrator, can only create child groups with the group they are an administrator of as the parent.

4. Assign the test types intended to be used by the group created. On the left side panel, all test types are available. The test types added to right side panel, makes those tests available for the newly created group. For example, Voice test types were added to the Voice group.

5. Select Users Tab and add the required users to the group. On the left side panel, all users are available. The users added to right side panel, makes those Users available for the newly created group.
6. Select Probes Tab and add the required probes to the group. On the left side panel, all probes are available. The probes added to right side panel, makes those probes available for the newly created group.
7. Select **Save** button to save the group created into the database. If everything is OK, the group should be present in the Group table.

	Id	Name	Description	Probe Count
☐	1	Administrators	Hawkeye Administrators	13
☐	3	DelayGroup_new	This group is for users testing high delay network	3
☐	5	PublicSpaceTesting		3
☐	6	Automation_Testing	A group for automation	0
☐	9	US IT	ITI group of the Us	2

	Id	Name	Description	Probe Count
☐	10	Voice	IP Telephony Group	2

Showing 1 to 1 of 1 entries

Showing 1 to 5 of 5 entries (filtered from 8 total entries)

Hawkeye application allows the user to edit the description, available test types, users and probes. To edit select the **Edit** icon next to the group ID or group name, of the group that you want to edit. All information about the group will be displayed and can be edited in the same manor it was created.

Hawkeye also allows the user to delete an existing group. Prior to deleting a group all its users need to be deleted from the User page or move to other groups. Then, select the delete icon of the group that you want to delete. A new pop up window will appear asking for confirmation. Select **OK** to delete the group.

Users Management

Creating a User

1. Log into the Hawkeye application. A new user can be created only by a member of **System Administrator** or **Group Administrator** groups.
2. Select the **Users** on the side bar and then select **+Add** button.
3. To add a new user, enter the details of the user in the text boxes as shown below:

User
✕

Authentication Mode

Local
▼

Login

✕

Force Change Password

☐ Off

Password

✕

Confirm Password

✕

First Name

✕

Last Name

✕

Email

✕

Groups

✕ Administrators

Level

User
▼

☒ Active

💾 Save

NOTE

User with System Administrator role can add new users to any of the existing groups. User with Group Administrator role can add new users only in the group or one of its child groups to which the user belongs.

There are five different user levels:

- **System Administrator** is the super user. This level has complete access to the Hawkeye application. The user with this privilege level can add and delete users and groups, enable and disable users and groups, view probes of each user, view scheduled tests by each user, and extract results.
- **Group Administrator** user role can perform the same actions as the system administrator, but the actions are limited only to the group that the user belongs to. A group administrator is not entitled to add and delete groups.
- **Group Viewer** user role can only view and extract the test results of the tests run by the users in that group.

- **Full System Viewer** user role can only view and extract the test results of the tests run by all the users belonging to various groups.
- User role can create own probes and schedule a test or run a test. The user can view, extract and delete the results of the tests being run.

NOTE

A user with System Administrator Role can assign any of the above five user levels to the new added user.

A user with Group Administrator role can assign only the following three user levels to the new added user: group administrator, group viewer, or user.

Edit a user

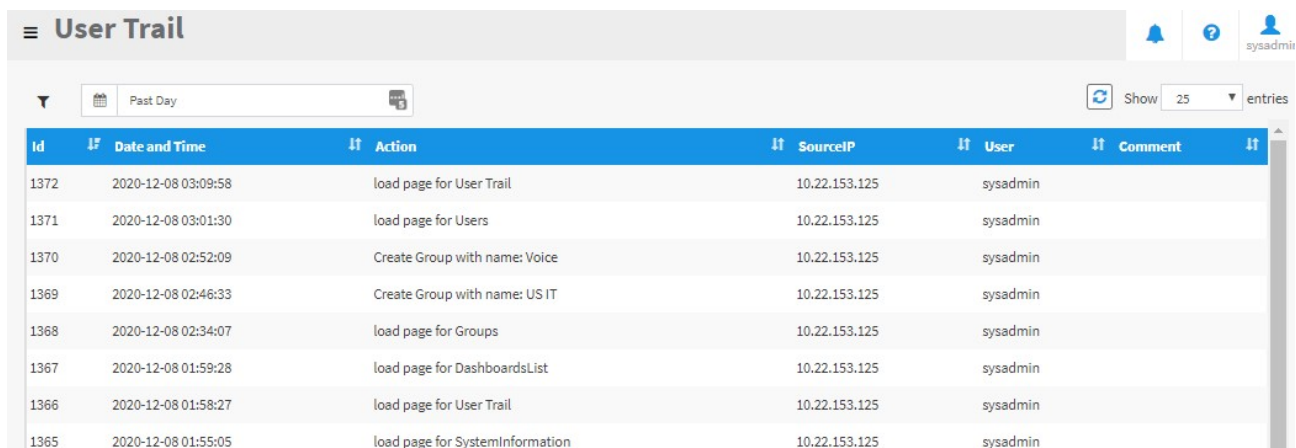
To edit a user, select . The same pop up box as create will be displayed with the current information about the user. You can modify any of the fields except the Login field, and select the Save button. This will update the user details in the database and the same will be displayed in the users table.

Delete a user

Select  next to the user you want to delete. A new pop up window will appear, asking for confirmation. Select **OK** to delete the user.

Track actions of a user

Hawkeye offers the possibility to track the actions that a user did in the system. To access this feature, select **User Trail** on the side bar. The following page will be displayed:



Id	Date and Time	Action	SourceIP	User	Comment
1372	2020-12-08 03:09:58	load page for User Trail	10.22.153.125	sysadmin	
1371	2020-12-08 03:01:30	load page for Users	10.22.153.125	sysadmin	
1370	2020-12-08 02:52:09	Create Group with name: Voice	10.22.153.125	sysadmin	
1369	2020-12-08 02:46:33	Create Group with name: US IT	10.22.153.125	sysadmin	
1368	2020-12-08 02:34:07	load page for Groups	10.22.153.125	sysadmin	
1367	2020-12-08 01:59:28	load page for DashboardsList	10.22.153.125	sysadmin	
1366	2020-12-08 01:58:27	load page for User Trail	10.22.153.125	sysadmin	
1365	2020-12-08 01:55:05	load page for SystemInformation	10.22.153.125	sysadmin	

This page can be filtered with the following filters:

- ID
- Date
- Action
- Source IP

- User
- Comment

The information provided is:

- ID of the action
- Date and time when action was taken
- Type of action taken
- Source IP from where the action was taken
- User name
- Comment

Test Execution

The following test topologies are available in Hawkeye:

1. Node to Node testing - allows execution of tests between one node (probe) and another node (probe);
2. Mesh - will allow execution of tests on a full mesh of probes;
3. Real Services – will allow real tests (HTTP,FTP,ICMP,etc) test from probes to servers located in internet.

Node to Node Test Configuration

The node to node test execution will allow the following selections:

- Probe from: probe where the test is executed FROM (can be network side);
- Probe to: probe where the test is executed TO (can be access side);
- Test type: the type of test that will be executed;
- Test duration: the duration of the test time while the active traffic will be generated;
- Test options: depending on the test types, some options would be available to select from (e.g. bit rate, packet size, number of concurrent pairs, etc...).

Add test
← Back ✕

Normal
Test Template

Configuration
Advanced
Thresholds
Alarms

Tag

Type

Network KPI
▼

Unidirectional Network Flow measuring Loss, Jitter, Delay

From

IXPR-TW19160025
▼

🖥

Default ▼

To

xr-vm-tt2
▼

🖥

Default ▼

Traffic Duration

30 sec
▼

Frequency

🕒

0

☐ Add another

▶ Start
Cancel

NOTE

The direction of the test will be from Node 1 to Node 2. When test names include downstream, the traffic will be generated from Node 1 to Node 2. When the name includes upstream the traffic will be generated from Node 2 to Node 1.

NOTE

Tests can only be executed between 2 manual probes or 2 automatic probes, you can not have 1 automatic and 1 manual probe into the same test schedule.

Mesh Test Configuration

By selecting **Test Execution Mesh** option from the Test Execution main menu, the user will have the option to configure tests for mesh topologies available. To see how to create a mesh, check Probe Management section.

Add test

← Back

✕

Configuration

Advanced

Thresholds

Alarms

Tag

Type

Skype4B Traffic from->to

Skype4B Voice and Video Traffic Mix in single direction. Set 0 throughput for disabling streams.

Mesh

minimesh

Traffic Duration

30 sec

Number Of Pairs

1

Total bitrate (kbps)

100

Audio RTP from->to

Total bitrate (kbps)

500

Video RTP from->to

Frequency

🔊

0

☐ Add another

▶ Start

Cancel

The mesh test execution will allow the following selections:

- Mesh Name: select the mesh under test previously configured;
- Test type: the type of test that will be executed;
- Test duration: the duration of the test time while the active traffic will be generated.

NOTE

Not all test types available for Node to Node topologies are available for Mesh topologies.

Starting a test on a mesh will add all available paths in the mesh (see mesh creation and configuration section).

Real Services Test Configuration

To configure a real service test scenario, select the **Test Execution Real Service** option located under the Test execution menu.

The real services test execution will allow the following selections:

- Probe from: probe where the test is executed FROM
- Test type: the type of test that will be executed
- Destination Server: the real server where the test is executed TO

- Test options: depending on the test types, some options are available to select from or configure to (for example, DNS server, packet size, and ping interval).

Add test
← Back ✕

Normal
Test Template

Configuration
Advanced
Thresholds
Alarms

Tag

Type

DropBox Download
▼

Dropbox Server Test download file

From

xr-vm-tt2
▼

DropBox File

File_100k
▼

Frequency

⌚

☐ Add another

▶ Start
Cancel

NOTE

Real Services test are available only for hardware probes type.

Test Queue Management

The status of a test schedule can be one of the following values:

- Running: the tests are under execution. This will be displayed into black color.
- Queued: waiting for execution – the test resources aren't available (busy), so the test is waiting in queue.
- Waiting next execution: the test is scheduled and the schedule is active, but the next execution time is not available yet.
- Schedule on hold: the test is scheduled but the schedule has been placed on hold (see putting a schedule on hold section).
- For mesh tests: queuing for completion. This status is displayed for a mesh test when the mesh is partially completed and the test is split into different test runs.

The following priority in the queue applies:

- The later next test execution takes priority;
- One shot tests are executed in priority to scheduled tests;
- The mesh schedules that need to be completed are executed in priority. The next execution time for a mesh is not changed until last run completion;

Node to Node tests are executed in priority to Mesh tests.

Test Scheduling Configuration

The test scheduling options are available for all types of test configurations. The functionality is the same all configurations.

Test interval - Minutes : Start schedule End Schedule

Test interval [minutes]: defines the time interval between tests. This interval is calculated on best effort basis, as the tests in the queue might be too numerous to allow all intervals to be respected. In case the interval is too small for tests to be executed, the queue will automatically adjust to best possible interval to execute the test.

If the test Interval is set to 0, then the test will be executed only one time. This will be displayed as one shot test. In this case, the test will be displayed into test execution table while waiting for execution (Queuing) or running. Once the test is completed, it will be removed from the test execution table and the results will be available into the test results lists.

Start schedule : defines the date when the schedule shall start.

- If left blank, the current date will be applied;
- If Interval is set to 0 (one shot test), then this will define when to start the test (in batch mode);
- To select the day and time, change time (24 hours selection), and then select it.

End schedule : defines the date when schedule must end.

- If left blank, the schedule will last forever;
- If Interval is set to 0 (one shot test), then this end schedule will not be considered;

To select the day and time, change time (24 hours selection), and then select it.

NOTE

The test execution list will display only the schedule currently active or active in the future. All schedules not active any more will not be displayed in the list.

NOTE

Test execution frequency of less than a minute is supported and needs to be enabled in preferences /main section by administrator.

Cancel a Schedule Test

Tests can be canceled by selecting the delete  button. This will cancel the test or schedule.

If the test is waiting for execution, in the queue or on hold, the test will be canceled directly.

If the test is canceled while running, first it will finish the current run and then will be canceled.

The scheduled test list is refreshed every minute by default. It might be the case that canceling a test or a schedule that appears queuing of waiting next execution gets the test canceled into a running mode instead. In that case the test execution will refresh and the new status of the test be displayed.

Set a Schedule on Hold

Tests can be put on hold by selecting the pause  button. This will put the schedule on hold so wait for next execution. The button will transform in play  button, and by selecting this button

the test schedule will resume.

	178	Node to Node	Austin	Calabasas	DNS Response Time	bitrate=2000 kbps latency=10ms	80	One shot	Running	2023/07/03 12:44:30	2023/07/03 12:44:28	NEVER	sysadmin
	133	Node to Node	Paris	Chicago	Voice bidirectional	voice=1000 kbps	30	10 min	Waiting next execution	2013/07/03 12:49:38	2013/05/22 00:10:58	NEVER	sysadmin
	175	Mesh	US_mesh	US_mesh	Traffic Mix - HTTP - Video - Voice	bitrate=Video Downstream=1000 kbps bitrate HTTP Downstream=1000 kbps	30	60 min	Waiting next execution	2013/07/03 12:55:08	2013/05/24 19:20:24	NEVER	sysadmin
	147	Mesh	US_mesh	US_mesh	Network KPI downstream	Network KPI downstream	15	15 min	Waiting next execution	2013/07/03 12:57:45	2013/05/03 13:18:48	NEVER	sysadmin
	174	Mesh	US_mesh	US_mesh	Traffic Mix - HTTP - Video - Voice	bitrate=Video Downstream=1000 kbps bitrate HTTP Downstream=1000 kbps	30	One shot	Waiting next execution	2023/05/24 19:20:55	2013/05/24 19:20:55	NEVER	sysadmin

If the test is waiting for execution, in the queue or on hold, the test will directly change status.

If the test is running, after the current run ends, the test will be put on hold. A specific status (running then hold) will be displayed.

Interval Optimizer and Enforce Schedule

Interval optimizer takes the start time of a test run and adds the interval for the next run. If the queue delays the start time for the first test or if there are some test run interruptions, the interval optimizer considers them and optimizes the queue for being as close as possible for the run interval. A downturn of this behavior is that the exact run test times are not guaranteed.

Turning on **Enforce Schedule** forces the test to run at the first run time + test interval. It means that when you run the test, the next test run time is set to first time + $n \times$ interval time, where n is set to be the next instance for the schedule.

Example: First time is 12:00 and the interval is 1 hour. If you run the test at 16:12, the next time is set to 12:00 + $5 \times$ (1 hour). Here $n=5$, that is, the fifth instance of the schedule, starting with 12:00. Therefore, the test is enforced to run at 17:00. This setting allows enforcing the test run schedule at exact times. But if the queue is full, the system delays the test run and does not optimize the queue for best use.

Add test
Back

Configuration
Advanced
Thresholds
Alarms

Tag

Type Network KPI

Unidirectional Network Flow measuring Loss, Jitter, Delay

From he-qa-sep1.xzm.is.keysight.com Default

To he-qa-sep1.xzm.is.keysight.com Default

Traffic Duration 30 sec

Frequency 0 min

Enforce Schedule Off

☐ Add another Start Cancel

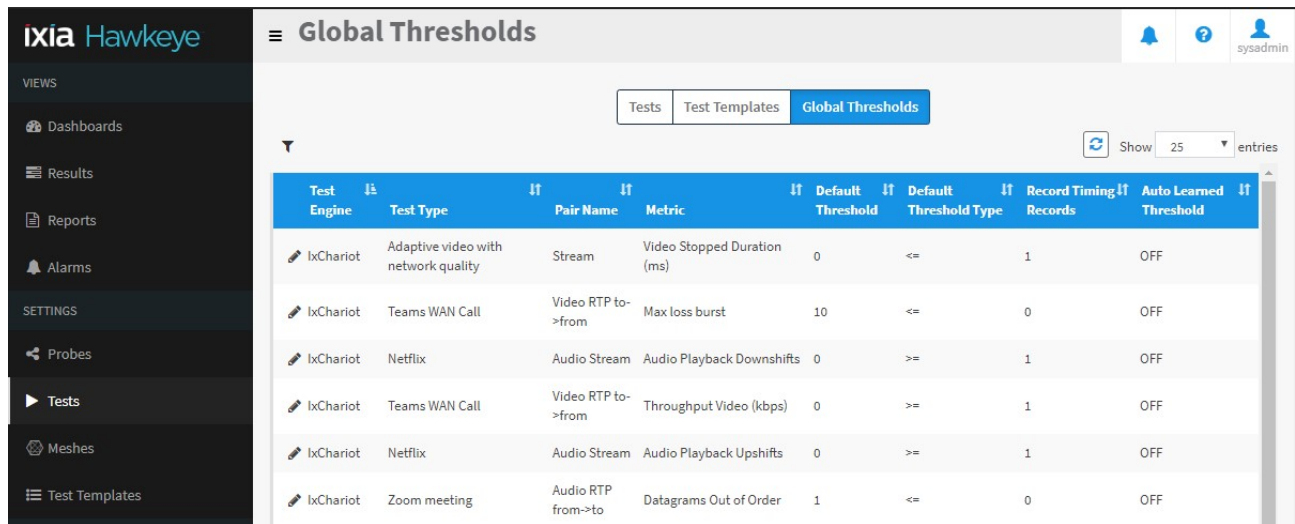
Threshold Management

Thresholds are the baseline to decide if tests are passing or failing. Setting up correct thresholds is essential for understanding the test results and making sure that the right level of information is in the database. Auto-learning of key thresholds can also be enabled to ensure they are adjusted to your specific network conditions.

View the Default Thresholds

To check the thresholds configured by default in the application, select the **Global Threshold** located at the top of the **Tests** page.

The list of available test types, corresponding pairs and metrics will be displayed:



Test Engine	Test Type	Pair Name	Metric	Default Threshold	Default Threshold Type	Record Timing Records	Auto Learned Threshold
IxChariot	Adaptive video with network quality	Stream	Video Stopped Duration (ms)	0	<=	1	OFF
IxChariot	Teams WAN Call	Video RTP to->from	Max loss burst	10	<=	0	OFF
IxChariot	Netflix	Audio Stream	Audio Playback Downshifts	0	>=	1	OFF
IxChariot	Teams WAN Call	Video RTP to->from	Throughput Video (kbps)	0	>=	1	OFF
IxChariot	Netflix	Audio Stream	Audio Playback Upshifts	0	>=	1	OFF
IxChariot	Zoom meeting	Audio RTP from->to	Datagrams Out of Order	1	<=	0	OFF

Different thresholds can be filtered based on test types, pair names, and metrics.

The following information per test type, pair name and metric is displayed:

- **Default threshold:** this is a system wide default threshold for the metric. The value is a float.
- **Threshold type:** currently three types of thresholds are supported:
 - **<=:** the test result value will PASS if the result is less or equal to threshold. Any result value above threshold will FAIL. Example: delay or jitter measurements.
 - **=>:** the test result value will PASS if the result is greater or equal to threshold. Any result value below threshold will FAIL. Example: throughput.
 - **%:** this defines a percentage of expected throughputs. This threshold is uniquely supported for throughput and test types where user can define throughput (bit rate) value. The test will PASS if the expected % of generated throughput is reached, it will fail otherwise.
- **Record timing records:** during some tests supported by Hawkeye, some timing records will be recorded during the test allowing Hawkeye to store information of behavior of test. This will depend on the test type and will be available when selecting individual test report (see browsing test results section).

- Auto Learned Threshold: When “ON” the thresholds value will be determined utilizing the results of the previous tests runs. See [Configure Auto Learn Threshold](#).

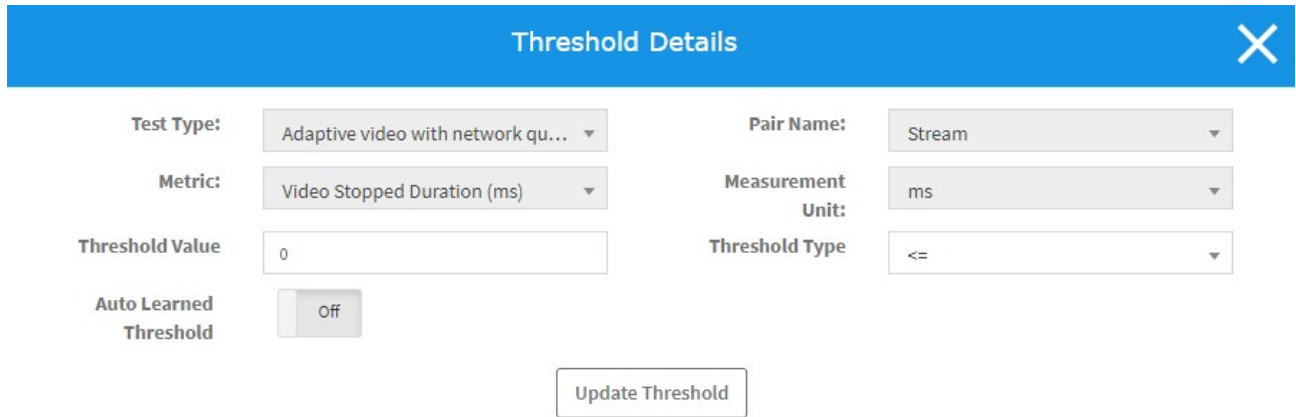
Change the Default Thresholds

Only users with administrator privileges can change default thresholds.

The default thresholds can be changed from the default threshold page.

By selecting the pencil  button, the threshold will be automatically selected.

The Threshold Details screen allows to change the value of the threshold, threshold type, and enable Autolearning.



The image shows a 'Threshold Details' dialog box with a blue header and a close button (X) in the top right corner. The dialog contains several configuration fields:

- Test Type:** A dropdown menu showing 'Adaptive video with network qu...'.
- Metric:** A dropdown menu showing 'Video Stopped Duration (ms)'.
- Threshold Value:** A text input field containing the number '0'.
- Auto Learned Threshold:** A toggle switch currently set to 'Off'.
- Pair Name:** A dropdown menu showing 'Stream'.
- Measurement Unit:** A dropdown menu showing 'ms'.
- Threshold Type:** A dropdown menu showing '<='.

At the bottom center of the dialog is a button labeled 'Update Threshold'.

To change the default threshold, edit the Threshold value field, configure the new value and select Update Threshold.

Configure Threshold per Test

Hawkeye application offers the possibility to change a specific threshold per test that will be configured to run either in a node to node topology, mesh or real service scenario.

To configure the threshold per test, select any test execution module. On the panel, where the test parameters are configured, select **Show threshold option** button. The available thresholds for the selected test type will be available. In the example below, the available thresholds for node to node, DNS response time are shown:

Add test

BackX

NormalTest Template

ConfigurationAdvancedThresholdsAlarms

Auto Learn Threshold

Auto Learn Tolerance

Enable Outlier

DNS Test

DNS Availability

1

>=

Off

Medium sensitivity- Percentile

Off

Params

DNS Test

DNS Response Time (Ms)

1000

<=

Off

Medium sensitivity- Percentile

Off

Params

Add another

Start

Cancel

The parameters that you can be change are:

- Threshold value
- Threshold type
- Enable Auto Learn
- Auto Learn Tolerance
- Enable Outlier Detection
- Outlier Parameters. See [Configure outlier](#)

NOTE

The threshold is changed only for the current test configuration. If a new test of the same type is configured, for which the same thresholds must be configured, the thresholds must be configured again in test configuration process. If the thresholds must be changed globally, follow the steps mentioned in the Change the default thresholds section.

Alarms Management

Alarms Configuration

When configuring a test, the users have the possibility to set up alarms to be sent in case of failure or error in the test.

To enable the alarm configuration, select the **Alarm** tab located on the **Add / Edit Test** screen.

Raise On defines the trigger for test status on Alarms:

- Status change: An alarm will be triggered when test result status will change. This will only be triggered on scheduled tests and allow notification of a test result status changing.

- **Failed:** An alarm will be triggered every time a test result is failed (test was completed but the threshold was not met).
- **Error:** An alarm will be triggered every time a test is reporting error (the test could not start or be completed).
- **Outlier:** An alarm will be triggered every time an Outlier is detected for metrics in this test that have Outlier Detection enabled. See [Configure Outlier](#)

The screenshot shows the 'Add test' configuration interface. At the top is a blue bar with the text 'Add test' and a 'Back' button. Below this are two tabs: 'Normal' and 'Test Template'. The 'Alarms' tab is selected, showing a configuration panel. The panel has two main sections: 'Configuration' and 'Notifications'. Under 'Configuration', there is a 'Raise on' section with four checkboxes: 'Status change', 'Failure', 'Error', and 'Outlier'. Under 'Notifications', there are two checkboxes: 'Email' and 'SNMP Trap'. At the bottom of the panel are three buttons: 'Add another', 'Start', and 'Cancel'.

The alarms can be sent either by e-mail or SNMP.

Both alarms types need to be setup at installation with third party Email (SMTP server) and/or SNMP alarm management system so that traps are generated to it. The administrator can configure only one or the other alarm or none depending on the Hawkeye integration.

You must select at least one **Raise on** for setting up the alarm. No alarm will be created if no option is selected in the **Raise on** section.

The user can choose between the different alarm types. The alarm will be on for the duration of the test schedule. Alarm configuration can be seen in the alarm section.

View Alarms Current Settings

The alarms are set based on tests schedules and when these are defined. The alarms will run while the test schedule is active. The Alarms screen displays the currently running tests with alarms setup and their statuses

The alarm information contains: from probe name, to probe name, alarm type and different alarm settings.

To change or remove an alarm, the related test execution needs to be cancelled and re-executed with new alarm settings, if required.

View Alarms List

Selecting the Alarms page on the side bar and clicking the Generated Button will display the alarm list in reversed chronological order.

The alarm list shows the current status of alarms, and the related test data record ID and schedule execution ID.

Mesh Management

This section describes the process of creating a mesh test using a group of probes. A key concept of Mesh tests is the IP used for each probe for test traffic is the default IP. You can change this for all probes so that the IP used for traffic in a mesh test is the IP associated with the interface that defines the default gateway. To set the IP, go to **Preference > Set Test IP that matches Default Gateway (Mesh tests only)**.

Select **Meshes** on the side bar to create and manage meshes.

Add a Mesh

- 1. Select **+ Add** button.

Add New Mesh

Number of Mesh Paths Selected is 6

Unselect All

Select All

IXPR-TW19160025

Configure Hub And Spokes

Probe From	Probe To	Selected
xr2000vm-323	IXPR-TW19160025	☒
xr2000vm-323	xr-vm-tt2	☒
IXPR-TW19160025	xr2000vm-323	☒
IXPR-TW19160025	xr-vm-tt2	☒
xr-vm-tt2	xr2000vm-323	☒
xr-vm-tt2	IXPR-TW19160025	☒

Mesh Name

Mesh Description

Is active

Probes For Mesh:

Available:

Filter

>

xr2000vm-qa-exp1 - xr2000vm-QA-exp1

xr2000-tt - xr2000-tt

he-qa-sep1.xzm.is.keysight.com - he-qa-sep1.xzm.is.keysight.com

IXPR-TW19290009 - IXPR-TW19290009

...

Selected:

Filter

<

xr2000vm-323 - xr2000vm-323

IXPR-TW19160025 - IXPR-TW19160025

xr-vm-tt2 - xr-vm-tt2

Save

- 113 - 913-2383-01 Rev A

2. Specify the name of the mesh in **Mesh name**.
3. Specify the description of mesh in **Mesh Description**.
4. Select **Is Active** to make the mesh test available in the test execution mesh. Default is selected. See mesh test execution selection for more details.
5. Select the probes from the **Available Probes for Mesh** list in the left column and select **add>>** to add the probes to the **Selected Probes for Mesh** column. By default no mesh paths are selected. To customize the mesh, select paths from the **Selected Probes for Mesh** column.
6. Select **select all** or **unselect all** to select or clear selection of all mesh paths.

NOTE

- For a full mesh created using the selected paths, if you add more probes to it, neither the mesh nor the hub and spoke is complete. You must manually update the mesh to be full mesh or hub and spoke. Appropriate messages are displayed in the top panel describing the type of mesh configured (Full mesh or Hub and spokes).
 - Meshes containing more than 200 selected paths can have performance impact on server when using default MariaDB configuration. It is essential to optimize MariaDB configuration as per instructions mentioned in [Manage Configuration Database](#).
 - The manual path selection table is only supported for meshes that have less than 50 selected probes. More than 50 selected probes will result in no full mesh option and only the buttons at the top can be used to configure hub and spoke mesh.
 - The maximum number of mesh paths supported is 2450.
7. Select **Save Mesh** to save the mesh.
 8. Select **Meshes** on the side bar to see all meshes that have been created.
 9. To edit a mesh, select a mesh from the **Mesh List** menu and select the edit  icon. The following options will be available for editing:
 - **Add probes to mesh**
 - **Remove probes from mesh**
 - **Change mesh name**

Configure a Mesh: Hub and Spokes

To configure a hub and spoke topology with a mesh, complete the following steps:

1. After you select a mesh from the **Mesh List**, select  to edit it. The following screen will be available.
2. Select the probe from the drop-down list, which you want to configure as hub.
3. Select **Configure hub and spokes** button. Automatically all paths between the hub and the spoke will be created.

In the example below, Austin probe was selected as hub. Automatically all paths were created when the Configure hub and spokes option was selected.

Remove a Mesh

- Select  to remove a mesh test.

MAP Configuration and Probe Location Configuration

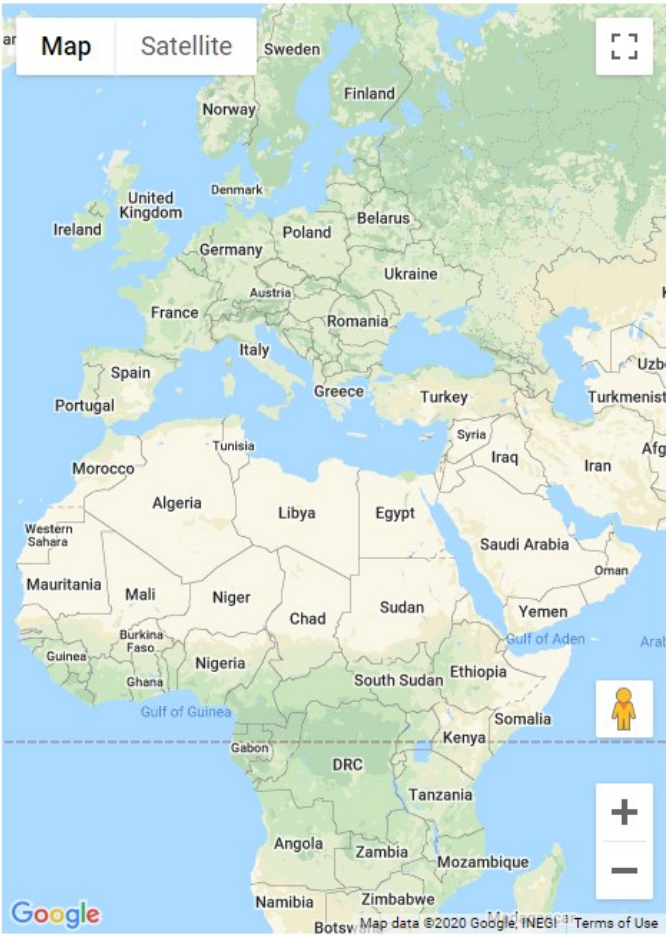
Hawkeye has a built in feature to configure geographical maps for displaying the probes physical location.

The feature is built on top of Google Maps application.

- The probe coordinates must be available to display the probe on the map. There is no GPS device installed on the probes.
- The Hawkeye Server must have internet access in order to able to access Google Maps.

To start the map configuration process, select Dashboards then select **Maps** button and select **Edit Maps** at the top right of the screen. From the Map Configuration screen select the **+ Create** button. The following window will be available:

Map Details
✕



Map Satellite

Google

Map data ©2020 Google, INEGI Terms of Use

Map Name:

Get Coordinates From Map:

Get Coordinates

Center Latitude:

Center Longitude:

Map Zoom:

Display Without Authentication:

No

Associated Mesh:

All

Associated Test Type:

Network KPI

Associated Group:

All

Probes:

Available:	Selected:
Filter	Filter
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">he-qa-sep1.xzm.is</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">IXPR-TW19160025</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">IXPR-TW19160031</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">IXPR-TW19290009</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">kes-qa-ec3 - kes-q</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">thothorn-rh7.xzm</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">xr-vm-tt1 - xr-vm-t</div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;">xr-vm-tt2 - xr-vm-t</div> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 2px;"></div> </div>

Create Map

On the left side, the Google map is displayed, on the right side the configuration area.

Complete the following steps to configure map.

1. Browse to the desired area and zoom at the desired level.
2. When the position is set, define the map name.
3. Select the Get Coordinates button.
4. Select the Update Map button to save the new center of the map.

In the example below, the desired map is the map of the United States, at a zoom level of 4.

Once the position is set and the **Get Coordinates** button is pressed, the coordinates and zoom level will be automatically filled in the specific fields.

Map Details
✕



Map Name:
Auto Mesh

Get Coordinates From Map:

Center Latitude:
40.8776

Center Longitude:
-99.1264

Map Zoom:
4

Display Without Authentication:
Yes

Associated Mesh:
auto

Associated Test Type:
All

Associated Group:
All

Probes:

Available:	Selected:
<input type="text" value="Filter"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> > </div> <div style="font-family: monospace; font-size: 0.8em;"> kes-qa-ec3 - kes-qa-e thothorn-rh7.xzm.js.k xr2000vm-322 - xr200 xr2000vm-323 - xr200 </div> </div>	<input type="text" value="Filter"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> < </div> <div style="font-family: monospace; font-size: 0.8em;"> he-qa-sep1.xzm.js IXPR-TW19160025 IXPR-TW19160031 IXPR-TW19290009 xr-vm-tt1 - xr-vm-t xr-vm-tt2 - xr-vm-t xr2000-26 - xr2000 xr2000-tt - xr2000- </div> </div>

After the position is set, the next step is to assign probes on it.

1. When creating/editing a map, the left column (available for map) of probes lists the available probes. When you move the probe to the right column (selected for map), the probe is placed on the map. The system uses the google latitude/longitude co-ordinates that were previously defined for the map creation. The probe is automatically placed at the configured position.
2. If no coordinates are configured for the probe, it appears in the center of the map and you can manually place the probe at the desired location.

To do this, complete the following steps:

- a. Select the probe from the **Available for map** group and add it to **Selected for map** group.
- b. After the probe is in the **Selected for map** group, select it. A marker automatically drops on the map.

NOTE

The marker always drops in the same position for all probes that are configured to be displayed on the map.

- c. Drag the probe to the required position on the map.
- d. After the marker is on the position, the coordinates of the probe are stored for that map.
- e. To configure the next probe, repeat these steps.

After all the probes are placed in the required locations on the map, to save it, select **Create Map** or **Update Map**.

By default the map is available for all groups of users and it is assigned to all meshes.

If a map is configured for a particular group of users, the administrator has the option to assign it only to that particular group. To do this, while configuring the map, select the group to which the map will be assigned from the “Associated group” and save the map.

NOTE

If the Associated group is particular, the map will be available only for that particular group and for the system administrator.

Maps can be defined to track the status of probes for only certain tests. By default, if a probe is on a map, any test type or mesh test will be reflected. The map can be configured to only reflect the status of a certain Mesh or test type. Refer to the **Associated Mesh** or **Associated Test Type** to achieve this.

You can build multiple maps and all are listed in Maps Management.

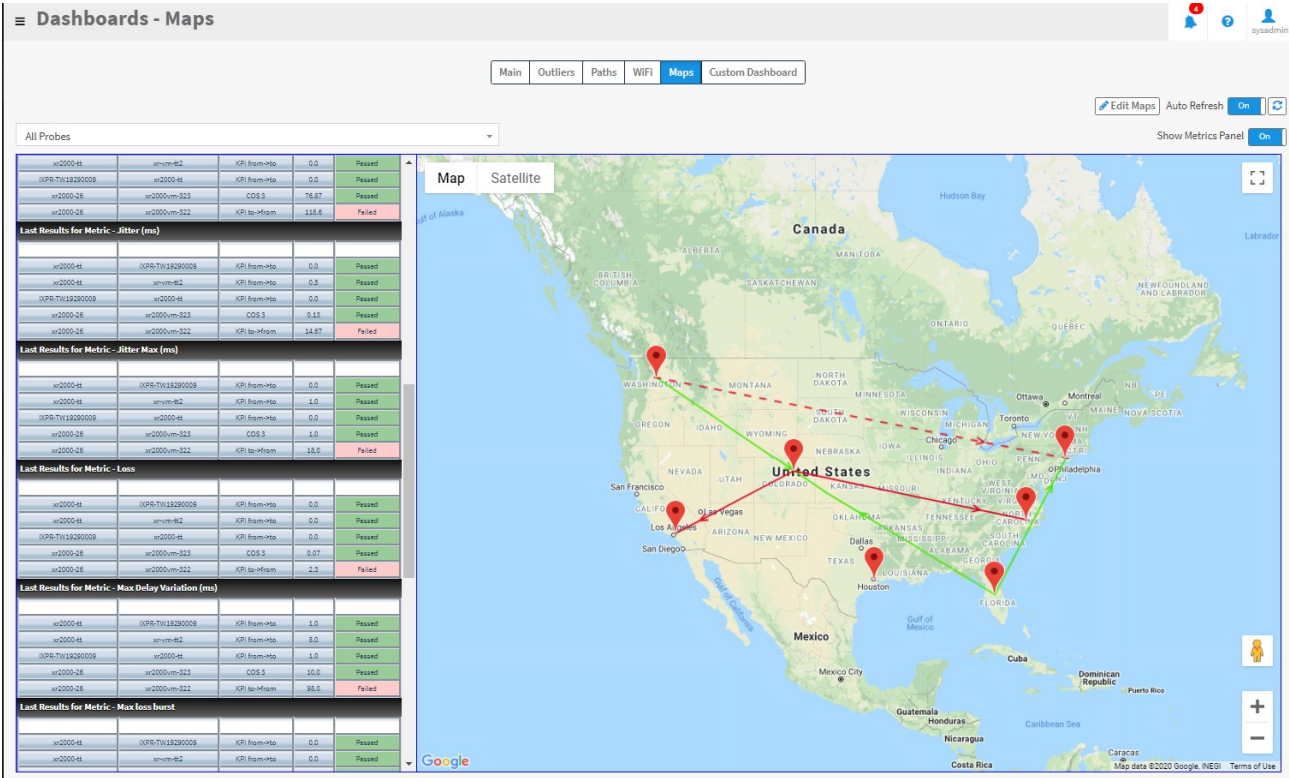
The screenshot shows the 'Map Configuration' interface. At the top, there's a header with a hamburger menu, the title 'Map Configuration', and user icons for notifications, help, and 'sysadmin'. Below the header, there's a '+ Create' button and a 'Maps' button. A 'Show' dropdown is set to '25'. The main area contains a table with the following columns: ID, Name, Type, Center Latitude, Center Longitude, and Zoom. There are two entries in the table:

ID	Name	Type	Center Latitude	Center Longitude	Zoom
1	Gmap	3	40	-95	3
2	Auto Mesh	3	40.8776	-99.1264	4

Below the table, it says 'Showing 1 to 2 of 2 entries'. At the bottom right, there are 'Previous', '1', and 'Next' buttons.

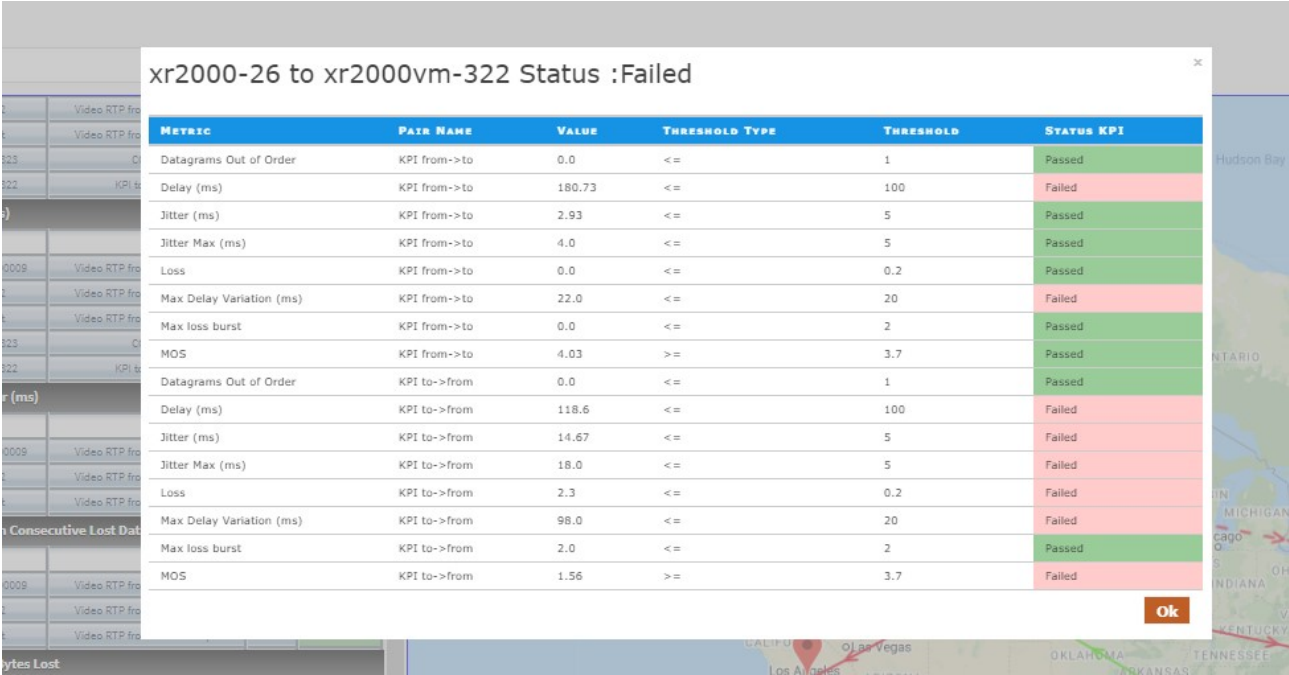
This menu offers the possibility to edit and remove maps. Also, the user can check quickly which probes are assigned to a map by expanding the desired map field.

To view the active status of a map, select **Dashboards**, select **MAPS**, then choose the map to monitor results.



The desired map will be displayed and the results of the tests that are executed between probes or inside the mesh.

To check details about the metrics measured on a particular path, select the line that connects those two points. A pop-up window will appear, showing the test details.



If the Hawkeye user, wants to check a different map, can do that by selecting it from the drop down list located on the bottom of the page.

NOTE

For system administrator users all maps are available. For group administrator users only the maps assigned to their group will be available.

NOTE

A map can be configured only by users with administrator privileges.

Custom dashboard

Hawkeye provides a way to customize dashboards by allowing you to create your own dashboards with certain widgets and filters. Thus, meeting your need to watch out for specific issues in your network.

Following are the available customizable widgets:

- Last Events
- Map
- Metric Graph
- Probes
- Top/Worst Probes/Paths

How do I...

This section covers the tasks that you can perform on custom dashboard:

Create a Custom Dashboard

As a first user, under Probes -> Manage Dashboard and Dashboards -> View Dashboards there will be one already created, demo dashboard.

To create a new Custom Dashboard, complete the following steps:

1. Go to **Probes > Manage Dashboards or Dashboards > View Dashboards**.
2. Select the **Add New** button to open a Create New page.
3. Fill in the details. Required fields are **Name**, **Probes**, **Visibility**, and **Dashboard Content**. You must select at least one from **Probes** list and **Dashboard Content**.
 - Select **Add Widget** to create a dashboard content from the available five widgets. See [Add Widget](#) for more information.
4. Select **Create**.

Add widget

Select **Add Widget** to create a dashboard content from the available five widgets.

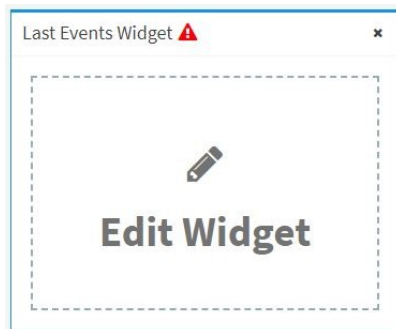
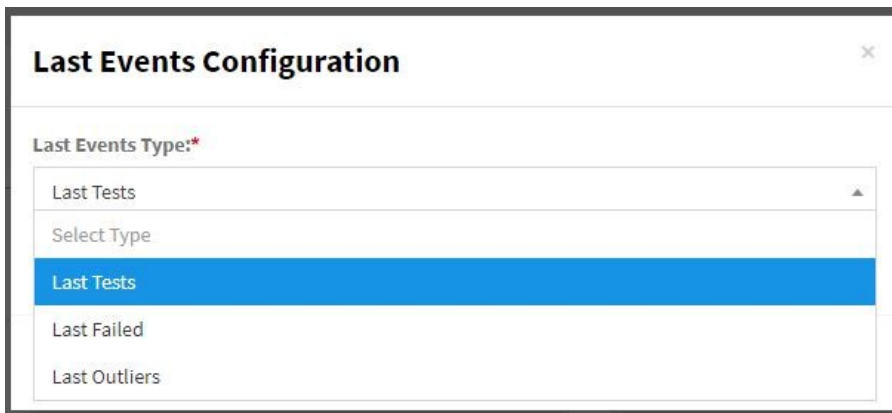
- Last Events
- Map
- Metric Graph

- Probes Status
- Top/Worst

Last Events

You can configure this widget based on configured tests, failed tests, number of outliers and number of rows.

- **Last Tests** shows the last configured number of tests.
- **Last Failed** shows the last configured number of failed tests.
- **Last Outliers** shows the last configured number of outliers.



Map

You must select a **Map Type**.

- You can move probes from one point to another.
- You can turn on or off the paths. When the **Path Representation** is turned on, the paths between probes are visible.
- You can turn on or off the Clustering Probes. When it is turned on, the map automatically shows a cluster of probes, instead of individual ones, when they are as close as 80px to each other.

Following are the available map types:

- **Logical Map**: You can upload an image of a map from your computer.

Map Configuration

Map Type: Logical Map

Select Your Image
 No file chosen

Define Test Passed Range For Each Color Representation Of Probe Icons:

Test Passed Range	Minimum(<)	Maximum(>)
Green (95% - 100%)	95 %	100 %
Yellow (75% - 95%)	75 %	95 %
Orange (50% - 75%)	50 %	75 %
Red (0% - 50%)	0 %	50 %

Display Path Representation:
☐ Yes ☒ No

Clustering Probes Enabled:
☒ Yes ☐ No

Select a marker on the map to enter the desired location!

- **Google Map:** This is the default map. You can select the probe marker to specify the address.

Map Configuration

Map Type: Google Map

Select Your Image
 No file chosen

Define Test Passed Range For Each Color Representation Of Probe Icons:

Test Passed Range	Minimum(<)	Maximum(>)
Green (95% - 100%)	95 %	100 %
Yellow (75% - 95%)	75 %	95 %
Orange (50% - 75%)	50 %	75 %
Red (0% - 50%)	0 %	50 %

Display Path Representation:
☒ Yes ☐ No

Clustering Probes Enabled:
☒ Yes ☐ No

Map Labels Hidden:
☒ Yes ☐ No

Map Color Mode:
☒ Dark ☐ Light

Select a marker on the map to enter the desired location!

Metric Graph

Select one metric to be displayed from all the available metrics. There are a few visual options for this widget that you can change later.

Metric Graph Configuration

Metric:

Delay (ms)

Graph Type:

Display Line:

Display Values:

Time Scale Granularity:

Threshold:

Save

Probes Status

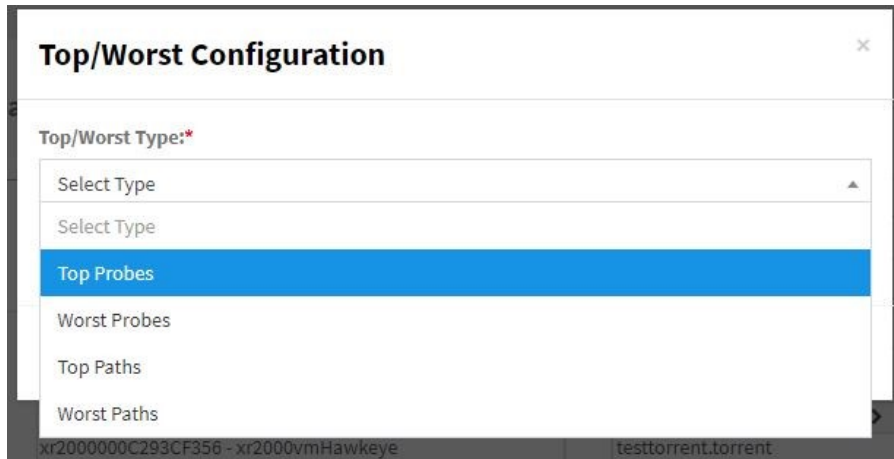
You cannot configure this widget. It shows the status (up or down) from the selected probes.

Probes Status Widget

Top/Worst

You can set your view based on top or worst probes, top or worst paths, and number of rows. Following are the available types:

- **Top Probes** option shows the probes with the best score within the filtered time frame. Score is calculated as a percentage from the total of tests.
- **Worst Probes** option shows the probes with the worst score.
- **Top Paths** option shows the paths with the best score within the filtered time frame. Score is calculated as a percentage from the total of tests.
- **Worst Paths** option shows the paths with the worst score.



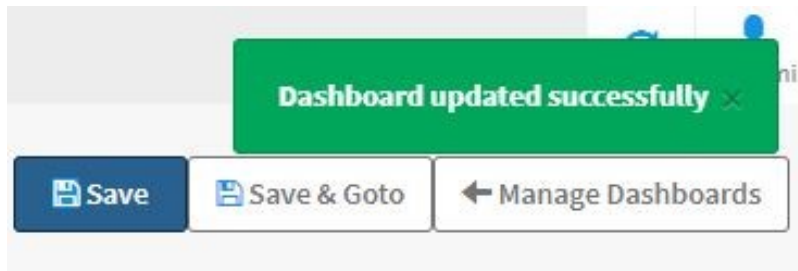
Update a Custom Dashboard

To update a Dashboard, complete the following:

1. Open the dashboard you want to edit by completing any of the following steps:
 - Go to **Probes > Manage Dashboards** and select the **Edit** for the dashboard you want to update.
 - Go to **Dashboards > View Dashboards** and select the desired dashboard from the drop down list and select **Edit**.

Any of the above step opens **Update dashboard** page that is similar to **Create New** page. You can update the dashboard from this page. You add, edit, or delete widget from this page.

2. Select **Save**, to show a green **Dashboard saved successfully** popup.



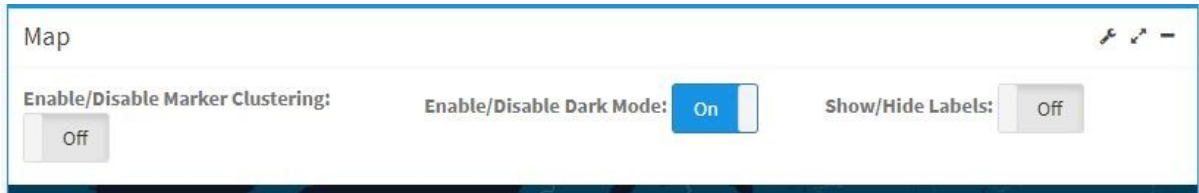
View a Custom Dashboard

To view a custom dashboard, complete one of the following:

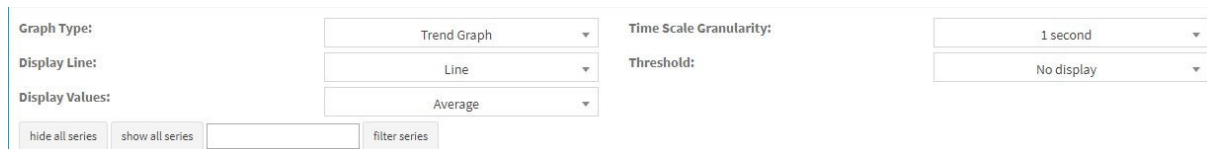
- When creating or updating a probe, select **Save & Goto** button. This action will redirect you to the **View Dashboards** page, with the selected dashboard as default.
- Go to **Dashboards > View Dashboards** and select the dashboard you want to view.

You can do the following from the **View Dashboards** page.

- You can expand or collapse a widget.
- You can turn on or turn off clustering, dark mode, and labels for **Map**.



- You can configure the graph type, line, values, time scale granularity, and threshold for **Metric Graphs**.



- You can reconfigure the number of rows to show and select another type of Event or Top/Worst Probe/Path.
- You cannot configure **Probe Status**.

Hawkeye preferences

Hawkeye application is configured through the **Preferences** screen.

Depending on user level some different configuration options can be accessed.

As system administrator (sysadmin user):

sysadmin

Administration - Preferences

Main

GUI

Alarms

Maps

Email

VisionE15

Traffic Port Management

Test Controller

Advanced Options

Installation Paths

Logs

Test Engine

Parameter Name

Value

Description

Details (Current Setting)

Result Access Control Type

0

Result access display control based on test execution (0) or probe group (1)

Access to results is based on test execution

Allow Test Frequency Time Unit Configuration

0

Allows to use frequency time unit configuration - in particular allow sub minute frequency

Disable Frequency Unit

Display Interval Optimiser

0

Each Scheduled test will be started n (test frequency) sec/min/hour from the start of the last test run. Over time slight drift may occur. If this preference is enabled (1) each test will show a 'Disable Interval Optimiser' checkbox that can be selected to force the test to be evenly spaced over time.

Tests will not display 'Disable Interval Optimiser' checkbox

Display Test Controller Status

1

1 to Display test controller (or agent) status table in administration table. Only required for system with distributed test controllers

Agent status table is displayed in administration table

Map Report

1

Enable/Disable map display

Map display is ENABLED

Maximum report generation Time

500

Maximum report generation time (seconds). Change to allow more time to generate reports

Number of days for database retention

365

Number of days for which data is stored. Value must be >= 10

Number of days for database retention for detailed metrics

180

number of days of keeping detailed metrics in the database

Number of days for database retention of admin elements

20

Number of days of keeping admin details (trail, execution logs, etc.) in the database.

Enforce Complex Password

0

Enforces users to use of mix of letters, numbers for password

Do not enforce

Save

Cancel

Restore Section To Default

Restore All To Default

Save DB Config Checkpoint

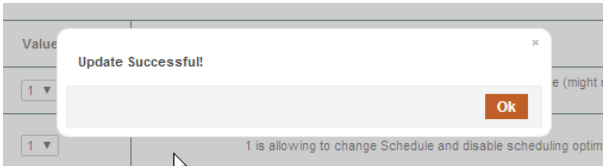
Restore Last DB Checkpoint

As user:

General	Parameter Name	Value	Description	Details (Current Setting)
	Default Calendar Range	LastDay	This parameters may take the following values: LastDay, LastHour, LastWeek. It defines the default time scale for the system when the user logs in. For best performance, use LastHour or LastDay.	Default calendar range is LAST DAY
	Refresh Table Interval (seconds)	120	Refresh table timer (in seconds). This will allow refreshing any table with autorefresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.	
	Use Droplist Search	1	In the drop lists there is an automatic search available (in filters). Set it to 0 to disable this and get standard drop lists.	Search in the dropdown lists (for filters) is ENABLED
	Dashboard Autorefresh	1	Enable/disable autorefresh for the main dashboard	Autorefresh for main dashboard is ENABLED
	Dashboard Autorefresh Interval (seconds)	180	Refresh interval for main dashboard (seconds). Setting it to lower than 30 seconds can result into a big impact on system performance.	
	Dashboard Real Test Display	all	OPTIONS: all, origin, destination. This setting allows the user to group the real test displays as: all - each pair client/server is one line; origin: each client is one line; destination: each server is one line.	Each pair client/server is one line
	Maximum lines displayed in Dashboard	20	Maximum of entries that will be displayed in Dashboard	
	Refresh Execution Table Interval (seconds)	20	Refresh Execution table timer (in seconds). This will allow refreshing the execution table with autorefresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.	
	Filter on IP format (v4 or v6) for automatic endpoint interfaces	IPv4only	Display only interfaces with specific IP format for automatic probes	IPv4 only
	Threshold for WiFi signal level in WiFi Dashboard	-50	Signal levels below this threshold will be displayed as weak levels and levels above this threshold will be displayed as good levels.	

Change setting

- 1. Change the desired settings in one screen (panel).
- 2. Save – a confirmation setting has been changed will be displayed.



Most of the parameters changing GUI aspects require a logout / login to be taken into account.

Section “General” for Users

The parameters located in section “GUI Settings” of the configuration file are explained, below.

Feature/Setting	Default Value	Comments
Display Interval Optimiser	0	Will allow schedule enforcing (see section on enforcing schedule in this guide Test Execution) => Disable Interval Optimizer.
Show Server/Client Time	0	Displays time on server to compare to client on top right. Note all times displayed in GUI are translated into CLIENT time.
Default Calendar Range	LastDay	This section allows: <ul style="list-style-type: none">• LastDay• LastHour• LastWeek It defines the default time scale for the system when user logs in. Recommendation is LastDay or Last Hour for better performance.

Refresh List Timer Value	120000	Refresh table timer (in milliseconds). This will allow refreshing any table with auto refresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.
Use Droplist Search	1 or 0	In the drop lists there is an automatic search available (in filters). Set it to 0 to disable this and get standard drop lists.
Dashboard Autorefresh	1 or 0	Enable/disable the auto refresh for main dashboard.
Dashboard Autorefresh Interval	180000	Refresh interval for main dashboard (milliseconds). Setting it to lower than 30 seconds can result into big impact on system performance.
Use Droplist Search	1 or 0	In the drop lists there is an automatic search available (in filters). Set it to 0 to disable this and get standard drop lists.
Dashboard Real Test Display	all	<p>OPTIONS: all, origin, destination</p> <p>This setting allows the global dashboard to group the real test displays per:</p> <ul style="list-style-type: none"> • all: each client/server is one line • origin: each client is one line • destination : each server is one line <p>It is recommended to use this setting if there are many tests executed against several destinations.</p>
Maximum lines displayed in Dashboard	20	Main Dashboard displays a maximum number of lines that will be displayed per pages. If there are more lines to display than user specific defined in this parameter, there will be several pages available to browse through results in GUI.
Refresh Execution List Timer	20000	<p>Refresh Execution table timer (in ms). This will allow refreshing the execution table with auto refresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.</p> <p>The refresh window is specific for test execution windows and overwrites the Refresh List Timer Value for test execution related lists (see Test Execution).</p>

Filter on IP format (v4 or V6) for automatic endpoint interfaces	IPV4only	Display only interfaces with specific IP format for automatic probes.
Threshold for WiFi signal level in WiFi Dashboard	50	The threshold value for WiFi signals indicating: <ul style="list-style-type: none"> • Weak levels, when signal levels are below threshold • Good levels, when signal levels are above threshold
Notification Alerts Silent Mode	0	Silence the notification alerts (bell icon in the top right corner)
Timezone	UTC	User Timezone

Section “Main” for Admins

The parameters located in section “GUI Settings” of the configuration file are explained, below.

Feature/Setting	Default Value	Comments
Result Access Control Type	0	Defines how the access to results is controlled. See Group User Management for full details. Value 0: the access control is based on test execution (who executed the test). Value 1: the access control is based on the probe (if all probes involved in test are available for the user group, the result will be available to the user).
Allow Frequency Unit Configuration	0	Allow to change the unit for test execution interval set. This will allow to use tests in schedules less than 1 minute. The default value is 0, set it to 1 so scheduling interval unit can be changed.
Add Port Numbers to Test Results	0	Setting this to 1 will allow all results for Node to Node to be enriched with the port used for the test pairs.
Display Test Controller Status	1	Displays test controller status into administration table.
Map Report	1	Setting to 0 will disable Map display. This can be useful if users do not have access to public internet and therefore cannot have access to Google map to display the maps.

Maximum report generation Time	500	Maximum time used to create report – can be changed to allow more time in case of extremely time consuming report creations.
Number of days for database retention	365	In Days Default time for keeping records in database.
Number of days for database retention for detailed metrics	180	Maximum time (days) for keeping detailed records on test results (individual results graphs).
Number of days for database retention of admin elements	20	Number of days of keeping admin details (trail, execution logs, etc.) in the database.
Enforce Complex Password	0	Enforces users to use of mix of letters, numbers for password.
Max Concurrent Tests in GUI	50	Is limitation in GUI of the number of concurrent tests (TCP) or voice calls (RTP). This is pure GUI. Allowing more than pair license will result on test impossible to execute and queuing forever.
Registration Server	localhost	IP or hostname of the Registration Server. Registration Server is a component that acts as a mediator between console and endpoints when firewalls exist between them. This should be left to localhost.
Allow Auto Registration of Endpoints	1	Allow/Block endpoints to register to the console automatically . This can be used for stopping more endpoints to register on the Hawkeye server.
Allow Full Range	1	Allows to use Full Range time lookup option for database lookup.
Display individual result graph time relative or absolute	Relative	Graph time relative or absolute in individual test results. This is for individual test result graph of detailed metrics. The timing can be absolute (exact date) or relative (start at 0s).
System Authentication Mode	Local	Mode for Authentication - (Local) Local Authentication only, (LDAP) Local or LDAP authentication [you can use the 'Test LDAP' button in the bottom button bar to test your settings once you save this preference], (Ixia) Ixia credentials when user has been added locally [internet connection required]

LDAP server address		LDAP Server (hostname or ip address) or a list of comma delimited servers
LDAP Domain		Domain DN in the format of either example.org or dc=example,dc=org
LDAP - Users Path		The user account folder in the LDAP tree. Example - CN=Users
LDAP - User Attributes		The comma separated list of user attributes to search for and compare the login against in the LDAP element.
LDAP - Enable secure LDAP (LDAPS)	0	Enable secure LDAP (LDAPS)
LDAP - Auto create Hawkeye user	0	Auto create Hawkeye user (if it does not exist already) when Authentication Mode is set to LDAP and user is authenticated successfully
LDAP - Enable group based authentication	0	Authenticate users based on their existence in the LDAP Group Path specified.
LDAP Group Path		Defines the group path as defined in the LDAP tree. (Used only when LDAP group based authentication preference above is set to 1)
LDAP Bind DN		Bind DN for connecting to LDAP. Leave it as empty for anonymous bind. (Used only when LDAP group based authentication preference above is turned on)
LDAP Bind DN Password		Password of LDAP Bind DN. Leave it as empty for anonymous bind (Used only when LDAP group based authentication preference above is turned on)

Section “GUI” for Administrator

Feature/Setting	Value	Comments
Timezone	UTC	User Timezone
Show Server/Client Time	0	<p>Displays time on server to compare to client on top right.</p> <div> NOTE All times displayed in GUI are translated into CLIENT time. </div>

Default Calendar Range	LastDay	<p>This section allows:</p> <ul style="list-style-type: none"> • LastDay • LastHour • LastWeek <p>It defines the default time scale for the system when user logs in.</p> <p>Recommendation is LastDay or Last Hour for better performance.</p>
Refresh List Timer Value	120000	Refresh table timer (in milliseconds). This will allow refreshing any table with auto refresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.
Max records per Page	50,000	Used for reporting long lists and limit the size of the reports (avoid very long report creation).
Allow URL	1 or 0	Set it to 1 to allow probe to have url instead of IP.
Use Droplist Search	1 or 0	In the drop lists there is an automatic search available (in filters). Set it to 0 to disable this and get standard drop lists.
Dashboard Autorefresh	1 or 0	Enable/disable the auto refresh for main dashboard.
Dashboard Autorefresh Interval	180000	Refresh interval for main dashboard (milliseconds). Setting it to lower than 30 seconds can result into big impact on system performance.
Dashboard Real Test Display	all	<p>OPTIONS: all, origin, destination</p> <p>This setting allows the global dashboard to group the real test displays per:</p> <ul style="list-style-type: none"> • all: each client/server is one line • origin: each client is one line • destination : each server is one line.
Maximum lines displayed in Dashboard	20	Maximum of entries that will be displayed in Dashboard - restricted to allow quick display. The results can be available clicking on the link in dashboard.
Refresh Execution List Timer	20000	Refresh Execution table timer (in ms). This will allow refreshing the execution table with

		<p>auto refresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.</p> <p>The refresh window is specific for test execution windows and overwrites the Refresh List Timer Value for test execution related lists (see Test Execution).</p>
Map Update Frequency in seconds	300	Map update frequency - do not set it with too low value (less than 30 seconds).
Max Idle Time	3600	Maximum session time (maximum time a user session is kept opened before being automatically disabled). Unit is second.
Allow Management from Probe in Probe Management	0	Displays test Controllers status. Only required if multiple controllers are used.
Display Threshold settings on Trend Graphs	0	Set to 1 to display thresholds on trend graphs.
Show Server/Client Time	0	Displays time on server to compare to client on top right. Note all times displayed in GUI are translated into CLIENT time.
Allow Management from Probe in Probe Management	0	<p>Configures availability of remote access button on probes:</p> <ul style="list-style-type: none"> • 0 - No buttons at all • 1 – allow restart to all users • 2 – allow all (restart and reboot) for all users • 3 – allow restart only for admin • 4 - 2 – allow all (restart and reboot) for admin
Threshold for Wi-Fi signal level in Wi-Fi Dashboard	-50	Signal levels below this threshold will be displayed as weak levels and levels above this threshold will be displayed as good levels.

Section “Alarms” for Administrator

Alarm Settings		
Feature/Setting	Value	Comments
SnmpTrapServerIP	x.y.z.t	IP address of the SNMP trap server. Default 192.168.174.130.

UseEmailAlarm	1 or 0	Enable/disable the alarms received by email.
UseSNMPAlarm	1 or 0	Enable/disable the alarms received using SNMP.
ConditionalTimeAlarms	1 or 0	Enable/disable the conditional time alarms.
StartAlarmTime	06:00	Value for start time of conditional time alarms.
EndAlarmTime	23:00	Value for end of conditional time alarms.

Section “Maps” for Administrator

The parameters located in section “MAPS Settings” of the configuration file are explained, below.

MAPS Settings		
Feature/Setting	Value	Comments
UseGoogleMap	1 or 0	Enable/disable the usage of Google Maps.
GoogleMapKey		See below details of how to obtain a Google Map Key.
MapRetentionMinute	240	Number of minutes for the map to look database results. Any results older than this value will not be considered (might result in empty map).
Google MAP API URL	Standard	Google MAP API URL - Standard for China location

Obtain Google Map Key

In order to use the Google map, a key must be generated.

On the following link there are details about the process of obtaining such key:

https://developers.google.com/maps/documentation/JavaScript/tutorial?hl=fr#api_key

A valid Gmail account is required in order to generate the key.

Section “Email” for Administrator

Feature/Setting	Value	Comments
SMTP_Server		The address of the SMTP server.
SMTPDebug		
SMTPAuth	true or false	True if authentication is used, false if no authentication is configured for the SMTP account.

SMTPSecure	SSL or TLS	Configure SSL if Secure Sockets Layer cryptographic protocol is used, TLS if Transport Layer Security protocol is configured for the SMTP account or none if no security is used.
Port	25 or 465 or 587	Configure port 465 for SSL, 587 port for TLS or 25 default SMTP port for no security.
Username		Username of the SMTP account.
Password		Password for the SMTP account.
EmailAddress		The SMTP e-mail address.
FullName		Sender name.
MaxEmailAttempts	3	How many times should the application try to send the message.

Example of settings for gmail account:

Parameter Name	Value	Description	Details (Current Setting)
SMTP Server	<input type="text" value="smtp.gmail.com"/>	The address of the SMTP server.	
SMTP Authentication	<input type="button" value="1"/>	True if authentication is used, false if no authentication is configured for the SMTP account.	Authentication for SMTP account is ENABLED
SMTP Security	<input type="button" value="SSL"/>	Configure SSL if Secure Sockets Layer cryptographic protocol is used, TLS if Transport Layer Security protocol is configured for the SMTP account or none if no security is used.	Secure Sockets Layer cryptographic protocol is used
Port	<input type="button" value="465"/>	Configure port 465 for SSL, 587 port for TLS or 25 default SMTP port for no security.	Using SSL
Username	<input type="text" value="user@gmail.com"/>	Username of SMTP account	
Password	<input type="password" value=""/>	Password of the SMTP account	
Email address	<input type="text" value="user@gmail.com"/>	The SMTP email address	
Full Name	<input type="text" value="IxChariotPro Email"/>	Sender name	
Max Email Attempts	<input type="text" value="3"/>	How many times should the application try to send the message.	



Save

Cancel

Restore Section to Default

Restore All to Default

Section “Traffic Port Management” for Administrator

Feature/Setting	Value	Comments
Destination Port Conf Option	0 or 1 or 2	<p>The test controller will increment the port to be used for each test as follows:</p> <ul style="list-style-type: none"> • 0: will be set to AUTO • 1: will start on range (increment 1 on per destination probe basis) • 2: Hawkeye Test controller will increment the port number for each test, regardless of probe used.
First Destination Port	10200	Destination port for Hawkeye test types start of

		range. Default 10116.
Source Port Conf Option	0 or 1 or 2	<p>The test controller will increment the port to be used for each test as follows:</p> <ul style="list-style-type: none"> • 0: will be set to AUTO • 1: will start on range (increment 1 on per destination probe basis) • 2: Hawkeye Test controller will increment the port number for each test, regardless of probe used.
First Source Port	10216	Source port for Hawkeye test types start of range. Default 10216.
Use Skype4B Special Range	0	Use special ports range for Skype4B traffic tests.
Skype4B - First Audio Source Port	10301	Skype4B - First Audio Source Port.
Skype4B - First Audio Destination Port	10201	Skype4B - First Audio Destination Port.
Skype4B - First Video Source Port	10351	Skype4B - First Video Source Port.
Skype4B - First Video Destination Port	10251	Skype4B - First Video Destination Port.
Add Port Numbers to Test Results	0	1 to add port used information in all N2N or Mesh tests. Note, one of "Destination Port Conf Option", "Source Port Conf Option" and/or "Use Skype4B Special range" must have the parameter set to "range".
Probe Firewall Configure	secure	Applies to vision1s and xr_vm probe types only. Secure = Close all ports / Configure = Disable Firewall and open ports based on Destination Port Conf Option, Destination Ports, Use Skype4B and Voice Spectial Range, Skype4B and Voice Audio Destination Ports, and Skype4B Video Destination Port

Section "Test Controller" for Administrator

Feature/Setting	Default Value	Comments
Real Test Max Duration	180	Maximum duration of a real test.

Probe Health Check	1	Enable/disable the probe health check engine.
Test E2 Available	1	Test both Endpoint 1 and endpoint 2 availability from Test controller for the test. In network configuration where Endpoint 2 is not available from test controller it might be useful to disable this test.
Probe management identification	1	<p>By default the probe id is used to identify a probe. For some systems where a physical probe has several interfaces. For the resource management to consider same physical probe this option needs to be activated (1) and probes management address set to the same interface (same IP or url).</p> <p>Note that when the Serial number is configured on an endpoint, that is, Web UI Probe Management serial number is not set to blank or 'default' for an endpoint, this always takes precedence over the method defined here.</p>
Endpoint Autorestart	1	Enable/disable the auto restart feature for Hawkeye endpoint. If enabled the endpoint will auto restart at AutorestartIntervalMinutes.
Endpoint Autorestart Interval	360 minutes	Interval for the endpoint auto restarts time.
Autorestart Max Duration	30	Maximum duration of autorestart process.
Real Service Port	22	Port required by the test agent to connect to the probes to run real services test types.
Alarm on Probe Status Change	0	Enable alarms (email or SNMP) when probe becomes not available. Send alarm when status changes (available/not available).
Alarm on Probe Health Fail	0	Send an alarm when probe is not available (every check).
Probe Default Login	root	Probe default Login - overridden by probe specific configuration.
Probe Default Password	Ixia!123	Probe default Password - overridden by probe specific configuration.
Clock synchronization between endpoints	Auto	To report UDP and RTP statistics, such as, One-Way Delay, Jitter, VoIP MOS and Video Delay Factor, it is necessary for IxChariot to know the difference between the clocks of the sending and receiving endpoint.

		<p>When Auto is selected, the endpoints use a proprietary algorithm, involving exchanging UDP packets over the UDP port 10115, to evaluate the clock difference. This algorithm is reasonably accurate and its error (which is somewhere between the reported statistics Estimated Error and Maximum Error) is generally between few milliseconds and tens of milliseconds.</p> <p>Occasionally, when a firewall blocks the UDP port 10115 or the network experiences high data loss, the endpoints are unable to synchronize their clocks through this method. This algorithm is increasingly inaccurate on asymmetric connections, where data travels faster in one direction than in the other.</p> <p>The External option assumes the endpoints have been synchronized through some external method (such as manual clock setting or NTP) to have the same local time. It is a way to avoid the limitations of the Auto method.</p>
Endpoint Management QoS	None	<p>Apply QoS template to the management traffic generated by the Endpoints to/from Hawkeye server and other endpoints. This will not apply to test traffic.</p> <p>Supported options are:</p> <ul style="list-style-type: none"> • None • EF
Report N2N delay metrics in microsecond resolution	0	<p>Report N2N delay metrics in microsecond resolution for metrics like Delay and Video Delay Factor. Values are displayed in the UI as milliseconds with microsecond decimal resolution. Warning: versions of endpoint older than 10.0 build 200 do not support this feature and tests with those endpoints will error with a corresponding error message.</p>

Section “Advanced Options” for Administrator

Feature/Setting	Default Value	Comments
Report Header Image	images/reportheader.gif	Customize the report header image by changing the reference to the gif image. The gif image needs to be placed into the installation folder. (see admin manual for report folder, typically c:/ixia/Hawkeye/main/webserver/images.)
Probe Busy	0 or 1	<ul style="list-style-type: none"> • 1 – Enable the Probe Busy functionality. • 0 – Disable the Probe Busy functionality.
License Reporting Threshold	0	<ul style="list-style-type: none"> • Description: Report in the Audit Trail when the count of active users exceeds percentage of licenses available (0=disable) • Details: Percentage in range 0 to 100%
Use Mesh	1	<ul style="list-style-type: none"> • 0 if the mesh testing is disabled • 1 if the mesh testing is enabled
Maximum time processing Node to node or mesh test	200	Advanced Setting : safety timer - maximum time (seconds) system waits before trashing node to node or mesh test - do not set below 120 seconds.
Maximum time processing real service test	120	Advanced Setting : safety timer - maximum time (seconds) system waits before canceling Hawkeye test - do not set below 60 seconds.
Use probe configuration Script for node to node real services	0	Advanced Setting : allow optional use of probe configuration script before and after tests.
Maximum pairs per test controller instance	500	Advanced Setting : maximum pairs in each controller instance - this setting is only taken into account if controllers are configured with ability to control same probe at same time with different times.
Allow probes to run NodetoNode and real services at same time	0	Advanced Setting : Allow probes to run NodetoNode and real services at same time. Can result into inaccurate test results as tests can interfere with each others.
Real Services: default interval time	5	Advanced Setting : refresh time for automatic endpoints - default is 5 seconds.

for automatic endpoints		
Real Services: default retry time for automatic endpoints	0	Advanced Setting : retry time for automatic endpoints - default is 0 seconds (immediate retry).
Disable Real Services and Autoregistration for Automatic Endpoints	0	Stop Responses to Automatic Endpoints - do not run any tests nor register new information or endpoints.
Test Controller: Polling Interval	4	Advanced Setting : Polling interval time in seconds for Test Controller - default is 4 seconds.
Maximum number of graphs in a saved or scheduled Report	100	Maximum number of graphs that will be created for a saved or scheduled report - setting this to higher than 2000 can impact system performance and delay or cause failure in report generation.
Set Test IP that matches Default Gateway (Mesh tests only)	0	Applies to Mesh tests on XR automatic endpoints with multiple network connections. When this flag is not enabled, eth0 is used for traffic, if flag is enabled, traffic will use network connection that matches the Default Gateway in Probe Management
Wifi Connect Test Execution Interval (minutes)	5	Only one Wifi Connect Test per endpoint will be executed in this configured interval window
Tests count before setting Auto Learned Threshold	25	Advanced Settings: tests counter. Specify the number of tests running in learning phase before setting auto-learned threshold for a metric. Note auto-learn threshold must be turned ON to use this setting.

Section “Installation Paths” for Administrator

These values are fixed at Install time Relative paths are relative to Server Path		
Parameter Name	Value	Description
Installation Path	/home/ixia/Hawkeye/	Directory where the installation is rooted
Configuration File	<InstallDir>/conf/configuration.txt	path for Hawkeye configuration file
Server Path	<InstallDir>/WebServer/	path for Hawkeye web files
IxChariot Logs	<InstallDir>/logs/Chariot/	path to IxChariot log files.
Hawkeye Logs	<InstallDir>/logs/Hawkeye/	path to Hawkeye log files.
Reports	<ServerPath>/tmp/reports/	path to report files
Saved Reports	<ServerPath>/SavedReports/	path to Saved report files
Temp Images	<ServerPath>/tmp/img	path to temporary folder for images

Section “IxProbe” for Administrator

Feature/Setting	Value	Comment
IxProbe Auto Upgrade	Disabled	Disable/Schedule/Enable auto upgrade global flag for IxProbes

Section “Logs” for Administrator

Feature/Setting	Value	Comments
Database Debug	1 or 0	Enable/disable debug on database.
Page Setup Debug	1 or 0	Enable/disable debug on page setup.
Page Action Debug	1 or 0	Enable/disable debug on page action.
Debug JavaScript	1 or 0	Enable/disable debug on java script.
Log Retention Minutes	240	How long the application logs will be retained. The application logs are located in C:\Ixia\HawkeyePro\log_server.
Test Engine Log Retention Minutes	1440	Log retention for underlying test engine - need to be more than 240 minutes. The engine logs are located in C:\Ixia\HawkeyePro\log_chariot.
Log Max Age days	1	Remove rotated logs older than X days
Log Rotation Interval	Daily	Log files are rotated when they grow bigger (daily/weekly/monthly/yearly)

Section “Test Engine” for Administrator

This section allows configuration of the C:/opt/hawkeye/conf/configTestEngine.txt file on the server.

Parameter Name	Default Value	Description
lowsendjitter	0	Enables low send jitter algorithm on probes. It allows probes to generate UDP or RTP traffic in an optimized way to avoid any bursty traffic. This parameter should be set to 1 to enable the feature. It is very useful in case of testing Class of Services or traffic shapers that can be sensitive to bursts.
maxWait	60 sec	Maximum time waiting for Hawkeye test engine to finish the test (on top of test duration + Statistics receive timeout).
maxInit	60 sec	Maximum time waiting for Hawkeye test engine to initiate the connection.
autoNAT	0	Needs to be set to 1 in order to allow probes to be managed behind NAT (their address are configured as Public IP from console). Setting this parameter to 1 will allow console to manage the probes behind NAT. Port forwarding still needs to be put in place on the probe NATing to allow management (10115) and traffic (configuration in Test controller section).
ForceE2managementInBand	0	Setting this parameter to 1 will force the management traffic between E1 and E2 to be in band. Console initiates connection on management interface but management between endpoints is in band. This option is required for specific installation.
ConsoleBehindFirewall	1	This needs to be set to 0 in case of using multiple threads in parallel. Constraint is console needs to be able to be directly connected to probes (ie not behind a firewall/NAT).
ALLOW_PAIR_REINIT	1	Activate probe pair setup retry capability. Useful in unstable network for management. Setting up this to 1 might create side effects on probes if tests are executed in volumes.
PAIR_REINIT_MAX	3	Numbers of tries before giving up. WARNING

		Setting this parameter to 0 will cause test engine to fail all execution.
PAIR_REINIT_RETRY_INTERVAL	100 sec	Interval for retrying. WARNING Setting this parameter to 0 will cause test engine to fail all execution.
ALLOW_PAIR_REINIT_RUN	0	Activate traffic retry capability during test. Useful in unstable network for traffic in case of TCP. Setting up this to 1 might create side effects on probes if tests are executed in volumes.
PAIR_REINIT_MAX_RUN	3	Numbers of tries before giving up. WARNING Setting this parameter to 0 will cause test engine to fail all execution.
PAIR_REINIT_RETRY_INTERVAL_RUN	100 sec	Interval for retrying. WARNING Setting this parameter to 0 will cause test engine to fail all execution.
Statistics receive timeout	30 sec	The timeout controls how long to wait for statistics until giving up and considering the test traffic connection failed. Error (CHR0529) is reported for the test traffic connections that do not report any statistics for the configured timeout duration.

Section “VisionE1S” for Administrator

Feature/Setting	Value	Comment
Set as Start Page	Main Dashboard	Landing page after login is Main Dashboard/VisionE1S

Configuring Automatic Email Notifications

The Hawkeye can optionally generate emails for scheduled reports and tests that fail or error. You can configure the email account for this service in **System Preferences > Email** section. You can configure the Hawkeye server to have an email client that can generate emails. You will need to configure your organizations email service provider SMTP server settings, such as Gmail server settings, and your organization’s email account credentials in **Email** section to handle sending emails for the Hawkeye server.

This page intentionally left blank.

CHAPTER 5

Hawkeye User Interface Results

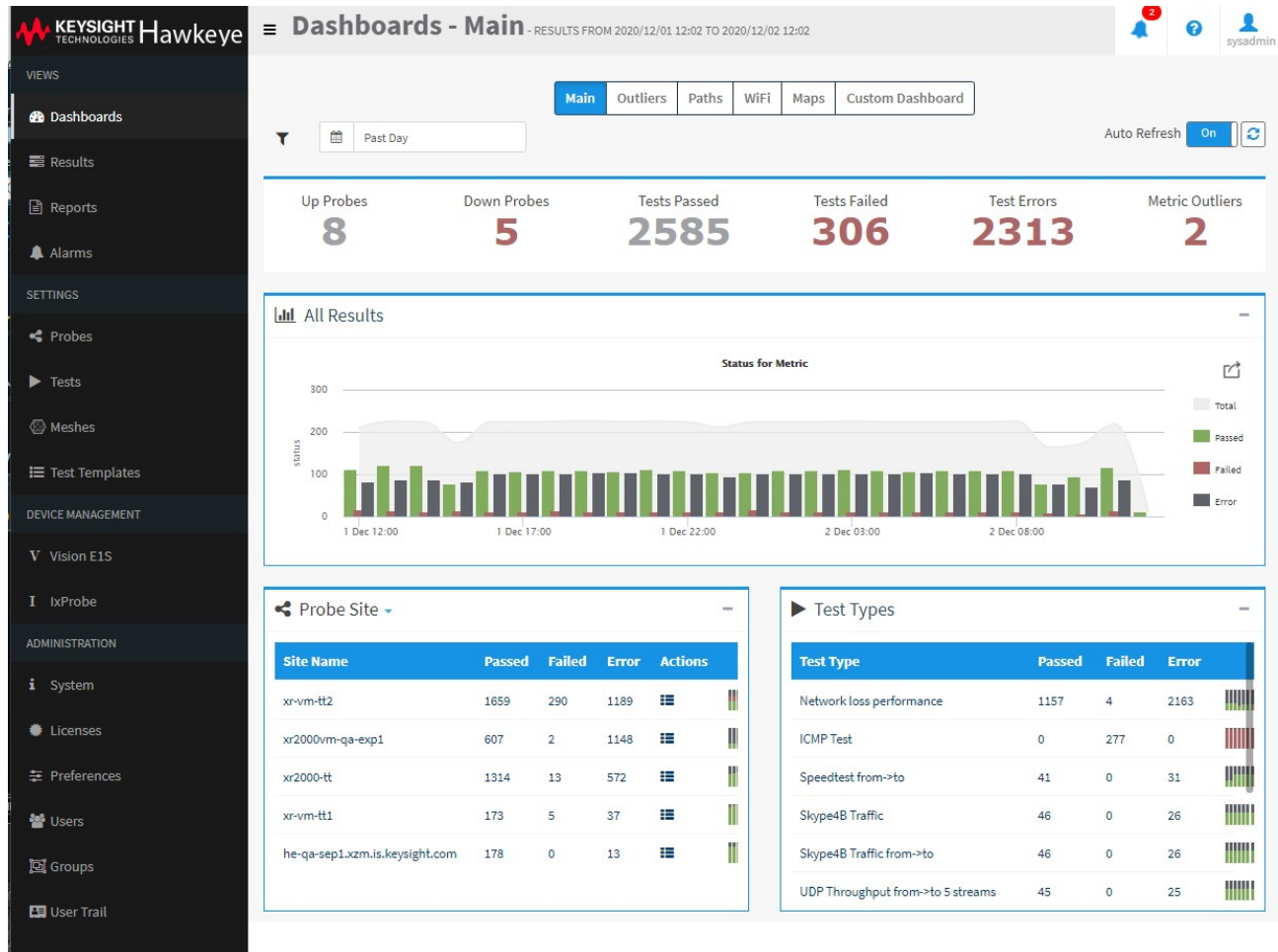
This chapter describes the user interface.

In this chapter:

Main Dashboard	146
Wi-Fi Dashboard	146
Test Results Screens	148
Map Status	152
Hawkeye Reports	152
Paths	159
Outlier	160

Main Dashboard

This is the first page that it is displayed after the user is logged in.

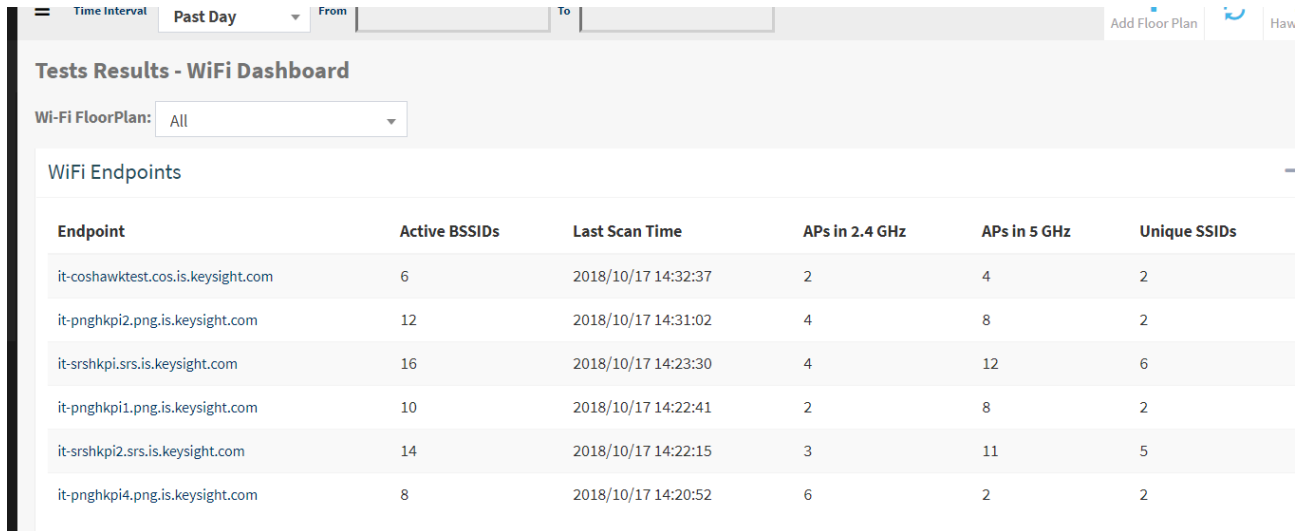


In the main dashboard the user can find the following:

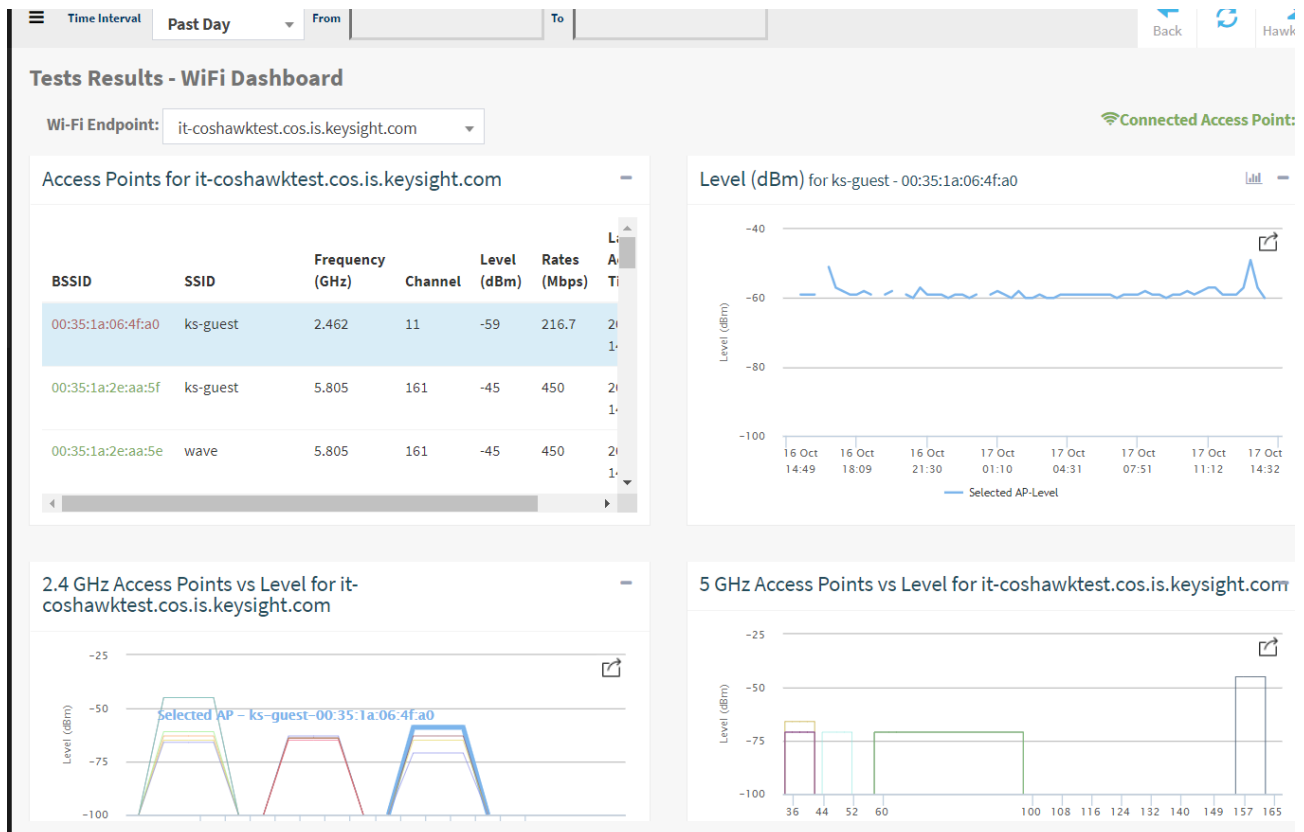
- summary of probe status;
- summary of tests passed/failed;
- summary of probes globally located;
- list of ten probes with most issues;
- list of 10 test types with most issues.

Wi-Fi Dashboard

The **Wi-Fi Dashboard** displays results of the Real Services Wi-Fi Inspect test performed on XRPi Wi-Fi probes. The **Wi-Fi Dashboard** displays the results when a XRPi Wi-Fi endpoint or a floorplan is selected.



Select a XRPi Wi-Fi endpoint to display four panes with information on the selected endpoint. The list of all Access Points (AP) in range and metrics of each selected AP in the list is displayed. Wi-Fi charts for 2.4 GHz and another one for 5 GHz shows the spread of available APs over the channel IDs, and provides an indication of possible interference amongst APs using the same channel IDs.



Test Results Screens

The results page contains all the details (such as, date and time of execution, which user executed the test, test type, from/to probe IP/name, test duration, status, reason) of all the tests that were executed.

You can find the test results by selecting **Results** located on the side bar.

Status	Date	From	To	Test Id	Test Tag	Test Type	Options	Reason
Failed	2020-12-02 14:31:09	xr-vm-tt2	www.espn.com	121		ICMP Test	Destination...	Threshold failed...
Success	2020-12-02 14:30:41	xr-vm-tt2	Office 365	93		Office365	Office365 Server...	
Success	2020-12-02 14:30:23	xr-vm-tt1	Office 365	92		Office365	Office365 Server...	
Success	2020-12-02 14:30:18	xr-vm-tt2	upload_2	26		DropBox Upload	DropBox File...	
Success	2020-12-02 14:29:06	xr-vm-tt2	upload_1	25		DropBox Download	DropBox File...	
Failed	2020-12-02 14:28:35	xr2000-tt	Office 365	94	2 hour	Office365	Office365 Server...	Threshold failed...
Success	2020-12-02 14:26:26	xr-vm-tt2	upload_2	26		DropBox Upload	DropBox File...	
Failed	2020-12-02 14:26:09	xr-vm-tt2	www.espn.com	121		ICMP Test	Destination...	Threshold failed...
Success	2020-12-02 14:26:03	xr-vm-tt2	upload_1	25		DropBox Download	DropBox File...	
Success	2020-12-02 14:24:53	xr2000vm-qa-exp1	IXPR-TW19290009	156		Voice from->to	Voice Codec...	
Success	2020-12-02 14:24:52	xr-vm-tt2	IXPR-TW19290009	156		Voice from->to	Voice Codec...	
Success	2020-12-02 14:24:52	xr2000vm-qa-exp1	xr2000-tt	156		Voice from->to	Voice Codec...	
Success	2020-12-02 14:24:51	xr-vm-tt2	xr2000-tt	156		Voice from->to	Voice Codec...	

By default, you can see the results of the tests that were ran on the last day. If you want to see the results of all the tests that were ran earlier, they can use the **full range** as the value for the **time interval** parameter under **time selection** tab on the left side. You can select one of the options (**full range, last hour, last day, last week, today, range**) for the time interval parameter based on the requirement.

Test results of other users can be viewed depending on your admin level privileges.

The table below explains the test results that a you can see depending on your admin level and option selected for result access rights:

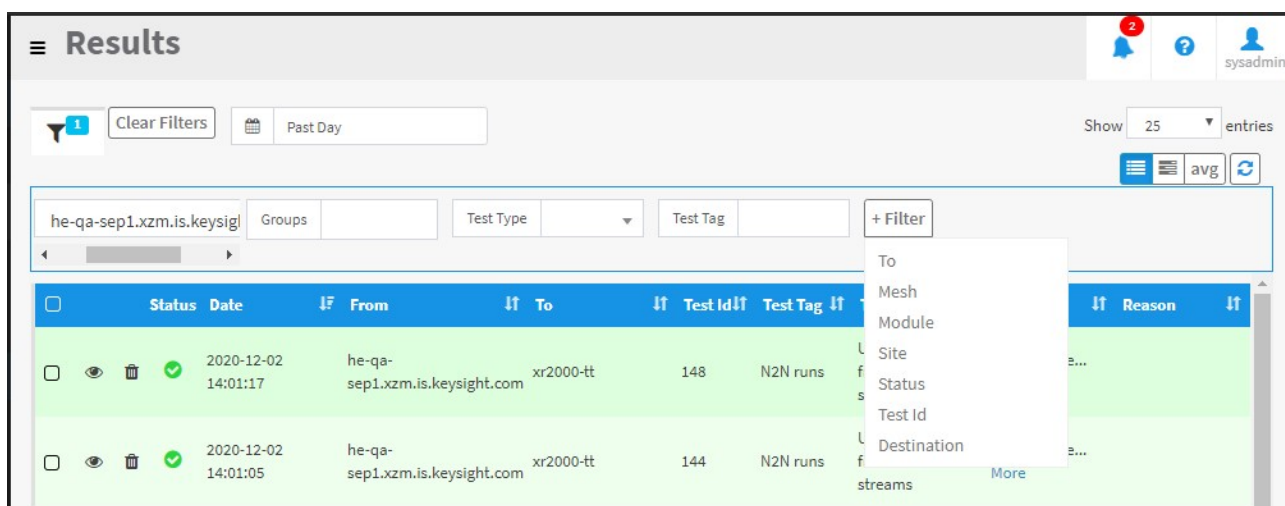
Main	Parameter Name	Value	Description	Details (Current Setting)
	Result Access Control Type	1	Result display control based on test execution (0) or probe group (1)	Access to results is based on probe group

Privilege Level	Test Results	Result Access Rights Option
-----------------	--------------	-----------------------------

Admin Level	Results Viewed. Test execution based.	Result viewed. Probe group access based.
System Administrator	View the test results of the tests executed by all users.	View the test results of the tests executed by all users.
Group Administrator	View the test results of the tests executed by the users belonging to that particular group.	View the results of the test executed with one (real service) or both probes (n2n) belonging to the user group.
Group Viewer	View the test results of the tests executed by the users belonging to that particular group.	View the results of the test executed with one (real service) or both probes (n2n) belonging to the user group.
User	View the test results of the tests executed the by the user itself.	View the results of the test executed with one (real service) or both probes (n2n) belonging to the user group.
Full System Viewer	View the test results of the tests executed by all the users. This right allows only viewing the results.	View the test results of the tests executed by all the users. This right allows only viewing the results.

Filters

Hawkeye allows you to filter the test results, as shown below:



You can set the filters as required.

For example: If you want to see the test results of the tests that were run between the Calabasas node and the Austin node, select **Calabasas** as the value for the **NODE FROM** field and **Austin** as the value for the **NODE TO** field, as shown above.

This will show the filtered results.

If you want to see only the results that passed, the user can select Passed value from the **status TDR** field.

Select **Clear Filters** button to clear the filters. After resetting, all the fields will be removed and all the test results will be displayed.

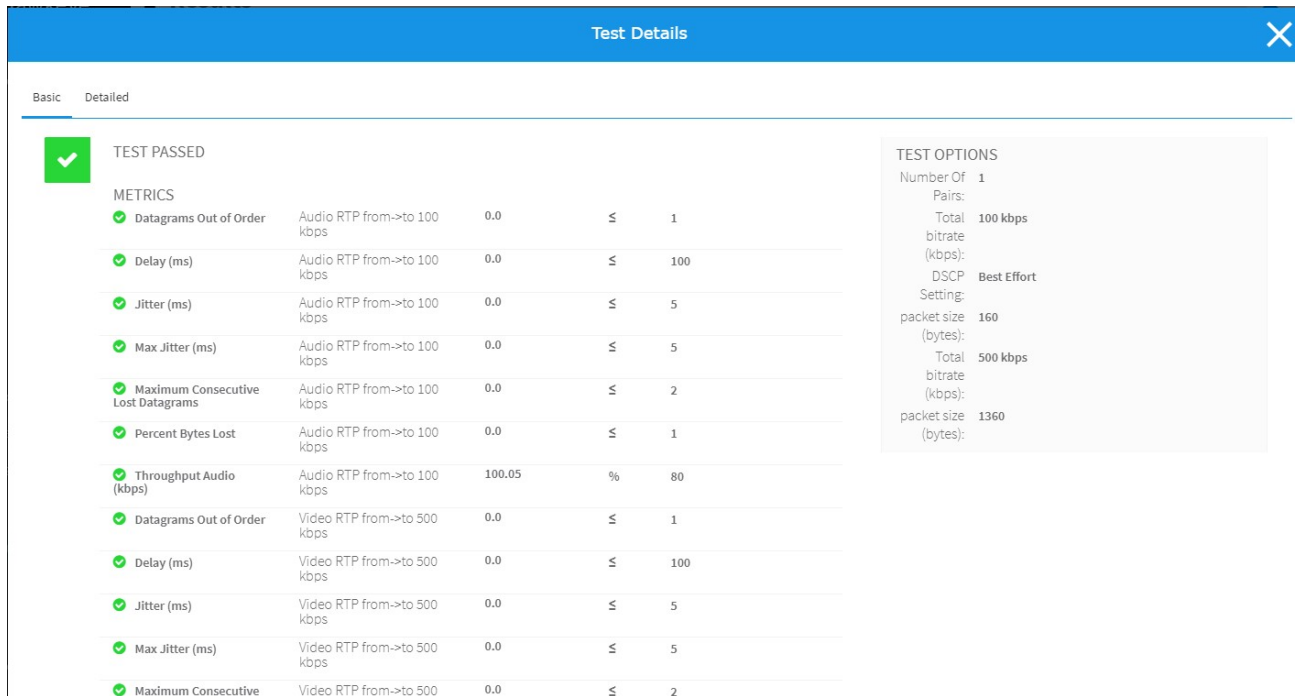
Select the **refresh table** button, at the bottom of the page, to update the test results of the tests that were in running stage.

NOTE

The test results of the tests that were in running stage will be updated only if the tests are complete.

Detailed Summary of a Test

To see the details of a test, select the  icon, as shown below:



Test Details

Basic Detailed

TEST PASSED

METRICS

✓ Datagrams Out of Order	Audio RTP from->to 100 kbps	0.0	≤	1
✓ Delay (ms)	Audio RTP from->to 100 kbps	0.0	≤	100
✓ Jitter (ms)	Audio RTP from->to 100 kbps	0.0	≤	5
✓ Max Jitter (ms)	Audio RTP from->to 100 kbps	0.0	≤	5
✓ Maximum Consecutive Lost Datagrams	Audio RTP from->to 100 kbps	0.0	≤	2
✓ Percent Bytes Lost	Audio RTP from->to 100 kbps	0.0	≤	1
✓ Throughput Audio (kbps)	Audio RTP from->to 100 kbps	100.05	%	80
✓ Datagrams Out of Order	Video RTP from->to 500 kbps	0.0	≤	1
✓ Delay (ms)	Video RTP from->to 500 kbps	0.0	≤	100
✓ Jitter (ms)	Video RTP from->to 500 kbps	0.0	≤	5
✓ Max Jitter (ms)	Video RTP from->to 500 kbps	0.0	≤	5
✓ Maximum Consecutive	Video RTP from->to 500 kbps	0.0	≤	2

TEST OPTIONS

Number Of Pairs: 1

Total bitrate (kbps): 100 kbps

DSCP Setting: Best Effort

packet size (bytes): 160

Total bitrate (kbps): 500 kbps

packet size (bytes): 1360

By selecting the **Test results metrics**  button on the **Results** page, you can access the detailed metrics report, as shown in the picture below:

Results

Past 3 Hours Metric All Pair All

avg Show 25 entries

Status	KPI	TDR	Date	From	To	Test Id	Test Tag	Test Type	Metric	Pair	Value	Limit
✓	✓	✓	2020-12-02 21:28:37	xr-vm-tt2	upload_1	25		DropBox Download	Download Rate (kbps)	DropBox Download	493.49	≥ 200
✓	✓	✓	2020-12-02 21:28:37	xr-vm-tt2	upload_1	25		DropBox Download	Download Time (ms)	DropBox Download	1660	≥ 0
✓	✓	✓	2020-12-02 21:28:37	xr-vm-tt2	upload_1	25		DropBox Download	File Size (kb)	DropBox Download	100	≥ 0
✓	✓	✓	2020-12-02 21:28:03	xr-vm-tt2	upload_2	26		DropBox Upload	File Size (kb)	DropBox Upload	500	≥ 0
✓	✓	✓	2020-12-02 21:28:03	xr-vm-tt2	upload_2	26		DropBox Upload	Upload Rate (kbps)	DropBox Upload	1412.41	≥ 200
✓	✓	✓	2020-12-02 21:28:03	xr-vm-tt2	upload_2	26		DropBox Upload	Upload Time (ms)	DropBox Upload	2900	≥ 0
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Availability	ICMP Test	1	≥ 1
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Jitter (ms)	ICMP Test	0	≤ 8
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Jitter standard deviation	ICMP Test	0	≤ 2
✗	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Packet loss	ICMP Test	4	≤ 1
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Round trip time avg (ms)	ICMP Test	0	≤ 300
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Round trip time max (ms)	ICMP Test	0	≤ 400
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Round trip time min (ms)	ICMP Test	0	≤ 300
✓	✗	✗	2020-12-02 21:27:35	xr-vm-tt2	www.espn.com	121		ICMP Test	Standard deviation (ms)	ICMP Test	0	≤ 20

By selecting the **Test results metrics average**  button on the **Results** page, you can access the average metrics report, as shown in the picture below:

Results

Past 3 Hours Metric All Pair All

avg Show 25 entries

From	To	Test Tag	Test Type	Metric	Pair	Count	Avg	Min	Max	Std. Dev
xr-vm-tt2	upload_1		DropBox Download	Download Rate (kbps)	DropBox Download	59	505.29	395.75	553.51	38.2
xr-vm-tt2	upload_1		DropBox Download	Download Time (ms)	DropBox Download	59	1631.53	1480	2070	136.34
xr-vm-tt2	upload_1		DropBox Download	File Size (kb)	DropBox Download	59	100	100	100	0
xr-vm-tt2	upload_2		DropBox Upload	File Size (kb)	DropBox Upload	59	500	500	500	0
xr-vm-tt2	upload_2		DropBox Upload	Upload Rate (kbps)	DropBox Upload	59	1392.81	477.39	1593.77	179.44
xr-vm-tt2	upload_2		DropBox Upload	Upload Time (ms)	DropBox Upload	59	3034.41	2570	8580	796.93

Skype4R Traffic from-

Remove a Test Result Entry

You can delete a test result by clicking the  delete icon located next to the **Run ID** column.

Bulk deletion of test results is possible by checking the boxes on the left of each result you want to delete then select the **Bulk Actions**  button and select **Delete**.

Results

Past 3 Hours

avg

Show

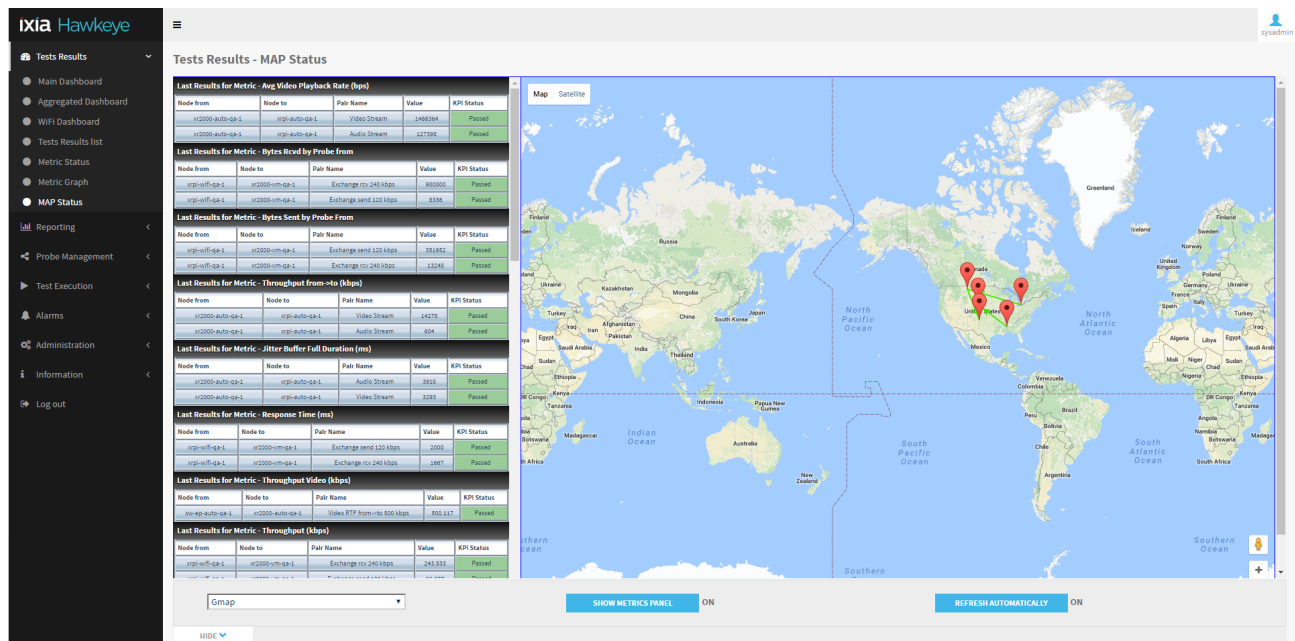
25

entries

☐				2020-12-02 21:55:18	xr2000-tt	xr-vm-tt2	158	SkypeMesh	Skype4B Traffic from->to	<div><div>Delete</div><div>More</div></div>
				2020-12-02 21:55:17	xr2000-tt	xr2000vm-qa-exp1	158	SkypeMesh	Skype4B Traffic from->to	<div>Number Of Pairs... More</div>
				2020-12-02 21:55:16	xr2000vm-qa-exp1	xr-vm-tt2	158	SkypeMesh	Skype4B Traffic from->to	<div>Number Of Pairs... More</div>
				2020-12-02 21:55:15	xr2000vm-qa-exp1	IXPR-TW19290009	158	SkypeMesh	Skype4B Traffic from-to	<div>Number Of Pairs... More</div>
☐				2020-12-02 21:55:14	xr2000vm-qa-exp1	xr2000-tt	158	SkypeMesh	Skype4B Traffic from->to	<div>Number Of Pairs... More</div>
☐				2020-12-02 21:54:10	xr-vm-tt2	upload_1	25		DropBox Download	<div>DropBox File... More</div>
☐				2020-12-02 21:52:54	xr-vm-tt2	www.espn.com	121		ICMP Test	<div>Destination... More</div> <div>Threshold failed... More</div>
☐				2020-12-02 21:52:27	xr-vm-tt2	upload_2	26		DropBox Upload	<div>DropBox File... More</div>

Map Status

The **Map Status** feature in Hawkeye allows you to see the status of endpoints on a global map. This allows you to see in real time the status of the endpoints. The map is updated based on test results. If endpoints are running tests successfully, the line between endpoints is displayed in green, but if tests start experiencing errors, the line between the probes are displayed in red.



Hawkeye Reports

The following table shows the descriptions of the Hawkeye reports:

Report Name	Description	Options
-------------	-------------	---------

Metrics summary	Based on selected filters, displays the global results and per metric pass/fail statistics.	<ul style="list-style-type: none"> Selected metrics
Metrics trend	Based on selected filters, displays the global results and per metric pass/fail statistics and adds a trend report per selected metric.	<ul style="list-style-type: none"> Selected metrics Display line type
Last 3 period dashboard	From current date, Last 3 period based on time selection (last hour, last day, etc.) dashboard, on filtered criteria. Contains Pie chart on PASS/FAIL/ERROR and statistics on metrics.	<ul style="list-style-type: none"> Selected metrics
Top N dashboard	Ranking of worst 10 results per metric, based on selected criteria.	<ul style="list-style-type: none"> Selected metrics, N value
Per path Matrix Status	Results are presented into color codes with matrix for meshes. This is a simpler more visual way to display the results than per path metric matrix report.	<ul style="list-style-type: none"> Selected metrics
Paths Error/Fail Summary	This report displays the number of errors reported and numbers of failures reported with % of total tests.	<ul style="list-style-type: none"> Selected metrics (not considered)
Paths Error/Fail Summary per KPI	This report displays the number of failures reported with % of total tests per KPI and sort them based on maximum rates failing.	<ul style="list-style-type: none"> Selected metrics
Per path summary	Does a KPI summary report per path in selection.	<ul style="list-style-type: none"> Selected metrics
Per path trend	Does a KPI trend report per path in selection.	<ul style="list-style-type: none"> Selected metrics Display line type
Site report summary	Per site KPI report.	<ul style="list-style-type: none"> Selected metrics.
Site report trend	Per site trend report.	<ul style="list-style-type: none"> Selected metrics Display line type
Site report detailed	Per site detailed report with per path per site report.	<ul style="list-style-type: none"> Selected metrics Display line type

Executive Summary	Based on selected filters, provides summary of Tests execute and gives Top Worst Probes, Worst Paths, Failed Tests, and Failed Metrics.	<ul style="list-style-type: none"> Selected metrics
-------------------	---	--

Truncated Reports

Running reports over too large selections can create memory allocation issues - therefore there is auto limitation into the report size that can result into displaying truncating report warning:



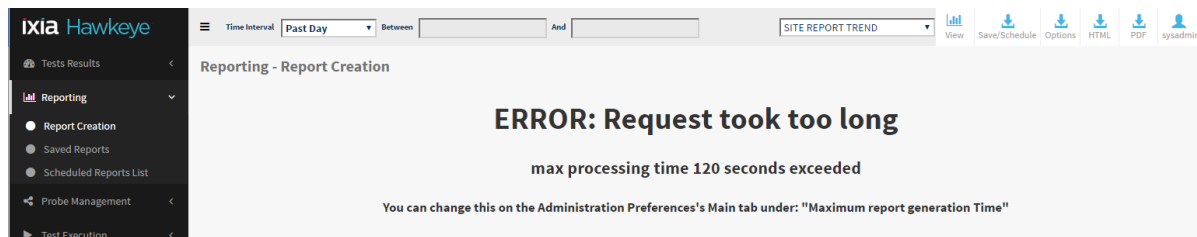
WARNING - TOO MANY PATHS IN QUERY - REPORT TRUNCATED

Report Takes too Long to Create

Reports created for large time periods and test data can take some time to process. You can configure the system processing time for processing a report. This is configured in **Preferences > Main > Maximum report generation Time**.

Administration - Preferences				
Main	Parameter Name	Value	Description	Details (Current Setting)
GUI	Result Access Control Type	0 ▼	Result access display control based on test execution (0) or probe group (1)	Access to results is based on test execution
Alarms	Allow Frequency Unit Configuration	0 ▼	Allows to use frequency unit configuration - in particular allow sub minute frequency	Disable Frequency Unit
Maps	Allow Schedule Enforcing	0 ▼	1 is allowing to change Schedule and disable scheduling optimization.	Schedule CANNOT be changed
Email	Add Port Numbers to Test Results	0 ▼	1 to add port used information in all N2N or Mesh tests	Used port information in tests is NOT ADDED
Traffic Port Management	Display Test Controller Status	1 ▼	1 to Display test controller (or agent) status table in administration table. Only required for system with distributed test controllers	Agent status table is displayed in administration table
Test Controller	Map Report	1 ▼	Enable/Disable map display	Map display is ENABLED
Advanced Options	Maximum report generation Time	120	Maximum report generation time (seconds). Change to allow more time to generate reports	
Installation Paths				

If the Hawkeye server exceeds the max allowed time to create a report the following error message will be generated.



Create a Report

To create a report, select the **Reports** located on the menu bar to open the saved reports page, which lists previously saved reports, and select the **+ Create** button.

Create/Schedule Report

Mesh + Filter

Create Schedule

Report Type: METRIC TRENDS

Metrics: x All

Name:

Display line: Line

Format: HTML PDF

Email:

Save

The report will be created according to the filters defined:

- Time range in time selection. The available time intervals are:
 - Last hour/day/week;
 - Today;
 - Full range;
 - Range: when range is selected the date picker becomes active.

The screenshot shows a date range selection dropdown menu. The menu is open, displaying a list of time-based filters. The 'Past Day' option is currently selected and highlighted in blue. Other options include 'Past 15 Minutes', 'Past Hour', 'Past 3 Hours', 'Past 6 Hours', 'Past 12 Hours', 'Today', 'Past Week', 'This Week', 'Previous Week', 'Past Month', 'This Month', 'Previous Month', and 'Custom Range'. At the bottom of the dropdown are 'Apply' and 'Cancel' buttons. To the right of the dropdown, a 'METRIC TRENDS' section is visible, showing a 'Line' chart type and a '× All' button.

- Filter criteria in the bottom section

The screenshot shows the filter criteria section of the Hawkeye User Interface. It includes a filter icon, a date range dropdown set to 'Past Day', and a 'Mesh' dropdown menu with a '+ Filter' button. At the bottom, there are 'Create' and 'Schedule' buttons.

After the report criteria has been defined, you will need to select the report type and format as well as name your report before you can save it. This is also where you can limit the metrics that are included in the report as well as set to have the finished report sent to you via email by checking the Email box and providing your email address.

To create the report one time you will select the save button and the report will be created in the background and a notification will be provided when completed.

To schedule this report to recur over time you will select the **Schedule** button in the center of the screen and you will be presented with the Frequency (in hours) as well as the Period fields. Selecting

the period field will present you with Calendars to select your start and end dates and adjust your Start and End times.

Create/Schedule Report

Clear Filters | Past Day

Mesh: auto | + Filter

Create | **Schedule**

Report Type: METRICS SUMMARY | Format: HTML | PDF

Metrics: x All

Name: AutoMesh_24hrTrend | Email: ☒ | netopsNC@keysight.com

Frequency: 24 | Period: Dec 07, 2020 @ 00:00 - Dec 07, 2020 @ 15:24

Dec 07, 2020 @ 00:00 | Dec 31, 2020 @ 23:00 | Apply | Cancel

12:00 AM | 11:00 PM

Dec 2020 | Jan 2021

Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5	27	28	29	30	31	1	2
6	7	8	9	10	11	12	3	4	5	6	7	8	9
13	14	15	16	17	18	19	10	11	12	13	14	15	16
20	21	22	23	24	25	26	17	18	19	20	21	22	23
27	28	29	30	31	1	2	24	25	26	27	28	29	30
3	4	5	6	7	8	9	31	1	2	3	4	5	6

After all configuration has been made you can select **Schedule** at the bottom right corner of the screen to schedule your report to run.

Create/Schedule Report

Clear Filters | Past Day

Mesh: auto | + Filter

Create | **Schedule**

Report Type: METRICS SUMMARY | Format: HTML | PDF

Metrics: x All

Name: AutoMesh_24hrTrend | Email: ☒ | netopsNC@keysight.com

Frequency: 24 | Period: Dec 07, 2020 @ 00:00 - Dec 07, 2020 @ 15:24

Dec 07, 2020 @ 00:00 | Dec 07, 2020 @ 15:24

Schedule

View a report

Reports are created in the background in Hawkeye, thus allowing you to set up your report and then get back to work. All while we work in the background to build the report. If you have run a once shot

report when it is ready you will get a notification



in the top bar of the Hawkeye screen. Select the bell and selecting the new notification will include a link to direct download the report.

Notifications Details		
Id	69	
Type	Report generated	
Content	Report Complete_System_Summary_pdf was successfully generated. Download link	
Is Active	yes	
Is Read	yes	
Login	sysadmin	
Created At	2020-12-07 20:47:12	

If you report runs on a schedule you will not get notifications at the top of the screen instead you will select **Reports** in the menu and on the **Saved** page you will see all the completed reports listed.

From here you can select the eye to view or the download  button to start a download of the report. You can also view previously run one shot reports and download them from here as well.

Reports - Saved

Saved
Scheduled

+ Create

Show

entries

ID	Name	Creation Date	Type	Format	Email Sent	Size	Created by
13	Complete_System_trend_email	2020-12-07 20:53:47	Full	html	yes	1469 kB	sysadmin
12	Complete_System_Summary_pdf	2020-12-07 20:47:12	PieOnly	pdf	no	889 kB	sysadmin
11	AutoMesh_24hrTrend	2020-12-07 20:43:49	Full	pdf	no	1022 kB	sysadmin
10	AutoMeshSummary	2020-12-07 20:24:40	PieOnly	pdf	yes	480 kB	sysadmin

Showing 1 to 4 of 4 entries (filtered from 12 total entries)

Previous
1
Next

Removing Scheduled Reports

If you want to stop a scheduled test before the schedule period is over you can do so by selecting **Reports** in the menu and then select the **Scheduled** button. From this screen you can either pause or delete a schedule by selecting the corresponding button on the left side of the row for a scheduled report.

≡ Reports - Scheduled

sysadmin

Saved
Scheduled

+ Create
▼

Show 25 entries

	ID	Name	Type	Format	Email	Status	Frequently (hour)	Next Time	First Time	Last Time	Created by
☐ 🗑️ 📄 14		AutoMesh_24hrTrend	Full	pdf	no	Waiting next execution	24 hour	2020/12/07 19:00:00	2020/12/06 19:00:00	2020/12/31 10:00:00	sysadmin

Showing 1 to 1 of 1 entries

Previous
1
Next

Paths

The **Paths** dashboard shows list of tested network paths with count of passed, failed and error test records. Test records graph shows count of tests ran in a given interval.

To view the results, complete the following steps:

1. Select **Paths** from the left hand menu.

sysadmin

Dashboards - Paths Beta

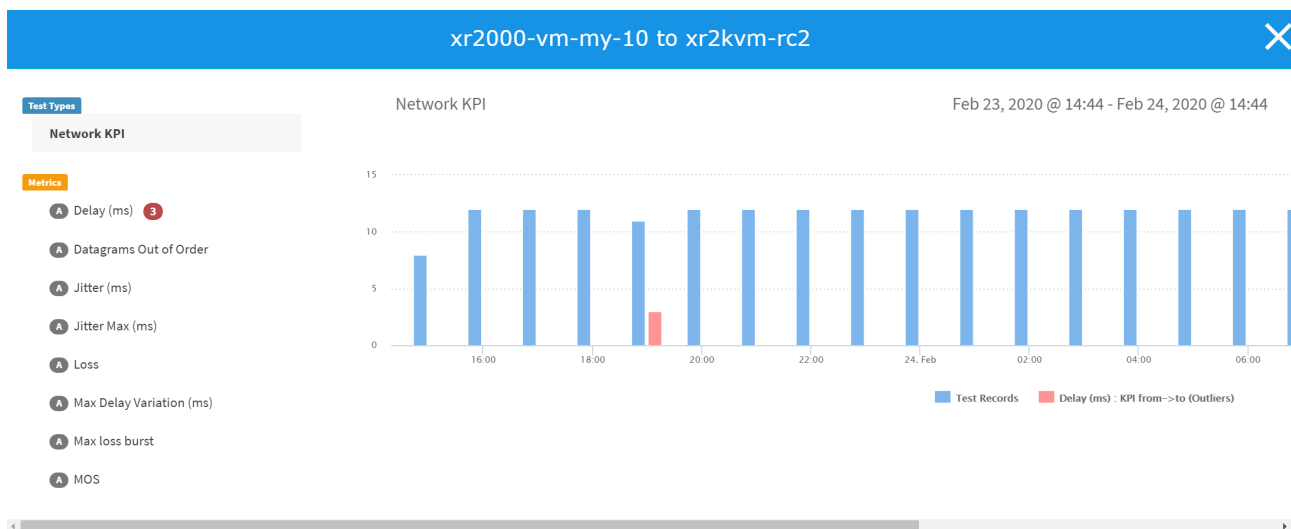
Show 25 entries

Probe From	Probe To/ Destination	Passed	Failed	Error	Actions
xr2kvm-rc1	xr2kvm-rc2	285	2	0	
xr2000-vm-my-10	xr2kvm-rc2	273	13	0	

Showing 1 to 2 of 2 entries

[Previous](#)
[1](#)
[Next](#)

2. Select a specific path row, to view the test records and metric data in a modal.

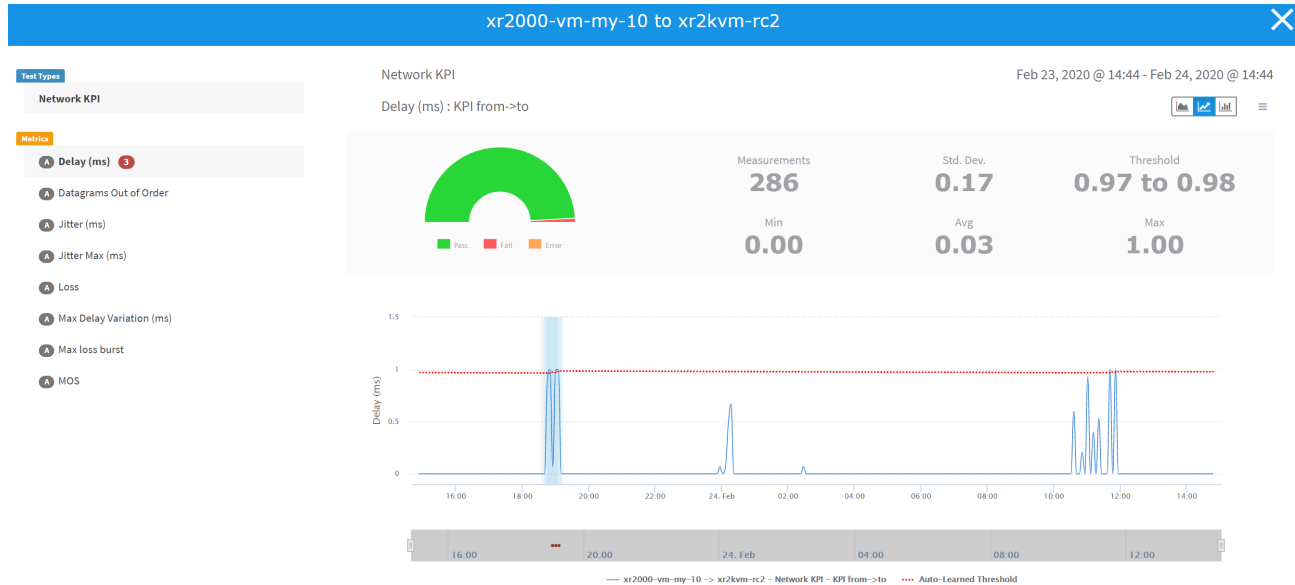


The results per metric provides average, maximum, and minimum values. The results are also notified with:

- standard deviation
- total measurements in samples
- threshold (can be range of threshold)

The graph for each metric show

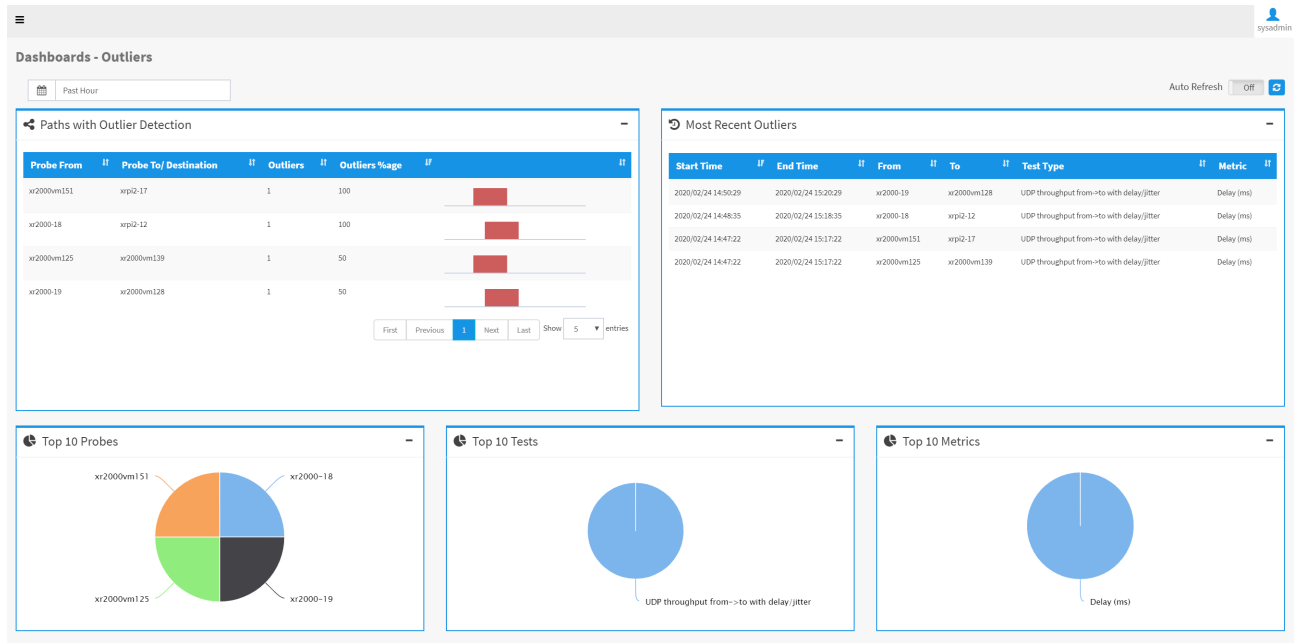
- Time Interval: time interval selected for browsing the data.
- Auto-Learned or Default Threshold displayed as a line
- Outliers displayed as blue plot bands



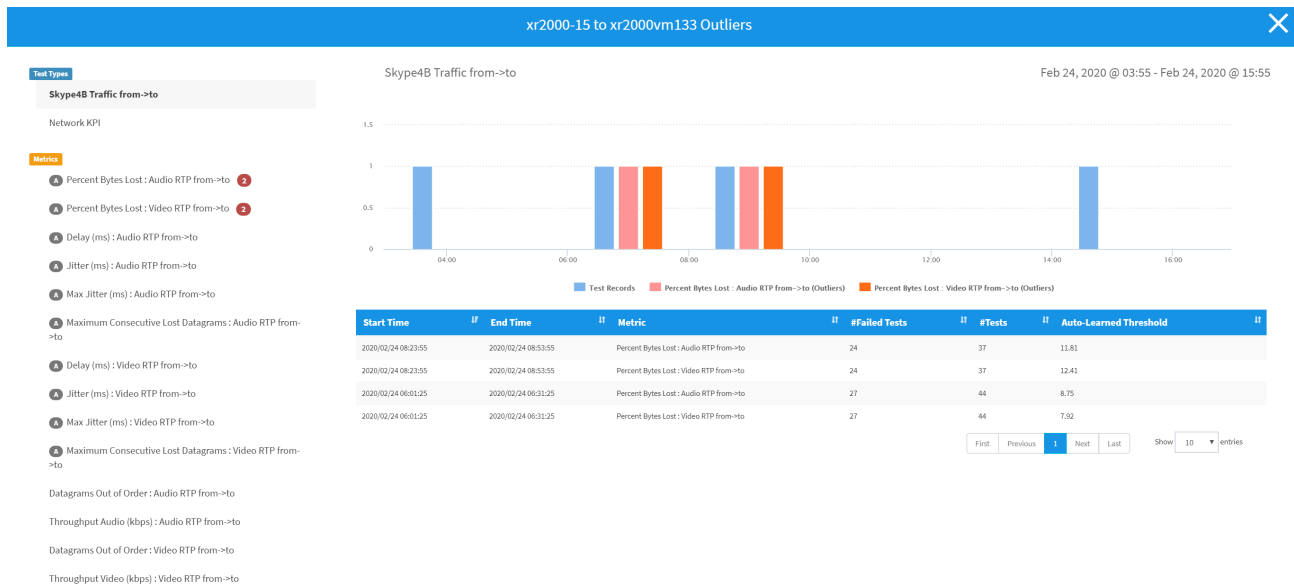
Outlier

To view the outliers of the tested network, complete the following steps:

1. Select **Outliers** from the left hand menu.



2. Select a row under **Paths with Outlier Detection** section to view the outlier details in a modal.



- Test records graph shows count of tests and different outliers triggered in a selected time interval.
- The graph for each metric shows the following:
 - Time interval selected for browsing the data.
 - Auto-learned or default threshold displayed as a line.
 - Outliers displayed as blue plot bands.



CHAPTER 6

Hawkeye Test Types

The scope of this section is to present the different test types available within Hawkeye application. It details the test methodology test types and configuration options, as well as test result KPIs.

In this chapter:

Test type general description	165
Node to Node	165
Understanding Node to Node Metrics	167
What is Goodput?	172
Testing Throughput Using TCP or UDP	172
Node to Node Test Types	173
TCP Throughput Tests	173
UDP Throughput Tests	183
Network KPI tests	191
QOS Qualification Tests	198
Voice and Video Tests	203
Video Stream	205
Unified Communications	215
Real Time Transactional Applications Tests	223
DSCP (QOS) Settings Explained	239
Details on Class of Service - Different Standards	240
Common Errors - N2N	243
Default Number of Tests per Probe Type (N2N)	246
N2N license cost per Test Types	252
Real Services	255
Licensing	256
Continuous	256
Advanced	261
Path Discovery	293
Real Service Endpoint Support Matrix	298
Replicating Tests Across Multiple Endpoints	302
Test Types Reporting Wi-Fi Statistics	302

Supported Protocols and Standards	308
Supported Voice over IP Codecs	311

Test type general description

You must be aware of scheduling tests too frequently for the probe. When scheduling tests the user needs to be aware that the test duration is more than the configured “traffic duration”. The total test duration will include time to setup the test, specifically time taken for the Hawkeye Server sending test configuration commands down to the endpoints, test setup on the endpoints, endpoints calculation of test statistics following test completion, endpoints then sending results back to Hawkeye Server, and the Hawkeye Server finally recording resulting test metrics in the Results database. One way to know how long a test takes is to schedule a test every 10 minutes, then see the timestamp in test results which reflects the start time, plus traffic duration plus processing overhead to get to test metrics stored in the Results database

This section explains the following topics:

[Node to Node below](#)

[Understanding Node to Node Metrics on page 167](#)

[What is Goodput? on page 172](#)

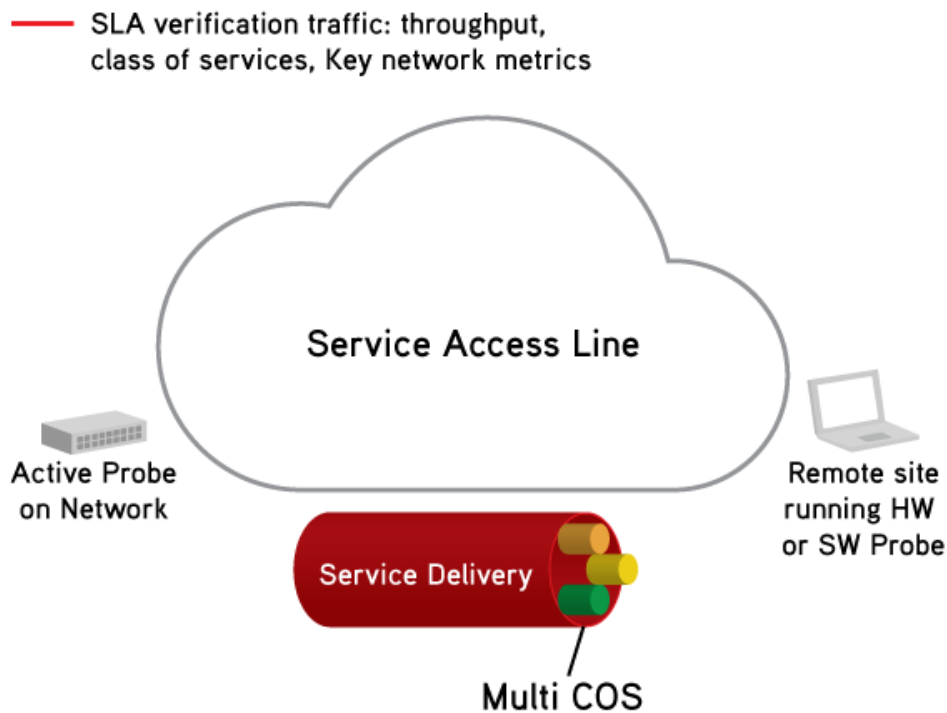
[Testing Throughput Using TCP or UDP on page 172](#)

Node to Node

Node to Node Testing Topology

The Node to Node (N2N) testing is based upon testing between two probes. The active probes are deployed in the network at different key locations and controlled by the Hawkeye test controller.

A typical testing topology is described in the following image:



Hawkeye is controlling tests through a central location. Probes are deployed in the different network locations, and run active traffic between themselves to generate traffic flows.

See description of available tests below.

The probes involved can be:

- XR3000 (up to 2x1GE Auto Media interfaces, +2x10GE SFP+ interfaces, 4x2.5GE copper interfaces, and 1xWifi-6 Interface)+
- XR-E1S (up to 8x1GE copper interfaces and 4x10GE SFP+ interfaces)
- XRVM (Virtual Machine delivered as an OVA or QCOW2)
- IxProbe/ IxTap / IxBypass (2x1G copper interfaces - it can only generate test traffic on single interface)
- Software probe (on laptop or computer (Windows, Linux) and android devices)
- XRPi (one ethernet and optional Wi-Fi interface) - End of Development
- XR2000 probe (up to 6 GE copper interfaces - 2 GE copper interfaces active by default) - End of Development

Node to Node testing allows full control of the tested path, as traffic is generated between nodes. This allows generating predictive traffic to receiving side, generate bidirectional traffic, and setup several classes of services with full control of the traffic sent.

Hawkeye is delivered with a default test type base.

Understanding Node to Node Metrics

The Test Totals are divided into three major sections that correspond to the three basic types of measurements taken in an Hawkeye test. Following are explanations of how Hawkeye calculates throughput, transaction rate, and response time.

Throughput

Hawkeye measures the throughput associated with packet payload, ignoring headers. This is referred to as Goodput in RFC 2647.

The throughput is calculated for pairs with the following equation:

$$\text{Bytes Received (by E2)} / (\text{Throughput_Units}) / \text{Measured time}$$

For pairs that are bidirectional (TCP based application type of traffic), throughput is aggregated in two directions:

$$(\text{Bytes_Sent} + \text{Bytes_Received_By_Endpoint_1}) / (\text{Throughput_Units}) / \text{Measured_Time}$$

In all calculations, elapsed time is the elapsed time of the longest-running pair in the test. The measured time is the sum, in seconds, of all the timing record durations returned for the endpoint pair.

Here's how each of the script variables is defined:

- Bytes_Sent: the number of bytes sent by Endpoint 1 of a pair.
- Bytes_Received: the number of bytes received by the endpoint of a pair.
- Throughput_Units: the current throughput units value, in bytes per second. For example, if the throughput units are KBps, 1024 is the Throughput_Units value. In this example, the throughput units number is shown in the column heading as Mbps, which is 125,000 bytes per second (that is, 1,000,000 bits divided by 8 bits per byte). See Raw Data Totals.

Transaction Rate

The calculations are shown in transactions per second. This rate is calculated as follows:

$$\text{Transaction_Count} / \text{Measured_Time}$$

Response Time

The response time is the inverse of the transaction rate. The calculations are shown in seconds per transaction. This value is calculated as follows:

$$\text{Measured_Time} / \text{Transaction_Count}$$

Lost Data

The lost data is the difference between the number of bytes sent by Endpoint 1 and the number of bytes Endpoint 2 actually received. Lost data is only calculated when a pair is running a streaming script (for example, in a VoIP or video). Only payload data is included in the calculations.

Max Loss burst

Maximum number of packets lost in a row during test.

Jitter

Hawkeye helps you determine the quality of a multimedia transmission or voice over IP call using measurements of jitter. RFC 1889 jitter (calculated for all RTP pairs) shows mean statistical deviance of packet inter-arrival times over a period of time.

The jitter (delay variation) maximum reveals when the greatest variation in delay seen for a timing record occurred during the test.

When a datagram is sent, the sender gives it a timestamp. When it is received, the receiver adds another timestamp. These two timestamps are used to calculate the datagram's transit time. If the transit times for datagrams within the same test are different, the test contains jitter. In a video application, it manifests itself as a flickering image, while in a telephone call, its effect may be similar to the effect of packet loss; some words may be missing or garbled.

The amount of jitter in a test depends on the degree of difference between the datagrams' transit times. If the transit time for all datagrams is the same (no matter how long it took for the datagrams to arrive), the test contains no jitter. If the transit times differ slightly, the test contains some jitter. Jitter values in excess of 50 ms probably indicate poor call quality.

Jitter statistics let you see a short-term measurement of network congestion and can also show the effects of queuing within the network. The jitter value is reset for each timing record, so the jitter statistic for a specific timing record shows the jitter for that timing record only.

Almost all data transfers experience jitter, but it is not necessarily a problem. Jitter occurs in several patterns. If the delay time for each datagram steadily increases, jitter values increase and the throughput decreases. But it is also possible for jitter to increase while throughput remains constant. In this case, the delay variation fluctuates widely, which could mean poor performance for delay-sensitive applications. Finally, "bursty" jitter—occurring in bursts of datagrams—has the most significant effect on call quality in voice over IP transmissions. If jitter occurs in bursts, it can lead to data loss and a degradation of call clarity. Hawkeye measures this "bursty" quality; refer to Max loss burst.

RFC 1889 Jitter

When calculated according to the specification for RTP, jitter (J) is defined as the mean deviation (smoothed absolute value) of the difference (D) in datagram spacing at the receiver compared to the sender for a pair of datagrams. As shown below, this is equivalent to the difference in the "relative transit time" for the two datagrams; the relative transit time is the difference between a datagram's RTP timestamp and the receiver's clock at the time of arrival, measured in the same units. If S_i is the RTP timestamp from datagram I, and R_i is the time of arrival in RTP timestamp units for Datagram I, then for two datagrams (I and j), D may be expressed as follows:

$$D(i,j)=(R_j-R_i)-(S_j-S_i)=(R_j-S_j)-(R_i-S_i)$$

The inter-arrival jitter is the jitter calculated continuously as each datagram (I) is received from the source. The jitter is calculated according to the formula defined in RFC 1889:

$$J=J+(\frac{3}{4}D(I-1,I)-J)/16$$

Jitter is measured in timestamp units and is expressed as an unsigned integer. Whenever the endpoint creates a timing record, the current value of J is sampled.

Delay

Endpoints can calculate delay statistics in a single direction for VoIP pairs and for pairs using the RTP protocol. Delay is calculated for each timing record in a test. These measurements are useful in testing time-sensitive applications because they can help to pinpoint sources of delay. One-way or network delay excludes sources of delay apart from the "wire" itself, while end-to-end delay includes all sources of delay, such as the codec used, jitter buffers, and fixed delays.

MOS

Treating each endpoint/probe pair as a separate voice over IP "call," Hawkeye gives an indication of the relative quality of each call made during a test on your network. Ixia uses a modified version of the ITU G.107 standard E-Model equation to calculate a Mean Opinion Score (MOS) estimate for each endpoint pair.

The E-Model, developed by the European Telecommunications Standards Institute (ETSI), has become ITU standard G.107. This algorithm is meant to evaluate the quality of a transmission by factoring in the "mouth-to-ear" characteristics of a speech path. It calculates an R-value, which correlates directly with the MOS estimate.

Hawkeye modifies the E-model slightly and uses the following factors to calculate the R-value and the MOS estimate:

- One-Way (Network) Delay
Similar to the propagation delay; only the delay factors associated with the network (the "wire") itself are included. Hawkeye measures this by synchronizing the endpoints' timers and determining delay in a single direction. Refer to One-Way Delay for more information.
- End-to-End Delay
Latency as measured by adding the following factors:

Delay Type	How Calculated
One-way (network) delay	Datagram's RTP timestamp subtracted from time it was received by Endpoint 2. See above.
Packetization delay	Fixed; dependent on codec selected.
Jitter buffer delay	Fixed; dependent on type and size of jitter buffer configured by user
Additional fixed delay	Fixed; user-configured

- **Data Loss**

Total number of datagrams lost. When a datagram is lost, you can lose an entire syllable, and the more datagrams that are lost consecutively, the more the clarity suffers. Hawkeye factors in lost data and also includes the amount of consecutive datagram loss that was measured. Refer to The Lost Data Tab for more information. In addition, if you have packet loss concealment (PLC) enabled for the G.711 codecs, a delay factor associated with PLC buffering is added. Refer to Codec Types for information about PLC.

- **Jitter Buffer Lost Datagrams**

Number of datagrams lost due to jitter buffer overruns and underruns. Refer to Jitter Buffers for more information.

A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The following table (taken from ITU G.107) summarizes the relationship between the MOS and user satisfaction:

Mean Opinion Scores (MOS) table

Mean Opinion Score (lower limit)	User Satisfaction
4.34	Very satisfied
4.03	Satisfied
3.60	Some users dissatisfied
3.10	Many users dissatisfied
2.58	Nearly all users dissatisfied

Media Delivery Index (MDI) Calculation

The Media Delivery Index (MDI) is a proposed metric, defined in RFC 4445, that can be used as a diagnostic tool or a quality indicator for monitoring the delivery of streaming media on a network. It specifically focuses on the measurement of packet jitter and packet loss in networks carrying streaming media, such as MPEG video, Voice over IP, and other information that is sensitive to arrival time and media loss. Hawkeye collects and reports MDI statistics for all Video Pairs.

The two major factors impacting the quality of a video stream transmitted over an IP network are packet loss and packet jitter. Packet loss can be caused by many factors, including data corruption, insufficient bandwidth, and out-of-order packet delivery. Any packet loss will adversely affect the quality of the delivered video. Packet jitter causes buffer overflows and underflows, either of which will cause unacceptable time distortions in the video streams.

Packet Jitter

Packet jitter is a measure of the variation in arrival rates between individual packets in a media stream. Streaming media requires a consistent and predictable time delay between successive packets as they are received at a destination node. Variations in this interpacket delay causes packet jitter. If packets are delayed by the network, some packets will arrive in bursts with diminished

interpacket delays while other packets will arrive with longer interpacket delays. Therefore, the node at the receiving end (the decoder) must buffer the video data to ensure that it can be displayed at its nominal rate. The size of the buffer determines the maximum amount of packet jitter than can be accommodated without experiencing buffer underrun or overrun.

Delay Factor

The MDI consists of two components: the Delay Factor (DF) and the Media Loss Rate (MLR).

The Delay Factor (DF) indicates the maximum difference between the arrival of streaming data and the drain of that data, as measured at the end of each media stream packet. The drain rate refers to the payload media rate. For example, for a typical 3.75 Mbps MPEG video stream, the drain rate is 3.75 Mbps—the rate at which the payload is displayed at a decoding node. The DF is computed at the time that each packet arrives at the Hawkeye endpoint, and is recorded for each timing record. The default timing record duration is three seconds.

The DF is computed at the arrival time of each packet at the point of measurement. For Hawkeye, the point of measurement is Endpoint 2. It is recorded at set time intervals, typically about one second. For Hawkeye, it is measured when each timing record is generated.

If X is a virtual buffer where DF is measured,

$$X = |\text{Bytes Received} - \text{Bytes Drained}|$$

Then, DF is calculated as follows:

$$\text{DF} = [\max(X) - \min(X)] / \text{media rate}$$

where media rate is expressed in bytes per second and $\max(X)$ and $\min(X)$ are the maximum and minimum values measured in an interval.

The largest difference is recorded for all intervals in a measurement period. That is, DF is the maximum observed value of the flow rate imbalance over the calculated interval.

Media Loss Rate

The second component in the MDI is the Media Loss Rate (MLR).

The MLR is the count of lost or out-of-order packets, measured over a selected time interval (such as three seconds). That is,

$$\text{MLR} = (\text{Packets Expected} - \text{Packets Received}) / \text{Interval}$$

There may be zero or more streaming packets in a single IP packet. For example, it is common to carry seven 188 byte MPEG Transport Stream packets in an IP packet. In such a case, loss of a single IP packet would result in seven lost MPEG Transport Stream packets. Counting out-of-order packets is important because many streaming media applications do not attempt to reorder packets that are received out of order.

Media Delivery Index

The Media Delivery Index (MDI) combines the Delay Factor (DF) and the Media Loss Rate (MLR) values for presentation, and is expressed as:

$$\text{DF:MLR}$$

The DF provides an indication of the size of the buffer needed to accommodate the packet jitter in the network. The MLR gives an indication of the extent of media loss as the streaming media traverses the network.

What is Goodput?

In computer networks, goodput is the application level throughput, i.e. the number of useful information bits delivered by the network to a certain destination per unit of time. The amount of data considered excludes protocol overhead bits as well as retransmitted data packets. This is related to the amount of time from the first bit of the first packet sent (or delivered) until the last bit of the last packet is delivered, see below.

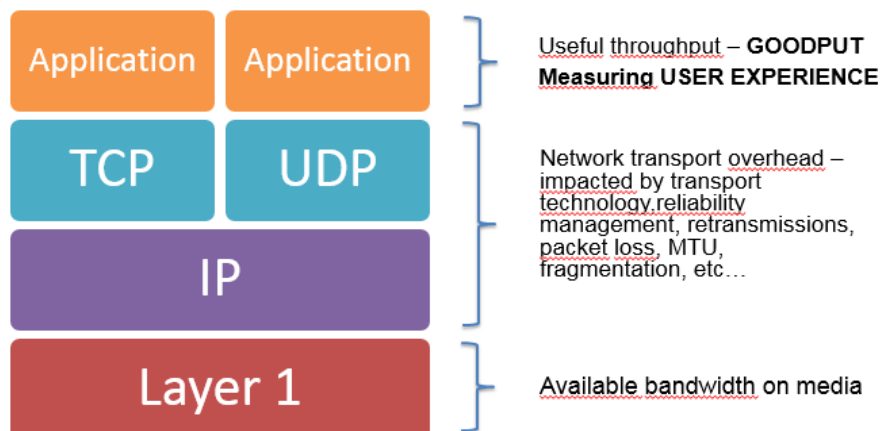
For example, if a file is transferred, the goodput that the user experiences corresponds to the file size in bits divided by the file transfer time. The goodput is always lower than the throughput (the gross bit rate that is transferred physically), which generally is lower than network access connection speed (the channel capacity or bandwidth).

Examples of factors that cause lower goodput than throughput are:

Protocol overhead; typically, transport layer, network layer and sometimes datalink layer protocol overhead is included in the throughput, but is excluded from the goodput.

Transport layer flow control and congestion avoidance, for example TCP slow start, may cause a lower goodput than the maximum throughput.

Retransmission of lost or corrupt packets due to transport layer automatic repeat request (ARQ), caused by bit errors or packet dropping in congested switches and routers, is included in the data link layer or network layer throughput but not in the goodput.



Testing Throughput Using TCP or UDP

Differences Explained

TCP	UDP
TCP stack adapts to available bandwidth.	UDP sends packets on best effort – sender is « bit blaster ».
TCP stack implementation and configuration	UDP stack is minimal (packets building).

has important impact.	
TCP traffic is bidirectional : one way sends traffic, other way acknowledges.	UDP is unidirectional – no acknowledgments from receiver.
High sensitivity to packet losses and network delay: Delay will impact acknowledgement speed – loss result in retransmissions resulting in exponential throughput degradation.	Not sensitive to network delay. Loss packets will result in linear degradation of throughput.
TCP is throughput QoE: that is what user experience.	UDP is throughput QoS : this is what network can deliver.

When to Use TCP

- Qualifying user experience.
- Validate available traffic on a network with live network active – no risk of congestion as TCP traffic will auto adapt to available bandwidth.
- Compare against typical FTP based measurements or Speedtest behaviors.
- Qualify impact of TCP stack configuration (window size, buffers, Operating system etc.

When to Use UDP

- Qualifying available bandwidth : stress line with datagrams traffic (RFC 2544).
- Validate transport in both directions at same time.
- Validate unused line – UDP traffic can cause network congestions affecting real users traffic.

Combination of TCP and UDP

A test called COS qualification offers pairs with TCP and pairs with UDP (RTP) and is designed to test different classes of services :

- data class of services are tested with TCP.
- voice/real traffic class of service is tested with RTP/UDP.

Node to Node Test Types

This section discusses the Node to Node test types.

TCP Throughput Tests

What is my target measuring TCP performance?

This is one very important question that needs to be well addressed before going through advanced TCP performance test.

TCP is the most widely used protocol for applications transiting over the Internet. Given all factors influencing its performance, it is very important to make sure of what one is trying to prove by doing TCP performance testing.

Test typical application behavior

Use the scripts called TCP Throughput. These scripts send large chunks of bytes from Endpoint 1 to Endpoint 2, then waits for an acknowledgment.

It thus simulates the core file transfer transaction performed by many applications.

TCP auto adapts to available bandwidth therefore will be a good indicator of the data available for an application.

Network transmission capability verification -> Use UDP

If one is after defining pure network transmission capability, TCP is likely not the best solution to prove the network. It will be a lot more efficient to use UDP tests which act more as bit blasters and would report transparently any unidirectional data loss. UDP is not connection oriented and therefore a lot more adequate when testing line transmissions.

When looking at network transmission capability, Ixia performance endpoint is able to run UDP tests that are a lot more precise to report on line capacity transmission capability and packet loss.

UDP traffic generation is however dangerous as it will not adapt to available bandwidth and therefore is likely to create router congestions and affect other traffic.

Make sure you use the right Operating System

One key factor is the TCP stack used by the performance endpoint in the test. The most common OS stacks, Linux and Windows, have different behaviors and therefore can behave with different performance on same environment. It is important to understand that Ixia performance endpoint is using the underlying OS stack and therefore the performance of the stack is part of the performance test itself.

Ixia performance endpoints come with most common OS and OS versions, allowing to control what version can be used.

It is also very important to understand the stack parameters on the OS can have a big impact on the results.

Define what the target performance is: what are you looking as a good result?

Depending on the characteristics of the line you are trying to test, it is important to define a target maximum throughput that is proving a good result for a single TCP stream.

This will help defining how the performance endpoint has to be used to use the stack.

For example, it is likely that a FTP server on a 1G local LAN can be expected to reach 500M throughput or more, but if 1G line is used between 2 different remote sites with long delays, is this 500M throughput still be a valid target?

Am I looking to prove a specific application?

All applications are specific in the way they would use the TCP stack: it cannot be expected that small volume transactions to a mail server would behave the same way as long download from FTP servers.

Hawkeye script libraries provide a very wide range of common applications that can be complemented by specific built applications to help understand the behavior over a specific network.

It is also important then to compare how a standard TCP throughput test compares to a specific application test over TCP. Hawkeye allows running both aspects and understanding what could explain the difference in expected performance.

Do I want to use default OS settings or tune them for the TCP stack?

Most real applications that use a TCP stack use default parameters. However, the most common Operating Systems (Windows and Linux) allow controlling the way the TCP stack is used through socket APIs. It does not allow controlling how the stack is going to behave and auto adjust its window based on the environment, but will allow to control the memory buffers for send and receive to optimize the use of the stack.

These parameters are very important if one's target is to understand the best possible TCP performance a stream can get. As changing these parameters can influence greatly on the stack optimization, there will be some performance impact by tuning these parameters.

Ixia performance endpoint has implemented these parameters. A typical test is to run a "default settings" TCP test to see what the default stack is capable of, and then adjust these parameters based on what is known of the environment (typically the RTT) to find out what is the maximum achievable performance.

IMPORTANT

WARNING: If you leave OS parameters by default then when you set Hawkeye manually force OS to use some buffers sizes it can happen that the values to are pushing are over the limits configured on the OS and so are not taken into account.

Do I need one or several TCP streams?

If one is testing a link for TCP performance, it is important to know if one single TCP stream is the best approach. Typically, links would transport in real life several streams in parallel. These streams would all correspond to different applications or even to same applications using different channels.

Therefore, if link capacity for TCP is the target, it is often more efficient to test several TCP streams in parallel, which would usually result in better aggregated performance than a single TCP stream.

One important point: speed measurements free tools that are available on the Internet usually use several concurrent TCP streams to assess line capacities.

IMPORTANT

Each Stream is limited to a maximum rate of 4.19Gbps. To test rates higher than 4.19Gbps, please use one of the N Stream Tests.

TCP Throughput Tests Descriptions

	TCP throughput from->to 1 stream
Description	One TCP stream - generates throughput with defined bit rate - from E1 to E2.
Purpose	Verify that a single TCP stream in one direction is going through.
Available Options	Generated Bitrate (layer 4 bit rate) that is pushed by sender (node from). DSCP setting (QOS).
Metrics	Average Throughput (Mbps) from->to.
Advanced Information	This test will optimize use of TCP throughput pair from E1 to E2 based on requested throughput. Test samples will be computed according to the requested bit rate so that there should be approximately one measurement per second.

	TCP throughput from->to 1 stream
Results interpretation	The result in throughput is displayed at layer 4 level (with ethernet, IP and TCP headers, and includes potential retransmissions). TCP result in one pair is very sensitive to delay or packet loss. Some result can show important discrepancy between expected line rate and result due to TCP protocol high dependency on line characteristic. It is recommended to complement this test with UDP or TCP multistream test for further pipe capacity assessment.
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected, check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	TCP throughput from->to N streams
Description	Multiple TCP stream - generates throughput with defined bit rate in multiple streams from E1 to E2.
Purpose	Verify that a mutipleTCP stream in one direction is going through. If several streams are configured (>5 typically) that provides a good assessment of the pipe capability as it makes each TCP stream less sensitive to delay and loss.
Available Options	Generated Bitrate (layer 4 bit rate) that is pushed by sender (node from). DSCP setting (QOS).
Metrics	Average Throughput (Mbps) from->to.
Advanced Information	This test will optimize use of TCP throughput pair from E1 to E2 based on requested throughput and shared between requested number of TCP pairs. The total throughput requested will be equally distributed by number of pairs. The timing record per pair will be optimized to be one timing record per second.
Results interpretation	Throughput information is layer 4 level. This test load shares throughput between different streams. This allows better repartition and management of TCP window to prevent high sensitivity to packet loss or low window sizes (therefore TCP retransmission). This test is recommended way to do capacity testing of lines with TCP. The recommended amount of TCP streams is between 5 and 10. The result is only displayed with aggregated results. Detailed report per second can be sometimes misleading as the average throughput per second is dependent on simultaneously aggregating information from the different streams and sometimes can show strange

	TCP throughput from->to N streams
	behavior.
Potential Errors	<p>If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected, check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.</p> <p>If the number of pairs is greater than available max number of pairs per license the test can be stuck in queue.</p> <p>The maximum number of simultaneous pairs (N value) each individual test can perform is also controlled by a parameter in the System Preferences > Max Concurrent Tests in GUI.</p>

	TCP throughput to->from 1 stream
Description	One TCP stream - generates throughput with defined packet size and bit rate - from E2 to E1.
Purpose	See TCP throughput from-> to 1 stream.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

	TCP throughput to->from N streams
Description	Multiple TCP stream - generates throughput with defined packet size and bit rate in multiple streams from E2 to E1.

	TCP throughput to->from N streams
Purpose	See TCP throughput from->to N streams.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

	TCP throughput bidirectional
Description	Bidirectional TCP throughput -with defined bitrate. The TCP throughput is generated concurrently.
Purpose	Verify that a mutiple TCP stream in two directions is going through. There is one stream per direction. Note this test is unlikely to fully assess the total bitrate available on either direction as some bandwidth will be reserved for acknowledgments (see below). Therefore this test shall be reserved to validate how much bidirectional streams can achieve based on TCP protocols.
Available Options	Generated Bitrate (layer 4 bit rate) that is pushed by sender (node from). Average Throughput from->to - Generated Bitrate to->from. DSCP setting (QOS).
Metrics	Average Throughput (Mbps) from->to and to->from.
Advanced Information	This test combines TCP stream from E1 to E2 and from E2 to E1. The timing record per pair will be optimized to be one timing record per second.
Results interpretation	Throughput information is layer 4 level. The TCP protocol works with send window management between sender and receiver. Therefore some packets (useful data) are sent from sender to receiver, and small acknowledgement packets are sent from receiver to sender. As a result, part of the bandwidth on both ways will be busy with small packets for acknowledgment. This will impact line capacity results if the max expected capacity is tested. Therefore, Ixia recommends to use this test for validating below expected capacity throughput availability and perform consecutive one way testing using TCP one direction tests.
Potential	see TCP throughput from->to 1 stream.

	TCP throughput bidirectional
Errors	Note that one direction can pass test while the other errors out.

	TCP throughput advanced
Description	One TCP stream - generates throughput with defined bit rate - from E1 to E2) with advanced configurable settings.
Purpose	Verify that a mutipleTCP stream in one direction is going through. If several streams are configured (>5 typically) that provides a good assessment of the pipe capability as it makes each TCP stream less sensitive to delay and loss.
Available Options	<ul style="list-style-type: none"> • Generated bitrate; • TCP send buffer size; • file size for timing record; • sockets size; • DSCP setting; • source/destination ports. <div style="background-color: #cccccc; padding: 5px; display: inline-block; margin-top: 10px;">NOTE</div> User must define bitrate, source, and destination ports. All other values will be default unless changed by User.
Metrics	Average Throughput (Mbps) from->to.
Advanced Information	This test allows full control of the TCP stream. It requires advanced understanding of the TCP architecture and testing engine.
Results interpretation	<p>Throughput information is layer 4 level.</p> <p>This test will allow to fine tune the TCP stack according to some settings that are dedicated to the test; See Annex for complete TCP stack configuration documentation.</p> <p>Recommended value is filesize to be around 1 second of data transfer at expected throughput so in that case (factor 8 to take into account the bytes to bit ratio):</p> $\text{filesize} = \text{throughput (Mbps)} * 1000 / 8$
Potential Errors	See TCP throughput from->to 1 stream.

	TCP optimized window size from->to
Description	One TCP stream - generates throughput with defined bit rate - from E1 to E2) with advanced configurable settings.

	TCP optimized window size from->to
Purpose	TCP throughput between E1 and E2. Optimized Windows size will be calculated according to delay, throughput and probe type.
Available Options	<ul style="list-style-type: none"> • Generated Bitrate • Expected one way delay on path • FileSize • DSCP setting
Metrics	Average Throughput (Mbps) from->to.
Advanced Information	<p>This test will allow optimization of the TCP window size according to the value the user entered for one way delay expected on the path and the file size. The calculations are performed for a single TCP stream. The test will maximize the TCP throughput through the use of a calculated window size. This calculated window size uses a TCP stack calculation provided by the OS (XR endpoints would be Linux) to maximize TCP throughput provided because of the test. The file size and one way delay are two key parameters used to calculate the TCP receive window. The TCP receive window size will impact total throughput. Other values such as network delay jitter are also considered to adjust the window size. The receive TCP window size impacts flow control by adjusting the frequency of ACKs. The size of the window determines the number of bytes that will be transmitted without an Ack. Note, the TCP process at each end of the connection can dynamically adjust the sliding window to avoid network congestion, A larger sliding window enables higher throughput.</p> <div> <div>NOTE</div> <div>XRPI and XR2000 support RFC1323 (TCP window scaling) by default which increases the TCP window size to use more than 64Mbps. However not all software endpoints may support RFC1323.</div> </div> <div> <div>NOTE</div> <div>Maximize total throughput a large file size and small network delay are required.</div> </div>
Results interpretation	<p>The filesize needs to be calculated according to expected delay. Filesize corresponds to each timing record information transfer. If file size is too important then there will too less (or known) timing record. If it is too small there will be too many timing records potentially impacting the efficiency of the test.</p> <p>Recommended value is filesize to be around 1 second of data transfer at expected throughput so in that case (factor 8 to take into account the bytes to bit ratio):</p> $\text{filesize} = \text{throughput (Mbps)} * 1000 / 8$
Potential Errors	See TCP throughput from->to 1 stream.

TCP throughput tests performance

TCP throughput tests are typically dependent on the underlying stack, overall capability (cpu, network card) of the active endpoint.

For powerful enough devices (xr2000, servers, high range laptops), it should be possible to generate up to line rate TCP streams (resulting in a goodput calculation of 960 to 970 Mbps depending on the transport layer.)

Less powerful endpoints will typically provide less capability that can be measured on case by case.

As long delays can influence dramatically TCP throughput calculations it is recommended to verify the maximum throughput capable with new devices by running end to end scripts.

Optimizing Ixia performance Endpoint for Performance Testing

Ixia performance endpoint Stack utilization parameters

The first item is the way the endpoint will be using the TCP script itself.

In tcp advanced test setup:

```
SEND
size = file_size (1000000)
buffer = send_buffer_size (65535)
rate = send_data_rate (to be filled up)
```

The parameters used are:

- Filesize:** how much data is sent, and then wait for acknowledgement. Increasing it will result into getting more data sent at once to the stack, and increase the length of the timing record (how long between each performance record).
 Recommendation for TCP performance testing is to target 1 timing record per second, so make sure based on expected throughput it takes at least 1 second to download filesize. Using up to 2 or even 5 seconds sometimes help getting the best performance.
- Send and Receive buffer size:** determine how much data will be sent to the TCP stack for processing for each SEND and RECEIVE operation. They are unrelated to TCP sliding window service.
 Recommendation for endpoint send and received buffer size for performance endpoint is to make sure they are not too small, so that they are not too many cycles. They should also not be in excess to the CONNECTION send and receive buffers (see below) that are used to configure the TCP stack. Typical recommended value is 16kbytes, 32kbytes or 64kbytes. Unless misconfigured, this should not have a great impact on TCP performance.
- Send data Rate:** determine the maximum data rate the Performance endpoint will try to push sending through the stack. It can be set to unlimited (in which case the data will be used at maximum rate) or any value in KB.
 Recommendation for endpoint send data rate is to use unlimited when trying to perform as much as possible. However, a side effect using unlimited value is that the stack will be used at maximum but can be overloaded by performance endpoint throwing data in bursts or spikes. When targeting a defined maximum throughput, it is a good idea to use the defined throughput

so that the TCP stack is used in a more even or stable way, and therefore it is stabilized. When pushing the stack and/or network to the limit, it is always better to do some binary search with send data rate to define the most stable value given network conditions and endpoint send and receive OS performance.

Operating System TCP Stack settings

A prerequisite to any further tuning in Ixia Performance Endpoint is to have the TCP stack parameters in the OS itself.

Find below optimization elements for the 2 main Operating Systems (Windows and Linux).

Linux Operating systems

The default values are found with TCP allocated memory:

```
$ cat /proc/sys/net/ipv4/tcp_mem
```

The default and maximum amount for the receive socket memory:

```
$ cat /proc/sys/net/core/rmem_default
$ cat /proc/sys/net/core/rmem_max
```

The default and maximum amount for the send socket memory:

```
$ cat /proc/sys/net/core/wmem_default
$ cat /proc/sys/net/core/wmem_max
```

The maximum amount of option memory buffers:

```
$ cat /proc/sys/net/core/optmem_max
```

Recommended changes:

Set the max OS send buffer size (wmem) and receive buffer size (rmem) to 16 MB for queues on all protocols. In other words set the amount of memory that is allocated for each TCP socket when it is opened or created while transferring files.

CAUTION: The default value of rmem_max and wmem_max is about 128 KB in most Linux distributions, which may be enough for a low-latency general purpose network environment or for apps such as DNS / Web server. However, if the latency is large, the default size might be too small. Please note that the following settings going to increase memory usage on your server

```
# echo 'net.core.wmem_max=16777216' >> /etc/sysctl.conf
# echo 'net.core.rmem_max=16777216' >> /etc/sysctl.conf
```

Set minimum size, initial size, and maximum size in bytes:

```
# echo 'net.ipv4.tcp_rmem= 10240 87380 16777216 ' >> /etc/sysctl.conf
# echo 'net.ipv4.tcp_wmem= 10240 87380 16777216 ' >> /etc/sysctl.conf
```

Turn on window scaling which can be an option to enlarge the transfer window:

```
# echo 'net.ipv4.tcp_window_scaling = 1' >> /etc/sysctl.conf
```

Enable TCP timestamps as defined in RFC1323:

```
# echo 'net.ipv4.tcp_timestamps = 1' >> /etc/sysctl.conf
```

Enable select acknowledgments:

```
# echo 'net.ipv4.tcp_sack = 1' >> /etc/sysctl.conf
```

By default, TCP saves various connection metrics in the route cache when the connection closes, so that connections established in the near future can use these to set initial conditions. Usually, this increases overall performance, but may sometimes cause performance degradation. If set, TCP will not cache metrics on closing connections. The benefits of activating or disabling caching might depend on test expected.

```
# echo 'net.ipv4.tcp_no_metrics_save = 1' >> /etc/sysctl.conf
```

Set maximum number of packets, queued on the INPUT side, when the interface receives packets faster than kernel can process them.

```
# echo 'net.core.netdev_max_backlog = 5000' >> /etc/sysctl.conf
```

The commands above configure the parameters and made them persistent into Linux. To reload the changes:

```
# sysctl -p
```

Windows Operating Systems

Please refer at following: [http://msdn.microsoft.com/en-us/library/cc558565\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/cc558565(v=bts.10).aspx)

This article contains all information from Microsoft to optimize TCP stack for performance management.

UDP Throughput Tests

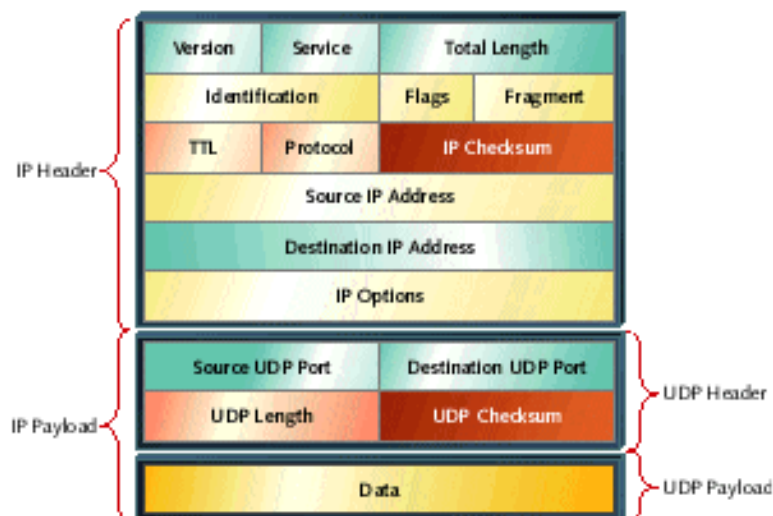
UDP Traffic Generation = Bit Blasting

UDP traffic generation with Hawkeye is a way to generate bit blasting from Keysight performance endpoints.

The traffic rate defined and packet size will be generated from one side to the other.

UDP traffic is generated at layer 4 by Ixia endpoints/probes.

The data is sent through the operating system stack with packet sizes:



- IP header : 20 byte
- UDP header : 8 bytes
- Layer 2 header : 14 to 18 bytes + 4 bytes checksum

All indications into Hawkeye are set at layer 4 (inside UDP header).

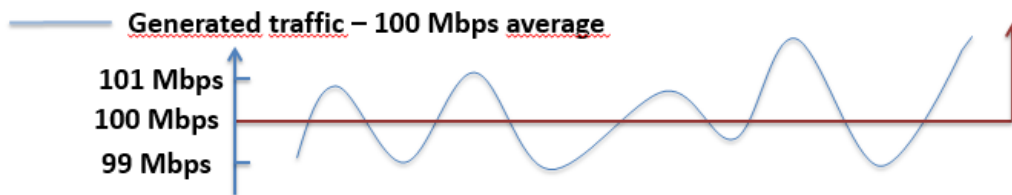
Even though the traffic generation is IP to IP (layer 4) inside UDP packets (layer 4) the result of the traffic generation can be considered as traffic blasting (aka RFC 2544 testing).

UDP Traffic Burstiness

Traffic generation from software based system can create some problems at high rates with traffic generation burstiness.

That means that traffic as sent from Ixia endpoint or probe can be generated with throughout bitrate as requested, but with a non linear profile.

The following figure illustrates a traffic generated with bursts of traffic - typical behavior from a software based traffic generation tool like Hawkeye.



Network equipments like traffic shapers or rate controllers would remove any traffic going at higher rates than 100Mbps in the above example resulting into a problematic measurement of the available bit rate.

Hawkeye implements an algorithm that can be used to reduce dramatically this jitter and side effects measuring UDP flows in networks.

This optimization algorithm that uses very precise timers to reduce jitter between sent packets and when this algorithm is enabled, the datagrams are sent by Endpoint 1 use a lot more precise intervals than when the standard algorithm is in effect.

Enabling this Low Sender Jitter algorithm:

In the **System Preferences > Administration > Preferences > Test Engine**, there is a parameter **lowsendjitter**. This parameter will enable more accurate jitter calculations on the XR2000. This parameter, however, can only be enabled on systems only using the XR2000 endpoints as it invokes a math co-processor that may not be supported on other endpoint types.

UDP packet size and performances

The limitation of packets that can be sent per second typically depends upon the following factors:

- the number of packets / second that Network interface card
- CPU of the system can manage (usually based on # packets per second as well).

The total capacity of network cards and therefore Hawkeye endpoint software is limited by number of packets per second.

Large packets usually result into significant bit rates capabilities.

Smaller packets will have less bit rate on the network, therefore it is expected the total amount of traffic endpoints will be able to generate are declining with the frame rate.

As an example for a network interface card able to generate packets at about line rate for max IP MTU (1500 bytes):

This is only an example and should be read to give guidance on expected throughput capabilities at different packet sizes and levels on an endpoint example. Real value would slightly differ from the table below depending on the endpoint type:

UNIT = BYTE			UNIT = Mbps			
Packet size UDP	Packet size IP	packet size layer 2	Goodput rate	IP rate	layer 2 rate	packets / second
1460	1488	1506	958	976	988	82000
1300	1328	1346	853	871	883	82000
1000	1028	1046	656	674	686	82000
500	528	546	328	346	358	82000
200	228	246	131	150	161	82000
100	128	146	66	84	96	82000
64	92	110	42	60	72	82000
10	38	56	7	25	37	82000

Using the traffic buffering algorithm optimization can help generating more packets per second for powerful cpu endpoints (where bottleneck is in the network interface card): by way of sending more even traffic to the stack, Hawkeye probes optimize the packets that can be sent.

Endpoints support the use of very large frames. When you choose the packet size as **optimized**, a packet size of 64,000 bytes will be used. You must be aware that errors can occur when using this value. The required bit rate will result in 64k packets being sent. If the required bit rate is less than 64 Mbps, no packets will be sent and the test will timeout as an error.

Exceeding UDP Traffic Generation Capability

Hawkeye does not limit the bit rate and packet size generation for users therefore it is essential that users have some understanding of the limits of the probes they are using.

Generating too much traffic will result into packets drops at the traffic generator stack (packets are never sent to the network) or packets being lost at reception of the stack (packets are not counted as received by receiving endpoint/probe).

IMPORTANT

Each Stream is limited to a maximum rate of 4.19Gbps. To test rates higher than 4.19Gbps, please use one of the N Stream Tests.

UDP Throughput Tests Descriptions

	UDP throughput from -> to
Description	One UDP stream - generates throughput with defined packet size and bit rate - from E1 to E2.
Purpose	Send UDP packets (bit blasting) at defined rate to validate the capacity between endpoints.
Available Options	<ul style="list-style-type: none"> • Generated Bitrate • Packet Size • DSCP setting
Metrics	<ul style="list-style-type: none"> • Average Throughput (Mbps) from->to • Loss (%) • Total bytes lost
Advanced Information	This test will generate UDP packets from E1 to E2 based on requested throughput. Test sample Filesize will be computed according to the requested bit rate so that there should be approximately one timing record per second. Optimized packet size is udp size used to optimize the stack therefore pushing packet size bigger than MTU to get full MTU packets on the line. While it provides better results for throughput it can be sensitive to packet fragmentation on the network therefore providing lot of packet losses in some network conditions.
Results interpretation	The result in throughput is displayed at layer 4 level (with ethernet, IP and UDP headers). UDP packet generation is similar to bit blasting therefore will not autoadjust to available bandwidth. Some higher than capacity traffic generation can result into network equipments traffic congestion and therefore cause some service drops.
Potential Errors	<p>If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out (unable to collect result). Small packet sizes are not able to generate as much throughput as large ones: at high traffic, it is possible that endpoints generate packet losses as they would be unable to generate the expected traffic rate.</p> <p>In case of use of UDP packet size optimized or 1460 packet size, be careful in case of low MTU or network fragmentation: this can cause packets to be fragmented therefore unexpected or higher than expected packet loss rates. It is recommended to use a lower UDP packet size (1300 for example) to</p>

	UDP throughput from -> to
	<p>validate there is no impact on test result.</p> <p>If there is unexpected loss this could be because of some bursty UDP traffic generation: make sure you have endpoints supporting the send low jitter option and enable in preferences/test engine in Hawkeye preferences.</p> <p>If results cannot be collected (some pairs did not complete error):</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that port for traffic is opened (no firewall). • Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	UDP throughput to -> from
Description	One UDP stream - generates throughput with defined packet size and bit rate - from E2 to E1 .
Purpose	See UDP throughput from -> to.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

	UDP throughput from -> to N streams
Description	Multiple UDP stream - generates throughput with defined bit rate in multiple streams from E1 to E2.
Purpose	Verify that a multiple UDP stream in one direction is going through. If several streams are configured (>3 typically), total throughput rates can exceed the single stream limit of 4.19Gbps.

	UDP throughput from -> to N streams
Available Options	<ul style="list-style-type: none"> • Generated Bitrate • Packet Size • DSCP setting
Metrics	<ul style="list-style-type: none"> • Average Throughput (Mbps) from->to • Loss (%) • Total bytes lost
Advanced Information	<p>This test will generate UDP packets from E1 to E2 based on requested throughput. Test sample Filesize will be computed according to the requested bit rate so that there should be approximately one timing record per second. Optimized packet size is udp size used to optimize the stack therefore pushing packet size bigger than MTU to get full MTU packets on the line. While it provides better results for throughput it can be sensitive to packet fragmentation on the network therefore providing lot of packet losses in some network conditions.</p>
Results interpretation	<p>The result in throughput is displayed at layer 4 level (with ethernet, IP and UDP headers). UDP packet generation is similar to bit blasting therefore will not autoadjust to available bandwidth. Some higher than capacity traffic generation can result into network equipments traffic congestion and therefore cause some service drops.</p>
Potential Errors	<p>If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out (unable to collect result). Small packet sizes are not able to generate as much throughput as large ones: at high traffic, it is possible that endpoints generate packet losses as they would be unable to generate the expected traffic rate.</p> <p>In case of use of UDP packet size optimized or 1460 packet size, be careful in case of low MTU or network fragmentation: this can cause packets to be fragmented therefore unexpected or higher than expected packet loss rates. It is recommended to use a lower UDP packet size (1300 for example) to validate there is no impact on test result.</p> <p>If there is unexpected loss this could be because of some bursty UDP traffic generation: make sure you have endpoints supporting the send low jitter option and enable in preferences/test engine in Hawkeye preferences.</p> <p>If results cannot be collected (some pairs did not complete error):</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that port for traffic is opened (no firewall). • Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test

	UDP throughput from -> to N streams
	<p>traffic is used.</p> <p>If the number of pairs is greater than available max number of pairs per license the test can be stuck in queue.</p> <p>The maximum number of simultaneous pairs (N value) each individual test can perform is also controlled by a parameter in the System Preferences > Max Concurrent Tests in GUI.</p>

	UDP throughput to -> from N streams
Description	Multiple UDP stream - generates throughput with defined packet size and bit rate in multiple streams from E2 to E1.
Purpose	See UDP throughput from -> to N streams.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

	UDP throughput bidirectional
Description	Bidirectional UDP throughput -with defined packet size and bitrate. The UDP throughput is generated concurrently.
Purpose	<p>Send UDP packets (bit blasting) at defined rate to validate the capacity between endpoints in both directions.</p> <p>Unlike TCP bidirectional, this measure is perfectly valid to measure both ways of communications simultaneously provided there is no max out of endpoint/probe performance.</p>
Available Options	<p>Per directions:</p> <ul style="list-style-type: none"> • Generated Bitrate • Packet Size • DSCP setting

	UDP throughput bidirectional
Metrics	<p>Per direction:</p> <ul style="list-style-type: none"> • Average Throughput (Mbps) from->to • Loss (%) • Total bytes lost
Advanced Information	<p>This test combines UDP stream from E1 to E2 and from E2 to E1. The timing record per pair will be optimized to be one timing record per second.</p> <p>Note that performance of an endpoint sending and receiving is typically lower than endpoint dedicated to sending or receiving.</p> <p>We see typically 20 to 30% performance reduction when traffic is generated both ways as opposed to one way only.</p>
Results interpretation	See UDPthroughput from-> to.
Potential Errors	See UDPthroughput from-> to.

	UDP throughput advanced
Description	UDP throughput between E1 and E2 with advanced parameter options.
Purpose	<p>Send UDP packets (bit blasting) at defined rate to validate the capacity between endpoints in both directions.</p> <p>Advanced options allow to be more specific about what is required.</p>
Available Options	<ul style="list-style-type: none"> • Generated bitrate • UDP send buffer size • file size for timing record sockets size • DSCP setting • source/destination ports
Metrics	<ul style="list-style-type: none"> • Throughput (Mbps) from->to • Loss (%) from->to • Total bytes lost to-->from
Advanced Information	<p>This test will allow to fine tune the UDP stack according to some settings that are dedicated to the test; See Annex for complete UDP stack configuration documentation. Recommended value is filesize to be around 1 second of data transfer at expected throughput so in that case (factor 8 to take into account</p>

	UDP throughput advanced
	the bytes to bit ratio): filesize=throughput (Mbps)*1000/8.
Results interpretation	See UDPthroughput from-> to.
Potential Errors	See UDPthroughput from-> to.

	Network Loss Performance
Description	Determines UDP loss quality metrics between two endpoints.
Purpose	Analyzes loss metrics for a UDP stream played in one direction.
Available Options	<ul style="list-style-type: none"> • Target UDP throughput for one stream • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Packet size
Metrics	Metrics <ul style="list-style-type: none"> • Loss (UDP bytes) • Lost Datagrams (UDP packets) • Max Loss burst • Total Datagrams Rcvd • Total Datagrams Sent
Advanced Information	Thresholds can be set for all above metrics.
Results interpretation	See Advanced Information.
Potential Errors	See <i>XR2000 Error Description Guide</i> .

Network KPI tests

The network KPI test described in this section will allow to test the network by sending "heatbeats" from node to node. These tests are especially suited for Mesh testing as they have little impact on the network and help understanding key transport metrics such as:

- loss
- jitter

- delay

Packet loss is the percentage of packets that are lost out of all packets transmitted. Packet loss burst is a count of the largest number of consecutive packets lost. Important to note that even a small percentage of packets lost can cause TCP packet retransmissions which can lead to network congestion and apparently slow down the network.

These are key SLA indicator for network health and Service Level Agreements.

	Network KPI from->to
Description	Test network delivery KPI with low foot print (100kbps) and 50 packets per second- From E1 to E2 direction.
Purpose	Measuring key KPI loss/jitter/latency.
Available Options	DSCP setting.
Metrics	<ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • voice MOS score • packet loss burst • Max delay variation(ms)
Advanced Information	<p>This test will generate unidirectional traffic with heartbeats to measure the key metrics. The traffic is similar to voice traffic - MOS score is an indicator of capacity of the link to transport Voice in a good quality.</p> <p>The following definitions help to understand key metrics:</p> <ul style="list-style-type: none"> • Max delay variation: The time from when a packet is sent from a probe to when it is received, end to end, is the delay. The max delay variation is the difference between the shortest time and the longest time for this end to end delay for exchanging packets. • Max jitter: This measures the variance in spacing between packets sent end to end. If the difference in time (spacing) between 1st and 2nd packet send from first probe is 2ms, and the time on far end probe receiving 1st and 2nd packets is 3.7ms, the jitter is 3.7ms - 2ms = 1.7ms.
Results interpretation	<p>The network KPI pair generates packets RTP stream.</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc...</p> <p>The packets are sent similarly to a G711 voice stream as this is expected to be a key application the network shall be able to transport.</p> <p>Voice MOS score gives an indication of the quality of transport network for voice G711 application.</p>

	Network KPI from->to
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used).

	Network KPI from->to 3 COS
Description	Test network delivery KPI with low foot print (100kbps per COS) and 50 packets per second- From E1 to E2 direction, on 3 different COS.
Purpose	Measuring key KPI loss/jitter/latency for 3 COS.
Available Options	<p>Per COS :</p> <ul style="list-style-type: none"> • DSCP setting
Metrics	<p>Per COS:</p> <ul style="list-style-type: none"> • one way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • voice MOS score • packet loss burst • max delay variation(ms)
Advanced Information	This test will generate unidirectional traffic with heartbeats to measure the key metrics. The traffic is similar to voice traffic - MOS score is an indicator of capacity of the link to transport Voice in a good quality.
Results interpretation	<p>The network KPI pair generates packets RTP stream.</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc...</p> <p>The packets are sent similarly to a G711 voice stream as this is expected to be a key application the network shall be able to transport.</p> <p>Voice MOS score gives an indication of the quality of transport network for voice G711 application.</p>
Potential	If test result pair cannot be collected:

	Network KPI from->to 3 COS
Errors	<ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used).

	Network KPI to->from
Description	Test network delivery KPI with low foot print (100kbps) and 50 packets per second- From E2 to E1 direction.
Purpose	Measuring key KPI loss/jitter/latency.
Available Options	DSCP setting.
Metrics	<ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • voice MOS score • packet loss burst • max delay variation(ms)
Advanced Information	This test will generate unidirectional traffic with heartbeats to measure the key metrics. The traffic is similar to voice traffic - MOS score is an indicator of capacity of the link to transport Voice in a good quality.
Results interpretation	<p>The network KPI pair generates packets RTP stream.</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc...</p> <p>The packets are sent similarly to a G711 voice stream as this is expected to be a key application the network shall be able to transport.</p> <p>Voice MOS score gives an indication of the quality of transport network for voice G711 application.</p>
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs).

	Network KPI to->from
	<ul style="list-style-type: none"> • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Network KPI bidirectional
Description	Test network delivery KPI with low foot print (100kbps) and 50 packets per second- From E1 to E2 direction and E2 to E1 simultaneously.
Purpose	Measuring key KPI loss/jitter/latency.
Available Options	DSCP setting.
Metrics	<p>Per direction:</p> <ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • voice MOS score • packet loss burst • max delay variation(ms)
Advanced Information	This test will generate unidirectional traffic with heartbeats to measure the key metrics. The traffic is similar to voice traffic - MOS score is an indicator of capacity of the link to transport Voice in a good quality.
Results interpretation	<p>The network KPI pair generates packets RTP stream.</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc...</p> <p>The packets are sent similarly to a G711 voice stream as this is expected to be a key application the network shall be able to transport.</p> <p>Voice MOS score gives an indication of the quality of transport network for voice G711 application.</p>
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management

	Network KPI bidirectional
	<p>UDP 10115).</p> <ul style="list-style-type: none"> • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Network KPI Low Bandwidth
Description	Test network delivery KPI with advanced parameters for packet settings - From E1 to E2 direction - with very low bandwidth (<2kbps line rate) . Only sends 1 heartbeat per second (lower precision).
Purpose	Measuring key KPI loss/jitter/latency.
Available Options	<ul style="list-style-type: none"> • Total bitrate (kbps) for the stream • DSCP setting • packet size
Metrics	<ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • packet loss burst • max delay variation(ms)
Advanced Information	This test will generate unidirectional traffic with heartbeats to measure the key metrics. the low bandwidth of measurements make them less precise than the standard network KPI tests.
Results interpretation	<p>The network KPI pair generates packets RTP stream .</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc...</p>
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Network KPI advanced
Description	Test network delivery KPI with advanced parameters for packet settings - From E1 to E2 direction.
Purpose	Measuring key KPI loss/jitter/latency.
Available Options	<ul style="list-style-type: none"> • Total bitrate (kbps) for the stream • DSCP setting • packet size
Metrics	<ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • max jitter (ms) • packet loss (%) • packet loss burst • max delay variation(ms)
Advanced Information	This test will generate unidirectional traffic with heartbeats to measure the key metrics.
Results interpretation	<p>The network KPI pair generates packets RTP stream .</p> <p>These packets traverse the network from one probe to the other and provides indication based on time sent and receive, how many are lost etc.</p>
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used. • RTP packet loss may be seen above 7 Mbps with default packet size of 50 bytes. In this case, we recommended you to increase packet size to 500 or 1400 bytes. This particularly can be encountered on the XRPI. <div style="display: flex; align-items: flex-start;"> <div style="background-color: #cccccc; padding: 5px; margin-right: 10px; width: 80px; text-align: center;">NOTE</div> <div> <p>The XRPI will encounter performance issues of increased packet loss for throughput above 8Mbps using a packet size of 50 bytes. Using a larger RTP packet size of 500 or 1400 bytes will result in fewer packets processed and lost.</p> </div> </div>

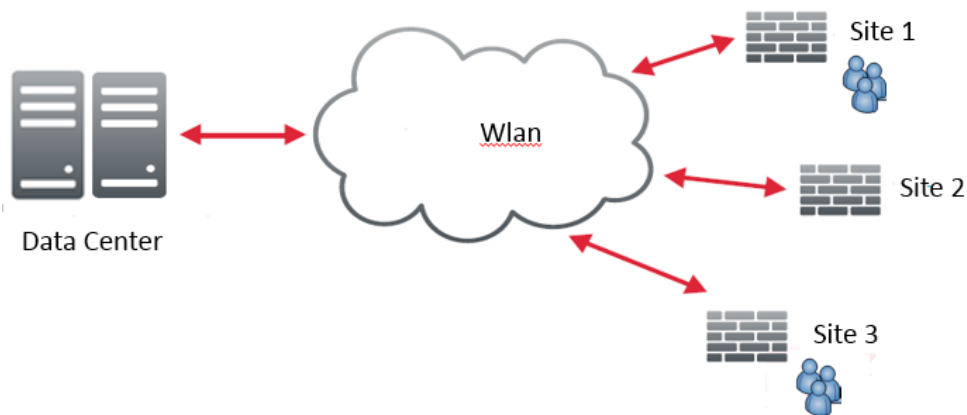
QOS Qualification Tests

The tests detailed in this section are used to qualify Class of Services.

The Class of service implementation in networks is often implemented at layer 3 and required on end to end for full validation. The tests presented in this section will help qualifying the QoS implementation and SLA end to end.

Typical Use Case

The wlan is implemented between sites with CoS



Each link going to remote sites will have same or different Class of Services implementation, tied to same or different SLA from carriers transporting last mile.

- Examples of CoS implementation

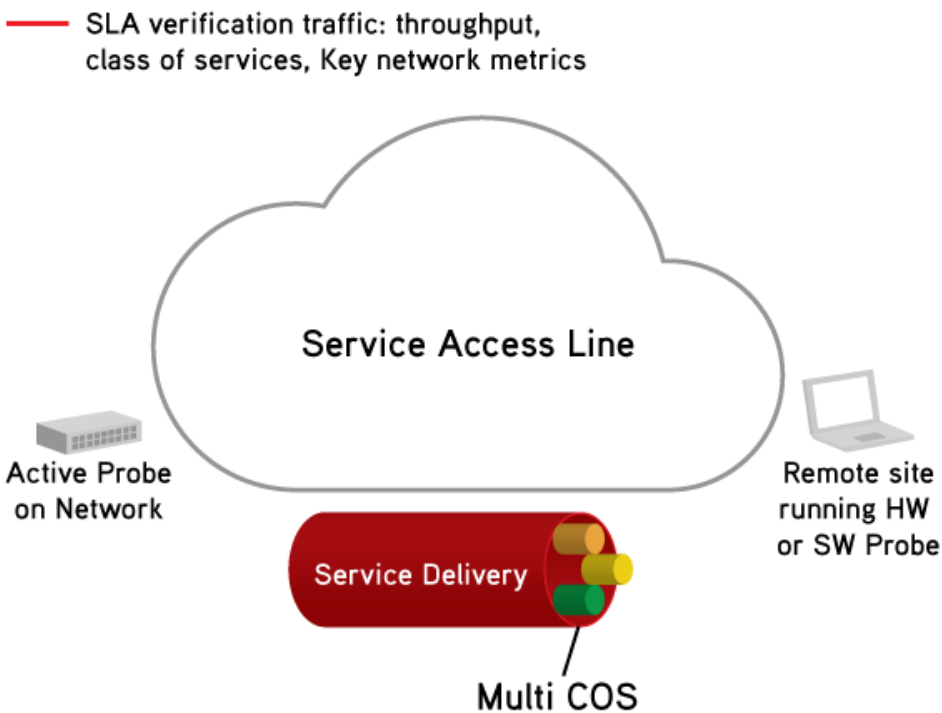


- Real time: Voice over IP, Unified communication voice
- Critical : Critical business applications
- Best Effort : Web, email etc...

The different classes of services are defined based on TOS parameter settings.

Layer 3 Quality of Service

Hawkeye provides support for Layer 3 Quality of Service used on DSCP class name - see dedicated section [ClassOfServices.htm](#) for full details.



You can generate traffic up to line rate with class of service targets, and generate class of service over-subscription traffic.

Typical example is:

- 10% Real time
- 20% critical
- 70% Best effort

In test scenario, try to fill up the link capacity with 100% best effort traffic and 10% voice, 20% critical application.

The scenario will pass if the link discards best effort traffic and sustains prioritized traffic.

Supported Test Types

For testing single class of service with ad hoc COS setting, the different test types described into [TCP throughput tests.htm](#) and [UDP throughput tests.htm](#) sections are available.

Some dedicated test types can be used to fill up different class of services and run over-subscriptions scenarios.

	UDP from->to up to 4 COS
Description	4 UDP streams - each generates throughput with defined packet size and bit rate - from E1 to E2.
Purpose	Send UDP packets (bit blasting) at defined rate to validate the capacity

	UDP from->to up to 4 COS
	between endpoints on all 4 different streams. This will allow to validate class of services mix with bit blasting on each one, and run over-subscription scenarios.
Available Options	<p>Per stream :</p> <ul style="list-style-type: none"> • Generated Bitrate • Packet Size • DSCP setting <p>NOTE If generated bitrate is 0 on one stream then this stream will be ignored</p>
Metrics	<p>Per stream:</p> <ul style="list-style-type: none"> • Average Throughput (Mbps) from->to • Loss (%) • Total bytes lost
Advanced Information	<p>Per stream</p> <p>This test will generate UDP packets from E1 to E2 based on requested throughput. Test sample Filesize will be computed according to the requested bit rate so that there should be approximately one timing record per second. Optimized packet size is udp size used to optimize the stack therefore pushing packet size bigger than MTU to get full MTU packets on the line. While it provides better results for throughput it can be sensitive to packet fragmentation on the network therefore providing lot of packet losses in some network conditions.</p>
Results interpretation	<p>The result in throughput is displayed at layer 4 level (with ethernet, IP and UDP headers). UDP packet generation is similar to bit blasting therefore will not autoadjust to available bandwidth. Some higher than capacity traffic generation can result into network equipments traffic congestion and therefore cause some service drops.</p>
Potential Errors	<p>If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out (unable to collect result). Small packet sizes are not able to generate as much throughput as large ones: at high traffic, it is possible that endpoints generate packet losses as they would be unable to generate the expected traffic rate.</p> <p>In case of use of UDP packet size optimized or 1460 packet size, be careful in case of low MTU or network fragmentation: this can cause packets to be fragmented therefore unexpected or higher than expected packet loss rates. It is recommended to use a lower UDP packet size (1300 for example) to validate there is no impact on test result.</p> <p>If there is unexpected loss this could be because of some bursty UDP traffic generation: make sure you have endpoints supporting the send low jitter</p>

UDP from->to up to 4 COS	
	<p>option and enable in preferences/test engine in Hawkeye preferences.</p> <p>If results cannot be collected (some pairs failures complete error):</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that port for traffic is opened (no firewall). • Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

COS line qualification	
Description	Test consists of up to 4 class of services validation. One is real time (UDP) and others are data oriented (mostly transporting TCP traffic).
Purpose	Send UDP packets (bit blasting) at defined rate to validate the capacity between endpoints on all 4 different streams. The TCP classes of services are tested with TCP stream mixes (3 mixed streams) trying to achieve as much traffic as possible. The class of services should "auto adjust" themselves to the defined compared capacity they should allow transport. For voice class of service, the expected throughput should be defined.
Available Options	<p>Global: filesize (in bytes)- will define which filesize shall be used for TCP traffic generation.</p> <p>Filesize is going to determine how precise and efficient traffic generation on TCP classes of service will be.</p> <p>Each class of service is sent 3 streams.</p> <p>So if classes of services are expected to adjust to :</p> <ul style="list-style-type: none"> • 1M : 40000 bytes • 5M: 200000 bytes • 10M: 400000 bytes <p>For Voice stream: defined bitrate</p> <p>Per stream :</p> <p>Destination port: leave to blank for auto, otherwise put a specific port used by the network architecture to define class of service</p> <p>DSCP setting: define stream class of service</p> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-top: 10px;">NOTE</div> If generated bitrate is 0 on voice stream then this stream will be ignored
Metrics	Voicestream:

	COS line qualification
	<ul style="list-style-type: none"> • Average Throughput (Mbps) from->to • Loss (%) • Total bytes lost • Delay • Jitter • Max loss Burst <p>For TCP streams:</p> <ul style="list-style-type: none"> • Throughput
Advanced Information	<p>Per stream</p> <p>This test will generate TCP packets for class of services and RTP packets for voice.</p> <p>The TCP packets are generated on each class of service so that they should all take most of the class of service.</p> <p>In case class of service reservation is higher on some COS than others the repartition should not be even but reflect what is configured.</p> <p>Each TCP class of service is filled with 3 concurrent streams.</p> <p>The (optional) voice test will provide throughput but also voice related parameters for jitter/loss/delay while the data network is under stress.</p>
Results interpretation	See advanced Information.
Potential Errors	<p>For voice:</p> <p>If the configured is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out (unable to collect result). Small packet sizes are not able to generate as much throughput as large ones: at high traffic, it is possible that endpoints generate packet losses as they would be unable to generate the expected traffic rate.</p> <p>For TCP: the filesize needs to be adjusted to the expected minimum COS throughput. Setting a filesize too high might result into test impossible to finish because file transfer is too long.</p> <p>If results cannot be collected (some pairs did not complete error):</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that port for traffic is opened (no firewall). • Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used).

Voice and Video Tests

A variety of voice and video tests are supported using the latest codecs.

Voice

	Voice from->to
Description	Test voice quality from E1 to E2, with G711, G729, AMR codecs.
Purpose	Voice Media stream is generated in one direction and key transport metrics are validated. At the same time a Mean Opinion Score is computed to validate the transport quality.
Available Options	Voice codec: G711, G729, AMR DSCP setting.
Metrics	<ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • jitter max (ms) • packet loss (%) • voice MOS score on path • packet loss burst
Advanced Information	This test will generate unidirectional Voice traffic with selected codec.
Results interpretation	The voice pair generates RTP stream according to selected codec. The content of the voice traffic itself is not actual voice. This test qualifies network transport capability for realistic voice traffic.
Potential Errors	<p>If test result pair cannot be collected: Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.</p> <p>If results cannot be collected (some pairs failures complete error): Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs).</p> <p>Check that port for traffic is opened (no firewall).</p> <p>Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.</p>

	Voice bidirectional
Description	Test voice quality from E1 to E2 AND E2 to E1, with G711, G729, AMR codecs. Metrics are gathered by direction. This reproduces a realistic voice media call.
Purpose	See Voice from-> to.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

	Voice n pairs unidirectional
Description	Test voice quality from E1 to E2, with G711, G729, AMR codecs, with N calls simultaneously.
Purpose	Voice Media stream is generated in one direction and key transport metrics are validated. At the same time a Mean Opinion Score is computed to validate the transport quality. This test is performed for N calls.
Available Options	Voice codec: G711, G729, AMR DSCP setting , Number of calls.
Metrics	Aggregated over the N pairs: <ul style="list-style-type: none"> • One way delay (ms) • jitter (ms) • jitter max (ms) • packet loss (%) • voice MOS score on path • packet loss burst Total Voice traffic throughput (layer 4)
Advanced Information	This test will generate N pairs. Test results are aggregated and there are no detailed results.

	Voice n pairs unidirectional
Results interpretation	See Voice from->to.
Potential Errors	<p>If the number of pairs selected is greater than available licenses the test can be stuck in queue. Note the number of pairs is N (one pair per voice direction).</p> <p>The maximum number of simultaneous pairs (N value) each individual test can perform is also controlled from an advanced setting. Only Administrator can modify this setting:</p> <p>In Main Section, Max Concurrent Tests in GUI</p> <p>See voice from->to for other potential issues.</p>

	Voice n pairs bidirectional
Description	<p>Test voice quality from E1 to E2 AND E2 to E1, with G711, G729, AMR codecs. Metrics are gathered by direction.</p> <p>This reproduces a realistic voice media call.</p> <p>This test does N calls.</p>
Purpose	See Voice N pairs unidirectional.
Available Options	
Metrics	
Advanced Information	
Results interpretation	
Potential Errors	

Video Stream

For public endpoint to private endpoint tests, complete the following steps:

1. Enable a range of source and destination ports for traffic in **Preferences > Traffic Management**.
2. Open the ports in the firewall for the private endpoint.

NOTE

If a CGN gateway is present for the private endpoint, it may not be possible to open the necessary ports which will prevent Video traffic. This will impact the following test types: Netflix, Youtube, Adaptive Video, Adaptive video with quality, Flash RTMP, and Multicast Video over RTMP.

	Video Stream
Description	Define a video stream from E1 to E2 with defined bit rate and MPEG2 or customizable codec. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	Generate a unidirectional video flow from E1 to E2. This can simulate video based on RTP/UDP flows going through the network.
Available Options	<ul style="list-style-type: none"> Generated bitrate DSCP setting
Metrics	<ul style="list-style-type: none"> One way delay (ms) jitter (ms) jitter max (ms) packet loss (%) max loss burst video MDI scores (Media Delivery Index, Delay Factor)
Advanced Information	This test allows generating video rtp streams - bitrate will define corresponding codec (HD or SD).
Results interpretation	This test generate Video stream on the selected path. It can be optimized with setting up send low jitter in the preferences to be 1 if the endpoints support it.
Potential Errors	If test result pair cannot be collected: Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). Check that synchronization port between pairs is opened (management UDP 10115). Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Multicast Video over RTP
Description	Multicast Flow. Emulates the standard streaming video codec. Measures video metrics. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	Generate a multicast video flows from E1 to (E2.....EN). Where N the number of endpoints supported in the Mesh. This can simulate video based on RTP/UDP flows going through the network.
Available Options	Test duration , Test bit rate (Mbps), DSCP Setting, Multicast Address: Port Video from->to.
Metrics	<ul style="list-style-type: none"> Datagrams Out of Order Delay (ms)

	<ul style="list-style-type: none"> • Jitter (ms) • Jitter Max (ms) • Loss • Max loss burst • Source and destination ports • Throughput Video (Mbps) • Total Bytes Lost Video • MDI Delay Factor (Media Delivery Index, Factor) • Video MDI Media Loss Rate (Media Delivery Index, Loss Rate)
Advanced Information	This test allows generating video rtp streams - bitrate will define corresponding codec (HD or SD).
Results interpretation	This test generate Video stream on the selected path. It can be optimized with setting up send low jitter in the preferences to be 1 if the endpoints support it.
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Ensure that synchronization port between pairs is opened (management UDP 10115). • Ensure that the port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Adaptive video
Description	Emulates Adaptive Video Streaming over HTTP. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	<p>In the case of this video streaming technique, the video is encoded on a server at several bitrates and divided into video segments of 2 to 10 seconds.</p> <p>The client first learns the available bitrates by downloading a video manifest, then starts requesting video segments from the server at a specific bitrate. The client starts requesting video segments at a medium bitrate, but this can be changed by altering the Starting Bitrate parameter of any Adaptive Video over HTTP flows.</p> <p>Depending on the network bandwidth and the local speed of video decoding and rendering, the client can decide to increase (upshift) or decrease (downshift) the requested bitrate for future video segments as compared to that requested for the previous video segments.</p>
Available	Test duration , Test bit rate list, DSCP Setting, Number of Parallel Streams.

	Adaptive video
Options	
Metrics	<ul style="list-style-type: none"> • Avg Video Playback Rate (bps) • Avg Video Pre-buffering duration (ms) • Jitter Buffer Full Count • Jitter Buffer Full Duration (ms) • Throughput from->to (Mbps) • Video Playback Downshifts • Video Playback Upshifts • Video Quality Segments - Very High • Video Quality Segments - High • Video Quality Segments - Medium • Video Quality Segments - Low • Video Quality Segments - Very Low • Video Stopped Count • Video Stopped Duration (ms)
Advanced Information	<p>Upshifting provides better video quality, but at a greater risk of playback interruptions, while downshifting increases playback smoothness at the expense of video quality.</p> <p>Through its adapting capability, this video streaming technique provides the best trade-off between video quality and smooth video streaming.</p>
Results interpretation	<p>Where no jitter buffer is used (there are no video download limitations), the video is downloaded at the maximum speed allowed by network conditions. This means that there are no pauses between GET requests.</p> <p>One in which the jitter buffer is used and as such, the download of the video segments is paused when the buffer becomes full. On average, the throughput will not exceed the maximum video bitrate.</p> <p>Video Playback Downshift is a decrease in the requested bit rate for future video segments as compared to that requested for the previous video segments. Video Playback Upshift is an increase in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video quality segments indicate the distribution of video playback quality. Video stopped count and duration indicate the video playback interruptions and its duration.</p>
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs).

	Adaptive video
	<ul style="list-style-type: none"> • Ensure that synchronization port between pairs is opened (management UDP 10115). • Ensure that port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Adaptive video with network quality
Description	Emulates Adaptive Video Streaming over HTTP and measure network quality with a separate stream. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	<p>In the case of this video streaming technique, the video is encoded on a server at several bitrates and divided into video segments of 2 to 10 seconds. The client first learns the available bitrates by downloading a video manifest, then starts requesting video segments from the server at a specific bitrate.</p> <p>The client starts requesting video segments at a medium bitrate, but this can be changed by altering the Starting Bitrate parameter of any Adaptive Video over HTTP flows. Depending on the network bandwidth and the local speed of video decoding and rendering, the client can decide to increase (upshift) or decrease (downshift) the requested bitrate for future video segments as compared to that requested for the previous video segments.</p> <p>Additionally this also tests the Network KPI along with video streaming on both directions : it adds a bidirectional very low footprint packet heartbeat to measure the network kpis (loss/delay/jitter) on the segment.</p>
Available Options	Test duration , Test bit rate list, DSCP Setting, Number of Parallel Streams.
Metrics	<ul style="list-style-type: none"> • Avg Video Playback Rate (bps) • Avg Video Pre-buffering duration (ms) • Jitter Buffer Full Count • Jitter Buffer Full Duration (ms) • Throughput from->to (Mbps) • Video Playback Downshifts • Video Playback Upshifts • Video Stopped Count • Video Stopped Duration (ms) <p>Network KPI Metric:</p> <ul style="list-style-type: none"> • Delay (Ms):

	Adaptive video with network quality
	<ul style="list-style-type: none"> • Jitter (Ms): • Jitter Max (Ms): • Loss:
Advanced Information	<p>Upshifting provides better video quality, but at a greater risk of playback interruptions, while downshifting increases playback smoothness at the expense of video quality.</p> <p>Through its adapting capability, this video streaming technique provides the best trade-off between video quality and smooth video streaming.</p>
Results interpretation	<p>This test is realistic and since jitter buffer is used and as such, the download of the video segments is paused when the buffer becomes full. On average, the throughput will not exceed the maximum video bitrate.</p> <p>Video Playback Downshift is a decrease in the requested bit rate for future video segments as compared to that requested for the previous video segments. Video Playback Upshift is an increase in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video quality segments indicate the distribution of video playback quality Video stopped count and duration indicate the video playback interruptions and its duration.</p> <p>Video Stopped Count Video Stopped Duration will tell for any user experience having video stalling during the watch.</p> <p>The number of Downshift and Upshifts indicate how often the adaptive rate needed to change: lots of changes indicate an instable network condition.</p> <p>The Avg Playback rate will indicate the overall video quality experience: high rate will mean the high quality segments could be transported, lower rates mean the video had to adapt to lower quality segments.</p>
Potential Errors	<p>This test can only work from public->public, private->private and private->public. It is NOT supported for public->private direction.</p> <p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Flash RTMP
Description	Emulates Adaptive Video Streaming With default RTMP bit rates sizes. "The client is the "From" endpoint and the server is the "To" endpoint".
Purpose	In the case of this video streaming technique, the video is encoded on a server

	Flash RTMP
	<p>at several bitrates and divided into video segments of 2 to 10 seconds.</p> <p>The client first learns the available bitrates by downloading a video manifest, then starts requesting video segments from the server at a specific bitrate.</p> <p>The client starts requesting video segments at a medium bitrate, but this can be changed by altering the Starting Bitrate parameter of any Adaptive Video over HTTP flows.</p> <p>Depending on the network bandwidth and the local speed of video decoding and rendering, the client can decide to increase (upshift) or decrease (downshift) the requested bitrate for future video segments as compared to that requested for the previous video segments.</p> <p>Additionally this also tests the Network KPI along with video streaming.</p>
Available Options	Test duration , Test bit rate list, DSCP Setting, Number of Parallel Streams.
Metrics	<ul style="list-style-type: none"> • Avg Video Playback Rate (bps) • Avg Video Pre-buffering duration (ms) • Jitter Buffer Full Count • Jitter Buffer Full Duration (ms) • Throughput from->to (Mbps) • Video Playback Downshifts • Video Playback Upshifts • Video Stopped Count • Video Stopped Duration (ms)
Advanced Information	<p>Upshifting provides better video quality, but at a greater risk of playback interruptions, while downshifting increases playback smoothness at the expense of video quality.</p> <p>Through its adapting capability, this video streaming technique provides the best trade-off between video quality and smooth video streaming.</p>
Results interpretation	<p>The download of the video segments is paused when the buffer becomes full. On average, the throughput will not exceed the maximum video bitrate.</p> <p>Video Playback Downshift is a decrease in the requested bit rate for future video segments as compared to that requested for the previous video segments. Video Playback Upshift is an increase in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video quality segments indicate the distribution of video playback quality. Video stopped count and duration indicate the video playback interruptions and its duration.</p> <p>Video Stopped Count Video Stopped Duration will tell for any user experience having video stalling during the watch.</p>

	Flash RTMP
	<p>The number of Downshift and Upshifts indicate how often the adaptive rate needed to change: lots of changes indicate an instable network condition.</p> <p>The Avg Playback rate will indicate the overall video quality experience: high rate will mean the high quality segments could be transported, lower rates mean the video had to adapt to lower quality segments.</p>
Potential Errors	<p>This test can only work from public->public, private->private and private->public. It is NOT supported for public->private direction</p> <p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Netflix
Description	Emulates Netflix Adaptive Video. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	<p>In the case of this video streaming technique, the video is encoded on a server at several bitrates and divided into video segments of 2 to 10 seconds.</p> <p>The client first learns the available bitrates by downloading a video manifest, then starts requesting video segments from the server at a specific bitrate.</p> <p>The client starts requesting video segments at a medium bitrate, but this can be changed by altering the Starting Bitrate parameter of any Adaptive Video over HTTP flows.</p> <p>Depending on the network bandwidth and the local speed of video decoding and rendering, the client can decide to increase (upshift) or decrease (downshift) the requested bitrate for future video segments as compared to that requested for the previous video segments. Additionally this also tests the Network KPI along with video streaming.</p>
Available Options	Test duration , Video Rates Video Stream, Audio Rates Audio Stream, quality for video (HD or SD), DSCP Setting, Number of Parallel Streams.
Metrics	<ul style="list-style-type: none"> • Avg Video Playback Rate (bps) • Avg Video Pre-buffering duration (ms) • Jitter Buffer Full Count • Jitter Buffer Full Duration (ms) • Throughput from->to (Mbps) • Video Playback Downshifts • Video Playback Upshifts

	Netflix
	<ul style="list-style-type: none"> • Video Stopped Count • Video Stopped Duration (ms)
Advanced Information	<p>Upshifting provides better video quality, but at a greater risk of playback interruptions, while downshifting increases playback smoothness at the expense of video quality.</p> <p>Through its adapting capability, this video streaming technique provides the best trade-off between video quality and smooth video streaming.</p>
Results interpretation	<p>Where no jitter buffer is used (there are no video download limitations), the video is downloaded at the maximum speed allowed by network conditions. This means that there are no pauses between GET requests.</p> <p>One in which the jitter buffer is used and as such, the download of the video segments is paused when the buffer becomes full. On average, the throughput will not exceed the maximum video bitrate. Video Playback Downshift is a decrease in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video Playback Upshift is an increase in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video quality segments indicate the distribution of video playback quality</p> <p>Video stopped count and duration indicate the video playback interruptions and its duration.</p> <p>Video Stopped Count Video Stopped Duration will tell for any user experience having video stalling during the watch. The number of Downshift and Upshifts indicate how often the adaptive rate needed to change: lots of changes indicate an instable network condition. The Avg Playback rate will indicate the overall video quality experience: high rate will mean the high quality segments could be transported, lower rates mean the video had to adapt to lower quality segments.</p>
Potential Errors	<p>This test can only work from public->public, private->private and private->public. It is NOT supported for public->private direction.</p> <p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

	Youtube
Description	Emulates Youtube Adaptive Video. The client is the "From" endpoint and the server is the "To" endpoint.
Purpose	In the case of this video streaming technique, the video is encoded on a server

	Youtube
	<p>at several bitrates and divided into video segments of 2 to 10 seconds. The client first learns the available bitrates by downloading a video manifest, then starts requesting video segments from the server at a specific bitrate.</p> <p>The client starts requesting video segments at a medium bitrate, but this can be changed by altering the Starting Bitrate parameter of any Adaptive Video over HTTP flows.</p> <p>Depending on the network bandwidth and the local speed of video decoding and rendering, the client can decide to increase (upshift) or decrease (downshift) the requested bitrate for future video segments as compared to that requested for the previous video segments. Additionally this also tests the Network KPI along with video streaming.</p>
Available Options	Test duration, Video Rates Video Stream, Test bit rate list, DSCP Setting, Number of Parallel Streams.
Metrics	<ul style="list-style-type: none"> • Avg Video Playback Rate (bps) • Avg Video Pre-buffering duration (ms) • Jitter Buffer Full Count • Jitter Buffer Full Duration (ms) • Throughput from->to (Mbps) • Video Playback Downshifts • Video Playback Upshifts • Video Stopped Count • Video Stopped Duration (ms)
Advanced Information	<p>Upshifting provides better video quality, but at a greater risk of playback interruptions, while downshifting increases playback smoothness at the expense of video quality.</p> <p>Through its adapting capability, this video streaming technique provides the best trade-off between video quality and smooth video streaming.</p>
Results interpretation	<p>Where no jitter buffer is used (there are no video download limitations), the video is downloaded at the maximum speed allowed by network conditions. This means that there are no pauses between GET requests. One in which the jitter buffer is used and as such, the download of the video segments is paused when the buffer becomes full. On average, the throughput will not exceed the maximum video bitrate.</p> <p>Video Playback Downshift is a decrease in the requested bit rate for future video segments as compared to that requested for the previous video segments. Video Playback Upshift is an increase in the requested bit rate for future video segments as compared to that requested for the previous video segments.</p> <p>Video quality segments indicate the distribution of video playback quality Video stopped count and duration indicate the video playback interruptions</p>

	Youtube
	<p>and its duration.</p> <p>Video Stopped Count Video Stopped Duration will tell for any user experience having video stalling during the watch.</p> <p>The number of Downshift and Upshifts indicate how often the adaptive rate needed to change: lots of changes indicate an instable network condition.</p> <p>The Avg Playback rate will indicate the overall video quality experience: high rate will mean the high quality segments could be transported, lower rates mean the video had to adapt to lower quality segments.</p>
Potential Errors	<p>This test can only work from public->public, private->private and private->public. It is NOT supported for public->private direction.</p> <p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that port in use is in range. See "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

Unified Communications

Unified communication traffic regenerates voice and video traffic that goes through networks.

	Citrix
Description	Citrix Traffic - From Probe Is Client And To Probe Is Server
Purpose	
Available Options	<ul style="list-style-type: none"> • Traffic Duration
Metrics	<ul style="list-style-type: none"> • Throughput (Mbps) from->to • Response Time (ms) • Transaction Rate (per sec)
Advanced Information	
Results interpretation	
Potential Errors	

	Skype4B traffic from -> to
Description	Microsoft Skype4B traffic. Default parameters for audio and video based on Microsoft recommended settings. User configurable parameters. This test is for bidirectional configuration.

	Skype4B traffic from -> to
Purpose	Reproduce Skype4B traffic to assess the network capability to transport this traffic either in volumes or for single calls.
Available Options	<p>For each direction, options include the following:</p> <ul style="list-style-type: none"> • Generated bitrate audio • Generated bitrate video • QOS for each traffic • Packet size audio • Packet size video • Total number of users (number of streams)
Metrics	<p>For each direction and each stream (audio/video), options include the following:</p> <ul style="list-style-type: none"> • Upstream and downstream loss • Jitter • Max jitter • One way delay • Throughput audio • Throughput video • Max loss bursts (max consecutive packet loss)
Advanced Information	<p>Skype4B traffic unidirectional emulates Skype4B users talking to each other in one way. This test is designed according to Microsoft recommended network validation of network use for Skype4B. You can use and fine tune the test for any Unified Communication solution that combines Voice and Video traffic. We recommend you to use the test in meshes so that both directions are tested at the same time.</p> <p>The number of users is typically not used to generate volume traffic. We recommend you to leave this setting to 1 and compute the total volume of traffic according to traffic profiles.</p>
Results interpretation	This test generates Skype4B Audio and Video streams on the selected paths. You can optimize the test by setting up Send Low Jitter in Preferences to be 1, if the endpoints support it.
Potential Errors	<p>If test result pair cannot be collected, check the following:</p> <ul style="list-style-type: none"> • Your E2 endpoint can open the 10115 port toward E1 for management (this is needed for stream pairs). • Synchronization port between the pairs is opened (management UDP 10115). • Port in use is in range. See Preferences > Traffic Port Management > Destination Port Conf Option and Preferences > Test

Skype4B traffic from -> to	
	<p>Controller > First Destination Port so that you can use the correct destination port for test traffic.</p> <p>NOTE Skype4B has its own port management control. Go to Preferences > Traffic Port Management > Destination Port Conf Option. If Use Skype4B Special Range option is set to 1 this will take precedence over the default port management for Skype4B tests (only for Skype4B tests).</p>

Skype4B traffic	
Description	Microsoft Skype4B traffic. Default parameters for audio and video based on microsoft recommended settings. User configurable parameters. This test is for unidirectional configuration.
Purpose	<p>Reproduce Skype4B traffic to assess the network capability to transport this traffic either in volumes or for single calls.</p> <p>This test is for bidirectional communication - reproducing the traffic of realistic conversations.</p>
Available Options	<p>Per direction:</p> <ul style="list-style-type: none"> • Generated bitrate audio • Generated bitrate video • QOS for each traffic • Packet size audio • Packetsize video • Total number of users (number of streams) <p>NOTE Typically traffic are symmetrical per transaction.</p>
Metrics	<p>For each direction and each stream (audio/video)</p> <ul style="list-style-type: none"> • Upstream/Downstream loss • jitter • max jitter • one way delay • throughput audio • throughput video • max loss bursts (max consecutive packet loss)
Advanced Information	Skype4B traffic unidirectional emulates Skype4B users talking to each other in one way. This test is designed according to Microsoft recommended network

	Skype4B traffic
	<p>validation of network use for Skype4B. You can use and fine tune the test for any Unified Communication solution that combines Voice and Video traffic. We recommend you to use the test in meshes so that both directions are tested at the same time.</p> <p>The number of users is typically not used to generate volume traffic. We recommend you to leave this setting to 1 and compute the total volume of traffic according to traffic profiles.</p>
Results interpretation	This test generates Skype4B traffic streams on the selected paths. You can optimize the test by setting up Send Low Jitter in Preferences to be 1, if the endpoints support it.
Potential Errors	<p>If test result pair cannot be collected, check the following:</p> <ul style="list-style-type: none"> • Your E2 endpoint can open the 10115 port toward E1 for management (this is needed for stream pairs). • Synchronization port between the pairs is opened (management UDP 10115). • Port in use is in range. See Preferences > Traffic Port Management > Destination Port Conf Option and Preferences > Test Controller > First Destination Port so that you can use the correct destination port for test traffic. <p>NOTE Skype4B has its own port management control. Go to Preferences > Traffic Port Management > Destination Port Conf Option. If Use Skype4B Special Range option is set to 1 this will take precedence over the default port management for Skype4B tests (only for Skype4B tests).</p>

	Teams Cloud Call
Description	<p>Microsoft Teams Cloud Call is generating Cloud calls emulating Microsoft Teams media protocols. Node from should be on prem while node to should be in the cloud. The same ports and traffic patterns than realistic cloud calls are going to be emulated.</p> <p>Ideally endpoint to (destination of the call) should be in Azure Cloud to emulate a Teams handler. Alternatively having any location on internet using other public clouds can be sufficient to validate the WAN/last mile portion.</p>
Purpose	<p>Reproduce Teams Cloud traffic to assess the network capability to transport this traffic either in volumes or for single calls.</p> <p>This test is handling bidirectional communication - reproducing the traffic of realistic conversations.</p>
Available	Per direction:

Teams Cloud Call	
Options	<ul style="list-style-type: none"> • Number of calls supporting Audio • Number of calls supporting Video (typically same or less than Audio only) • QOS for each traffic • Packet size audio (only option is 100 bytes) • Packet size video (only option is 1000 bytes) • Port to use for contacting server – defaults to Microsoft Teams cloud range. <div>NOTE</div> Typically, traffic is symmetrical per transaction.
Metrics	<p>For each direction and each stream (audio/video), following are the metrics:</p> <ul style="list-style-type: none"> • Upstream/Downstream loss • jitter • max jitter • one-way delay • throughput audio • throughput video • max loss bursts (max consecutive packet loss)
Advanced Information	The number of calls is typically not used to generate volume traffic. We recommend you to leave this setting to 1 and compute the total volume of traffic according to traffic profiles.
Results interpretation	This test generates Teams Audio and Video streams on the selected paths. Default thresholds are set according to Microsoft minimum recommendations.
Potential Errors	<p>If test result pair cannot be collected, check the following:</p> <ul style="list-style-type: none"> • Your E2 endpoint can open the 10115 port toward E1 for management (this is needed for stream pairs). • Synchronization port between the pairs is opened (management UDP 10115). • Port in use is in range. See Preferences > Traffic Port Management > Destination Port Conf Option and Preferences > Test Controller > First Destination Port so that you can use the correct destination port for test traffic. <div>NOTE</div> Ports used are part of the test parameters and not from ones set in preferences

Teams WAN Call	
Description	Microsoft Teams WAN Call is generating WAN calls emulating Microsoft Teams

	Teams WAN Call
	media protocols. Node from and to should be on same WAN emulating calls between computers or from computers to a gateway. The same ports and traffic patterns than realistic cloud calls are going to be emulated.
Purpose	<p>Reproduce Teams WAN traffic to assess the network capability to transport this traffic either in volumes or for single calls.</p> <p>This test is handling bidirectional communication – reproducing the traffic of realistic conversations.</p>
Available Options	<p>Per direction:</p> <ul style="list-style-type: none"> • Number of calls supporting Audio • Number of calls supporting Video (typically same or less than Audio only) • QOS for each traffic • Packet size audio (only option is 100 bytes) • Packet size video (only option is 1000 bytes) • Port to use for contacting server – defaults to Microsoft Teams WAN range. <p>NOTE Typically, traffic is symmetrical per transaction.</p>
Metrics	<p>For each direction and each stream (audio/video), following are the metrics:</p> <ul style="list-style-type: none"> • Upstream/Downstream loss • jitter • max jitter • one-way delay • throughput audio • throughput video • max loss bursts (max consecutive packet loss)
Advanced Information	The number of calls is typically not used to generate volume traffic. We recommend you to leave this setting to 1 and compute the total volume of traffic according to traffic profiles.
Results interpretation	This test generates Teams Audio and Video streams on the selected paths. Default thresholds are set according to Microsoft minimum recommendations.
Potential Errors	<p>If test result pair cannot be collected, check the following:</p> <ul style="list-style-type: none"> • Your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Synchronization port between the pairs is opened (management UDP 10115). • Port in use is in range. See Preferences > Traffic Port Management

Teams WAN Call	
	<p>> Destination Port Conf Option and Preferences > Test Controller > First Destination Port so that correct destination port for test traffic is used.</p> <p>NOTE Ports used are part of the test parameters and not from ones set in preferences</p>

Traffic Mix – HTTP – Video - Voice	
Description	Traffic Mix. Emulates three different traffic types. Measures voice, video and HTTP metrics.
Purpose	This can simulate three traffic types through network with one test.
Available Options	Test duration, Total bitrate voice from->to, and Total bitrate HTTP from->to.
Metrics	<ul style="list-style-type: none"> • HTTP throughput (Kbpa) • HTTP Transactions per sec • Delay video (ms) • Jitter video (ms) • Loss video • Max loss burst video • Throughput Video (Mbps) • Total Bytes Lost Video • Delay voice (ms) • Jitter voice (ms) • Loss voice (ms) • Max Loss Burst voice (ms) • MOS
Advanced Information	This test uses pre-defined configurations for Video and Voice codec traffic.
Results interpretation	This test generates test metrics for HTTP/Video/Voice.
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Ensure that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Ensure that synchronization port between pairs is opened (management UDP 10115).

	Traffic Mix – HTTP – Video - Voice
	<ul style="list-style-type: none"> • Ensure that ports for video and voice are open.

	Zoom meeting
Description	<p>Zoom meeting is generating traffic emulating Zoom meeting media protocols. Node from should be on prem while node to should be in the cloud. The same ports and traffic patterns than realistic cloud calls are going to be emulated. Ideally endpoint to (destination of the call) should be in any location on internet using public clouds to validate the WAN/last mile portion.</p>
Purpose	<p>Reproduce Zoom traffic to assess the network capability to transport this traffic either in volumes or for single calls.</p> <p>This test is handling bidirectional communication - reproducing the traffic of realistic conversations.</p>
Available Options	<p>Per direction:</p> <ul style="list-style-type: none"> • Number of calls supporting Audio • Number of calls supporting Video (typically same or less than Audio only) • QOS for each traffic • Packet size audio (only option is 100 bytes) • Packet size video (only option is 1000 bytes) • Port to use for contacting server – defaults to Zoom Meeting cloud range. <p>NOTE Typically, traffic is symmetrical per transaction.</p>
Metrics	<p>For each direction and each stream (audio/video), following are the metrics:</p> <ul style="list-style-type: none"> • Upstream/Downstream loss • jitter • max jitter • one-way delay • throughput audio • throughput video • max loss bursts (max consecutive packet loss)
Advanced Information	<p>The number of calls is typically not used to generate volume traffic. We recommend you to leave this setting to 1 and compute the total volume of traffic according to traffic profiles.</p>
Results interpretation	<p>This test generates Zoom Audio and Video streams on the selected paths. Default thresholds are set according to Zoom minimum recommendations.</p>

Zoom meeting	
Potential Errors	<p>If test result pair cannot be collected, check the following:</p> <ul style="list-style-type: none"> • Your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Synchronization port between the pairs is opened (management UDP 10115). • Port in use is in range. See Preferences > Traffic Port Management > Destination Port Conf Option and Preferences > Test Controller > First Destination Port so that correct destination port for test traffic is used. <div> NOTE Ports used are part of the test parameters and not from ones set in preferences. </div>

Real Time Transactional Applications Tests

Transactional application tests are all based on the same principle:

Tests consist of a number of transactions between endpoints based on a defined network pattern.

The unitary transaction consists on exchange of information - typically from client (E1, or endpoint from) to server (E2, endpoint to).

This transaction is based on simple exchange (one GET and file reception) or multiple exchange.

The defined throughput will take into account TOTAL throughput on both sides (adding upstream and downstream traffic) and is mostly used to limit the impact on transactions on the network.

RTSP	
Description	Simulate RTSP streaming—client (from probe) requests video to server (to probe) - to probe sends video traffic to client (RTP/UDP). It is a simple transaction (one packet) with get from client (endpoint from-E1) and response from server (endpoint to-E2). And it defines a video stream from E2 to E1 with defined bit rate and MPEG2 or customizable codec. The client is the 'From' endpoint and the server is the 'To' endpoint.
Purpose	Measure simple TCP response time and / or transaction rate. Allows to understand response time for TCP through very simple transactions on network. Also generates a unidirectional video flow from E2 to E21. This can simulate video based on RTP/UDP flows going through the network.
Available Options	<ul style="list-style-type: none"> • Test Duration • Generated bitrate • DSCP setting
Metrics	<ul style="list-style-type: none"> • Delay (ms) • Jitter (ms) • Jitter max (ms)

	RTSP
	<ul style="list-style-type: none"> • Loss (%) • Max loss burst • Throughput video (Mbps) <p>RTSP Control:</p> <ul style="list-style-type: none"> • Response Time (ms)
Advanced Information	<p>This test sends tcp sync and waits for response. Then 100 bytes are sent from E1 to E2 and 100 bytes are sent from E2 to E1. Typically, only 2 packets are exchanged for full transaction.</p> <p>This test allows generating video rtp streams—bitrate defines corresponding codec (HD or SD).</p>
Results interpretation	<p>The response time is the expected time to transfer very simple packets in both directions into two payloads with TCP. In case of retransmissions, the response time increases significantly.</p> <p>By default, no objective is set to throughput: any result is good enough, because the total throughput must reflect the response time and transaction rate (transaction rate is 1/response time).</p> <p>This test generates video stream on the selected path. It can be optimized with setting up send low jitter in the preferences to be 1 if the endpoints support it.</p>
Potential Errors	<p>If the configured bitrate is set too high compared to the expected line capacity:</p> <ul style="list-style-type: none"> • The test may not be able to accomplish first measurement. This configuration results in an error with time out ('Some pairs in tests failures complete'). <p>If the test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs). • Check that synchronization port between pairs is opened (management UDP 10115). • Check that port in use is in the range. See preferences/Test Controller/Destination Port Conf option and preferences/Test Controller/First Destination Port, so that correct destination port for test traffic is used.

	TCP response time
Description	Simple transaction (one packet) with get from client (endpoint from) and response from server (endpoint to).

	TCP response time
Purpose	Measure simple TCP response time and / or transaction rate. Allows to understand response time for TCP very simple transactions on network.
Available Options	<ul style="list-style-type: none"> • Test duration , DSCP setting
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)
Advanced Information	<p>This test sends tcp sync and waits for response.</p> <p>then 100 bytes are sent E1 to E2 and 100 bytes are sent from E2 to E1.</p> <p>Typically only 2 packets are exchanged for full transaction.</p>
Results interpretation	<p>The response time is the expected time to transfer very simple packets in both directions into 2 payloads with TCP. In case of retransmissions the response time will increase significantly.</p> <p>By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).</p>
Potential Errors	<p>If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.</p>

	http/https response time
Description	http or https transactions from E1 (client) to E2 (server) - download file or gif.
Purpose	Measure simple TCP response time and / or transaction rate for http requests. Request is 300 bytes, response is 25 kbytes which is size of typical web page.
Available Options	<ul style="list-style-type: none"> • Test duration • Test bit rate • http format (txt or gif)
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)

	http/https response time
Advanced Information	Synthetic transactions are simulated between E1 and E2 reproducing http or https traffic with same network pattern and footprint to measure network capability to transport this type of traffic.
Results interpretation	The response time is the expected time to transfer web page. By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	pop3/smtp response time
Description	pop3 or smtp transactions from E1 (client) to E2 (server) - download file or gif.
Purpose	Measure simple TCP response time and / or transaction rate for pop3 or smtp requests. E1 is email client, E2 is email server. The traffic reproduces synthetic transactions.
Available Options	<ul style="list-style-type: none"> • Test duration • Test bit rate
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)
Advanced Information	Synthetic transactions are simulated between E1 and E2 reproducing pop3 or smtp traffic with same network pattern and footprint to measure network capability to transport this type of traffic.
Results interpretation	The response time is the expected time to transfer email. By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures

	pop3/smtp response time
	complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	ftp response time
Description	ftp transactions from E1 (client) to E2 (server) - download or upload file of 100kbytes.
Purpose	Measure simple TCP response time and / or transaction rate for FTP requests. E1 is ftp client, E2 is ftp server. The traffic reproduces synthetic transactions.
Available Options	<ul style="list-style-type: none"> • Test duration • Test bit rate • ftp get or ftp put
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)
Advanced Information	<p>Synthetic transactions are simulated between E1 and E2 reproducing ftp traffic with same network pattern and footprint to measure network capability to transport this type of traffic.</p> <p>File size for transactions is 100 kbytes.</p>
Results interpretation	<p>The response time is the expected time to transfer ftp file.</p> <p>By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).</p>
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	DNS response time
Description	DNS transactions from E1 (client) to E2 (server).

	DNS response time
Purpose	Measure simple TCP response time and / or transaction rate for DNS requests. E1 is DNS client, E2 is DNS server. The traffic reproduces synthetic transactions.
Available Options	<ul style="list-style-type: none"> • Test duration • Test bit rate
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)
Advanced Information	Synthetic transactions are simulated between E1 and E2 reproducing DNS queries with same network pattern and footprint to measure network capability to transport this type of traffic.
Results interpretation	<p>The response time is the expected time to accomplish DNS request.</p> <p>By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).</p>
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	Exchange traffic
Description	Exchange protocol transactions from E1 (client) to E2 (email server).
Purpose	Measure simple Exchange transactions based on sending and receiving traffic from remote site to central site hosting server.
Available Options	<ul style="list-style-type: none"> • Number of users • Send traffic bitrate • Receive traffic bitrate • Emails size (sent) • Emails size (Received) <div>NOTE The total throughput is distributed amongst number of users !</div>
Metrics	<ul style="list-style-type: none"> • Per traffic type (sent or received)

	Exchange traffic
	<ul style="list-style-type: none"> • Response time Average (ms) • throughput total transactions (Mbps) - bidirectional throughput • Transaction rate (per second) • Total bytes sent and received
Advanced Information	Synthetic transactions are simulated between E1 and E2 reproducing Exchange messages sent and received. The maximum throughput is the limit set to allow this traffic to go through on each direction.
Results interpretation	<p>The response time is the expected time to transfer email or received.</p> <p>By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).</p>
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	SIP response time
Description	SIP protocol transactions from E1 (caller) to E2 (call server).
Purpose	Measure simple TCP response time and / or transaction rate for SIP requests. E1 is SIP client, E2 is SIP server. The traffic reproduces synthetic transactions that are representative of typical SIP based functions.
Available Options	<ul style="list-style-type: none"> • Test duration • Test bit rate • type of SIP transactions
Metrics	<ul style="list-style-type: none"> • Response time Average (ms) • Throughput (Mbps) • Transaction rate (per second)
Advanced Information	Synthetic transactions are simulated between E1 and E2 reproducing SIP transactions with same network pattern and footprint to measure network capability to transport this type of traffic.
Results	The response time is the expected time to accomplish SIP transaction.

	SIP response time
interpretation	By default no objective is set to throughput : any result is good enough as total throughput should reflect response time and transaction rate (transaction rate is 1/response time).
Potential Errors	If the configured bitrate is set too high compared to expected line capacity, this might result in the test not able to accomplish first measurement. This would result in an error with time out ("Some pairs in tests failures complete"). If results cannot be collected Check that port in use is in range (see "preferences/Traffic Port Management/Destination Port Conf Option" and "preferences/Traffic Port Management/First Destination Port" so that correct destination port for test traffic is used.

	Multicast video over RTP
Description	Broadcast of RTP (over UDP) video stream to single.
Purpose	Broadcast of video stream to single (node to node test) or multiple probes (hub and spoke mesh test).
Available Options	Define multicast source IP address and port. Configure stream bit rate.
Metrics	<ul style="list-style-type: none"> • Datagrams out of order • Delay • Jitter • Loss throughput video rate • Total bytes lost
Advanced Information	Can be used for N2N or Mesh tests.Only available for hub and spoke mesh.
Results interpretation	Confirm all probes receive video stream at acceptable rate and quality.
Potential Errors	Port blocked errors.

	Speedtest from->to
Description	Determines average speed between two endpoints in one direction (upload).
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average

	Speedtest from->to
	throughput is reported.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction
Advanced Information	If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate. The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection. As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test. During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

	Speedtest to->from
Description	Determines average speed between two endpoints in one direction (download).
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address

	Speedtest to->from
	<ul style="list-style-type: none"> • Average TCP throughput (Mbps) in one direction
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test.</p> <p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.</p>
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

	Speedtest bidir
Description	Determines average speed between two endpoints in both directions.
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request</p>

	Speedtest bidir
	<p>more chunks throughout the duration of the test.</p> <p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.</p>
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

	Speedtest from->to 2 COS
Description	Determines average speed between two endpoints in one direction (download) using two Class of Service (COS) TCP streams.
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported. Each of the two TCP streams will be using a different QOS setting impacting priority of data packets and across the network which will be reflected in throughput.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction for each COS
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test.</p> <p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.</p> <p>The lower the COS number the lower the priority of the TCP stream (QOS).</p>

	Speedtest from->to 2 COS
	<p>The software endpoint is dependent upon endpoint base OS to add COS to IPv4 packets and it is possible the base OS (particularly if windows) will not always do this. Additionally, COS is layer 2 traffic, just the ToS 1 byte value in the IP header.</p> <div> NOTE QOS is layer 3 traffic where COS and traffic type are both taken into consideration. </div>
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

	Speedtest from->to 3 COS
Description	Determines average speed between two endpoints in one direction (download) using three Class of Service (COS) TCP streams.
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported. Each of the three TCP streams will be using a different QOS setting impacting priority of data packets and across the network which will be reflected in throughput.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction for each COS
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over a TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test.</p> <p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.</p>

Speedtest from->to 3 COS	
	<p>The lower the COS number the lower the priority of the TCP stream (QOS). The software endpoint is dependent upon endpoint base OS to add COS to IPv4 packets and it is possible the base OS (particularly if windows) will not always do this. Additionally, COS is layer 2 traffic, just the ToS 1 byte value in the IP header.</p> <p>NOTE QOS is layer 3 traffic where COS and traffic type are both taken into consideration.</p>
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

Speedtest from->to 4 COS	
Description	Determines average speed between two endpoints in one direction (download) using four Class of Service (COS).
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported. Each of the four TCP streams will be using a different QOS setting impacting priority of data packets and across the network which will be reflected in throughput.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction for each COS
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test.</p> <p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads</p>

Speedtest from->to 4 COS	
	<p>are required to more accurately measure the throughput speed.</p> <p>The lower the COS number the lower the priority of the TCP stream (QOS).</p> <p>The software endpoint is dependent upon endpoint base OS to add COS to ipv4 packets and it is possible the base OS (particularly if windows) will not always do this. Additionally, COS is layer 2 traffic, just the ToS 1 byte value in the IP header.</p> <div> NOTE QOS is layer 3 traffic where COS and traffic type are both taken into consideration. </div>
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

Speedtest from->to 5 COS	
Description	Determines average speed between two endpoints in one direction (download) using five Class of Service (COS).
Purpose	Performs TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported. Each of the five TCP streams will be using a different QOS setting impacting priority of data packets and across the network which will be reflected in throughput.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction for each COS
Advanced Information	<p>If the test duration is too short the time taken to ramp up TCP throughput will reflect in a lower average throughput rate.</p> <p>The endpoint establishes multiple connections with the server over TCP port. An initial chunk of data is sent. The endpoint then adjusts the chunk size and buffer size based on TCP metrics to maximize usage of the network connection.</p> <p>As the chunks are received by the other endpoint, the endpoint will request more chunks throughout the duration of the test.</p>

	Speedtest from->to 5 COS
	<p>During the initial stages of the test, the endpoint will establish extra TCP connections (streams) to the other endpoint if it determines additional threads are required to more accurately measure the throughput speed.</p> <p>The lower the COS number the lower the priority of the TCP stream (QOS).</p> <p>The software endpoint is dependent upon endpoint base OS to add COS to ipv4 packets and it is possible the base OS (particularly if windows) will not always do this. Additionally, COS is layer 2 traffic, just the ToS 1 byte value in the IP header.</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">NOTE</div> QOS is layer 3 traffic where COS and traffic type are both taken into consideration.
Results interpretation	Speed test between endpoints.
Potential Errors	See Common Errors - Real Services.

	Speedtest from->to with KPI
Description	Speedtest along with network KPI measures speed with TCP + latency/jitter/loss with RTP/UDP packets. It determines average speed between two endpoints in one direction (upload), along with the test network delivery KPI with low footprint (100 Mbps) and 50 packets per second—from E1 to E2 direction.
Purpose	The purpose of this test is to perform TCP traffic using several TCP pairs. The test attempts to generate as much TCP throughput as possible using several TCP streams. The average throughput is reported during the test. While the throughput test is run, key KPI loss/jitter/latency are also measured.
Available Options	<ul style="list-style-type: none"> • Test duration (sec) • Specify which QOS (DSCP setting) to request between switches in network • Number of pairs
Metrics	<ul style="list-style-type: none"> • Identifies from IP address • Identifies to IP address • Average TCP throughput (Mbps) in one direction <p>Network KPI Metrics:</p> <ul style="list-style-type: none"> • One way delay (ms) • Jitter (ms) • Max jitter (ms)

	Speedtest from->to with KPI
	<ul style="list-style-type: none"> • Loss (%) • Voice MOS score • Packet loss burst • Max delay variation(ms)
Advanced Information	<p>If the test duration is too short, the time taken to ramp up TCP throughput reflects in a lower average throughput rate. The endpoint establishes multiple connections with the server over TCP port. An initial set of data is sent. The endpoint then adjusts the data size and buffer size based on the TCP metrics to maximize usage of the network connection. As the data set is received by the other endpoint, the endpoint requests more data sets throughout the duration of the test. During the initial stages of the test, the endpoint establishes extra TCP connections (streams) to the other endpoint; if it determines that additional threads are required to more accurately measure the throughput speed.</p> <p>This test generates unidirectional traffic with heartbeats to measure the key metrics. The traffic is like voice traffic—MOS score is an indicator of capacity of the link to transport voice in a good quality.</p> <p>The following definitions help you to understand key metrics:</p> <ul style="list-style-type: none"> • Max delay variation: The time from when a packet is sent from a probe to when it is received, end to end, is the delay. The max delay variation is the difference between the shortest time and the longest time for this end to end delay for exchanging the packets. • Max jitter: This parameter measures the variance in spacing between packets sent end to end. If the difference in time (spacing) between 1st and 2nd packet sent from the first probe is 2 ms, and the time on far end probe receiving 1st and 2nd packets is 3.7 ms, the jitter is $(3.7-2)$ ms = 1.7 ms.
Results interpretation	<p>Speed test between endpoints:</p> <ul style="list-style-type: none"> • The network KPI pair generates packets in RTP stream. • These packets traverse the network from one probe to the other and provides indication based on the time sent and received, how many are lost and so on. • The packets are sent similarly to a G711 voice stream, because this behavior is expected to be a key application of the network's ability to transport. • Voice MOS score gives an indication of the quality of transport network for voice G711 application.
Potential Errors	<p>If test result pair cannot be collected:</p> <ul style="list-style-type: none"> • Check that your E2 endpoint can open 10115 port toward E1 for management (this is needed for stream pairs).

Speedtest from->to with KPI

- Check that synchronization port between pairs is opened (management UDP 10115).
- Check that port in use is in range (see "preferences/Test Controller/Destination Port Conf Option" and "preferences/Test Controller/First Destination Port" so that correct destination port for test traffic is used.

Also see [Common Errors – N2N](#).

DSCP (QOS) Settings Explained

Hawkeye implements Class of Service based on DSCP setting. The following table details table name and different settings (as explained in following section) correspondence.

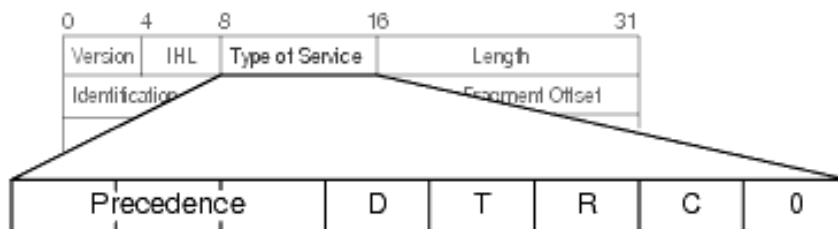
DS CP Class	DSCP (bin)	DSCP (hex)	DSCP (dec)	ToS (dec)	ToS (hex)	ToS (bin)	ToS Pre c. (bin)	ToS Pre c. (dec)	ToS Del ay Flag	ToS Throg hput Flag	ToS Reliab ility Flag	TOS String Format
none	000000	0x00	0	0	0x00	00000000	000	0	0	0	0	Routine
cs1	001000	0x08	8	32	0x20	00100000	001	1	0	0	0	Priority
af11	001010	0x0A	10	40	0x28	00101000	001	1	0	1	0	Priority
af12	001100	0x0C	12	48	0x30	00111000	001	1	1	0	0	Priority
af13	001110	0x0E	14	56	0x38	00111100	001	1	1	1	0	Priority
cs2	010000	0x10	16	64	0x40	01000000	010	2	0	0	0	Immediate
af21	010010	0x12	18	72	0x48	01001000	010	2	0	1	0	Immediate
af22	010100	0x14	20	80	0x50	01010000	010	2	1	0	0	Immediate
af23	010110	0x16	22	88	0x58	01011000	010	2	1	1	0	Immediate
cs3	011000	0x18	24	96	0x60	01100000	011	3	0	0	0	Flash

af3 1	011 010	0× 1A	26	104	0× 68	01101 000	011	3	0	1	0	Flash
af3 2	011 100	0× 1C	28	112	0× 70	01110 000	011	3	1	0	0	Flash
af3 3	011 110	0× 1E	30	120	0× 78	01111 000	011	3	1	1	0	Flash
cs4	100 000	0× 20	32	128	0× 80	10000 000	100	4	0	0	0	FlashOverri de
af4 1	100 010	0× 22	34	136	0× 88	10001 000	100	4	0	1	0	FlashOverri de
af4 2	100 100	0× 34	36	144	0× 90	10010 000	100	4	1	0	0	FlashOverri de
af4 3	100 110	0× 26	38	152	0× 98	10011 000	100	4	1	1	0	FlashOverri de
cs5	101 000	0× 28	40	160	0xA 0	10100 000	101	5	0	0	0	Critical
ef	101 110	0× 2E	46	184	0xB 8	10111 000	101	5	1	1	0	Critical
cs6	110 000	0× 30	48	192	0xC 0	11000 000	110	6	0	0	0	Internetwork control
cs7	111 000	0× 38	56	224	0xE 0	11100 000	111	7	0	0	0	Networkcon trol

Details on Class of Service - Different Standards

IP TOS

The type-of-service (TOS) byte in an IP header specifies traffic precedence and type of service (as defined in RFC 791 and RFC 1349). Figure 9-1 shows the TOS byte in the IP header.



The precedence field comprises the first three bits and supports eight levels of priority. The lowest priority is 0, the highest is 7 (values 6 and 7 are reserved for network control packets).

The precedence field setting

Precedence	Bit Setting	Description
Network Control	111	Intended for intranetwork use only. Lowest drop preference.
Internetwork Control	110	Intended for use by gateway control originators.
CRITIC/ECP	101	A priority setting for voice data.
Flash Override	100	Network-specific setting; generally means "maximize throughput."
Flash	011	Network-specific setting.
Immediate	010	Network-specific setting; generally means "maximize reliability."
Priority	001	Network-specific setting; generally means "low maximum delay," for real-time traffic.
Routine	000	Roughly corresponds to Best Effort Service. Highest drop preference.

The four bits following the precedence field specify the type of service. Only one of these bits can be enabled at one time. Each bit defines the desired type of service:

- D – The delay bit instructs network devices to choose high speed to minimize delay.
- T – The throughput bit specifies high capacity links to ensure high throughput.
- R – The reliability bit specifies that reliable links should be used to minimize data loss.
- C – The cost bit specifies that data transmission should be accomplished at minimal cost.

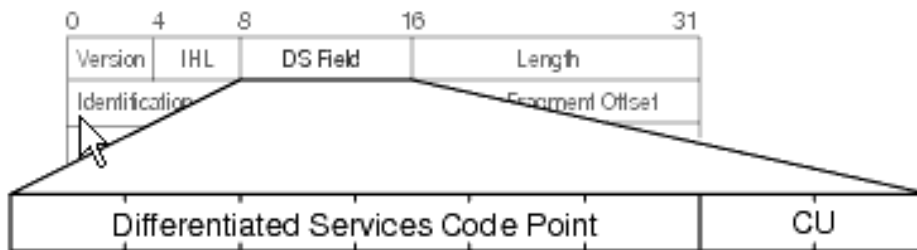
The last bit in the TOS byte is reserved and is always set to 0.

NOTE

On Microsoft Windows Server 2008 (32- and 64-bit) and on Microsoft Windows Vista (32- and 64-bit), IP TOS can be set only via qWave templates. If endpoints are used on these types of Operating systems, qwave needs to be installed so that the endpoint can tag with correct TOS.

DiffServ

Differentiated Services (DiffServ) is a QoS model defined by the IETF for IP networks (refer to RFC 2474). This model is designed to be scalable and to provide consistent service classes independent of application. DiffServ redefines the TOS byte of the IP header (see Figure 9-1) as the DS field.



The first six bits of the DS field are used as a differentiated service code point (DSCP), and the last two bits are currently unused (CU).

In the DiffServ QoS model, traffic is classified by marking the DS field with a DSCP value. Queuing mechanisms provide differentiated forwarding of the traffic at each hop, based on the DSCP value.

NOTE

On Microsoft Windows Server 2008 (32- and 64-bit) and on Microsoft Windows Vista (32- and 64-bit), IP TOS can be set only via qWave templates. If endpoints are used on these types of Operating systems, qwave needs to be installed so that the endpoint can tag with correct DSCP.

Per-Hop Behavior (PHB)

The DSCP selects the Per-Hop Behavior (PHB) that a packet experiences at each node. RFC 2474 defines PHB as the externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ Behavior Aggregate.

There are currently four standard PHBs:

- Default ("Best Effort") PHB (as defined in RFC 2474)
- Class-Selector PHB (as defined in RFC 2474)
- Assured Forwarding (AF) PHB (as defined in RFC 2597)
- Expedited Forwarding (EF) PHB (as defined in RFC 2598).

Default PHB

RFC 2474 recommends codepoint 000000 as the Default PHB.

Class-Selector PHBs

RFC 2474 defines 21 codepoints, including the Class-Selector PHBs listed below:

Class Selector Name	DS Field Bit Value
CS0	000 000
CS1	001 000
CS2	010 000
CS3	011 000
CS4	100 000
CS5	101 000
CS6	110 000
CS7	111 000

Assured Forwarding (AF) PHB

The Assured Forwarding (AF) PHB group provides delivery of IP packets in N independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of M different levels of drop precedence. Currently, four classes with three levels of drop precedence in each class are defined for general use. (Additional AF classes or levels of drop precedence may be defined for local use.)

RFC 2597 recommends the codepoints described below.

	AF Class 1	AF Class 2	AF Class 3	AF Class 4
Low Drop Prec	001010	010010	011010	100010
Medium Drop Prec	001100	010100	011100	100100
High Drop Prec	001110	010110	011110	100110

This table shows each of the AFMN bit values, where M is the AF class and N is the drop precedence. In list form, these are:

- AF11 = 001010
- AF12 = 001100
- AF13 = 001110
- AF21 = 010010
- AF22 = 010100
- AF23 = 010110
- AF31 = 011010
- AF32 = 011100
- AF33 = 011110
- AF41 = 100010
- AF42 = 100100
- AF43 = 100110

Expedited Forwarding (EF) PHB

RFC 2598 defines the EF PHB as a PHB that can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS domains. RFC 2598 recommends codepoint 101110 as the default EF PHB.

Common Errors - N2N

Errors Received for Node-to-Node and Mesh Tests

If you encounter problems while running node-to-node and mesh tests, they're probably related to failed connections, to the communications software in your network, or to the way you've configured your tests. Hawkeye messages offer information to help you understand why errors occur and guidance to help you avoid them in the future.

The following topics will help you find the information necessary to solve problems you encounter.

Investigate which Probe Detected the Error

The first step in troubleshooting is usually determining which probe detected the error. All Operator Actions described by the message help should be taken at the computer that detected the error, unless otherwise specified.

For most errors involving setup and file manipulation, the Test Agent is the computer that detects the error.

For errors that occur while running a test, the error could have been detected on a particular endpoint pair by the Test Agent, by Endpoint 1, or by Endpoint 2. The program that detects the error reports to the Test Agent, which shows the error and logs it. The first line of the Test Agent error message tells which endpoint probe detected the error.

If for some reason you cannot see the error at the Test Agent, examine the error log at the endpoints involved in the problem. A formatted error log entry should contain a line that resembles the following:

Some pairs in tests did not complete.

One of the following reasons explains the situation:

- Hawkeye test engine started the test but had to abandon at result collection
- Your test generates too much traffic on the link and the first result collection is never happening as result collection intervals depend on requested traffic : this would result into Hawkeye timing out test execution.
=> Solution: Start a test with low traffic between endpoints.
- Check firewall NAT rules between endpoints : this can be test path not opened on ports, can be E2 unable to reach E1 on port 10115 (you need that for the tests).
=> Solution: open relevant ports. Force user traffic to use specific port from Hawkeye (preferences, test agent tab)
- Endpoint process in bad state : this happens sometimes on linux when there was a problem with a test.
Solution=> Restart the endpoint process on the probes (/etc/init.d/endpoint stop; /etc/init.d/endpoint stop). For hardware probes you can do that from the probe management / probe remote management menu of Hawkeye. There is also an automatic endpoint cleanup process that would do that every hour per default. A hard reboot on the probe also does the job.
- Hawkeye test engine gets stuck at test initialization stage.
- Port 10115 udp must be opened both ways between probes for sync.
- Endpoint process in bad state: same solution than above.

Error was detected by Endpoint 1

If the error was detected by Endpoint 1 or Endpoint 2, check the test setup at the Test Agent to determine the actual network address of the probe where the error was detected.

Although one probe may detect an error, the solution may actually lie elsewhere. For example, if Endpoint 1 detects an error indicating that a network connection could not be established, it may be because of a configuration error in the middle of the network at Endpoint 2, or between Endpoint 1 and Endpoint 2.

Reading Error Messages

Hawkeye errors are reported in the GUI in the "Reason cause" column of the "Test results list" table. Below is an example of error received when one of the test ports was used by another application:

Status	Reason Cause
Status	Reason Cause
Error	Error was detected at Thu Jan 1 08:17:32 1970- Error was received at Tue Feb 26 19:51:56 2013- Error was detected by the Endpoint 2.-The return code was 3.-CHR0264: Port number 10116 is already in use or access denied.-The info message was:-CHR0316: Error working with the test file .- Pair 1- localhost to 10.205.14.62-

- The first line of the error message shows the timestamp when the error was detected and received;
- The next lines tell you which endpoint detected the error, the error number and error explanation together with other error details.

Below, is an explanation of the error codes received in Hawkeye, when running node-to-node or mesh tests:

Code	Type	Reason
CHR0200	Error	Connection attempt timed out
CHR0204	Error	No endpoint program is installed on partner computer/probe.
CHR0206	Error	Cannot complete scripts because the assigned port is already in use.
CHR0225	Error	The TCP address is unreachable- the endpoint or phone is unavailable. Check connectivity to the endpoint.
CHR0264	Error	RUNTST cannot run while the Test Agent is loaded. The RUNTST program is installed at the Test Agent in the \Ixia\Hawkeyegram folder.
CHR0335	Warning	A timing record was received with a measured time of 0 milliseconds. A script command was performed in less than one millisecond, an insignificant amount of time.
CHR0336	Warning	A timing record was received with a measured time between 1 and 20 milliseconds. The clock timers used in timing scripts are generally accurate to within 1 millisecond (ms). For most tests, this is more than sufficient, but if the transactions in a test are too short, problems may arise.
CHR0337	Warning	More than 500 timing records per pair were generated in Batch Reporting Mode. Excessive timing records create extra traffic on the line and interfere with performance results.

CHR0338	Warning	The test has run for less than 1 second while collecting endpoint CPU utilization. Meaningful data on CPU utilization at the endpoints cannot be collected unless the test runs for a longer period of time.
---------	---------	--

Common Problems

High-Precision Timer (CHR0359 error)

If you attempt to execute a VoIP or streaming pair test and you receive a CHR0359 error message (An error was detected in the high precision timer), you may be able to resolve the issue by following the instructions given in the Microsoft Knowledge Base article entitled "Programs that use the QueryPerformanceCounter function may perform poorly in Windows Server 2000, in Windows Server 2003, and in Windows XP". You can either search for the article by name or reference it at this address: <http://support.microsoft.com/kb/895980>.

Insufficient Resources

If you receive an Insufficient Resource error while running node-to-node/mesh tests, the test agent computer does not have access to the amount of memory required to successfully run these tests. Close other applications that currently run and restart the tests.

Insufficient Threads

The Hawkeye Test Agent creates one or more threads for each endpoint pair when running a test. This is in addition to the threads created by the underlying network software (as well as those used by other concurrently-running applications).

In our testing, we did not exhaust threads in our default settings for Windows NT or Windows 2000/2003 until we reached about 7000 threads. We don't believe you'll encounter out-of-threads problems, but please let us know if you do.

Protection Faults and Traps

Protection faults or traps are the operating system's way of telling you when a program is trying to use memory that it doesn't own. They can occur in an Hawkeyegram, in any library routines called by Hawkeye, or in the operating system itself. The default way that they're handled is with a message box. This message box shows program instruction values in hex, which aren't helpful to you as a user.

- If you are using Windows NT, Windows 2000/2003, or Windows XP:

Windows NT, Windows 2000/2003, and Windows XP write an entry to a file named drwtsn32.log when they encounter a trap or protection fault. This file is written to the directory where you installed Windows. Its default location is c:\Winnt. It contains information that is immensely helpful to us in finding and fixing bugs. When you contact the Technical Support team, they may suggest that you send the Dr. Watson file to us via email.

Default Number of Tests per Probe Type (N2N)

Queue Management Concept

While trying to execute the tests configured by the users and scheduled on the system, the scheduler will follow following rules:

- pick first tests that are earlier in Next Execution time
- give priority to Mesh tests in Meshes that are left to complete (see Mesh tests for details)
- give priority to One shot tests over scheduled tests
- Check probe execution capability and:
 - do not allow to run 2 different test types at the same time on same probe
 - allow running simultaneous tests on same probe only in same test run (once a probe is running it cannot be used for other tests even if this is same test type.
 - max total number of tests per probe depends on probe type and test type. See table below.

How is a Probe Identified

A probe is by default identified by its Serial Number. If this is empty and Use probe Management IP is defined (should be default), probes with same management IP will be identified as sharing same hardware.

	Parameter Name	Value	Description	Details (Current Setting)
Main	Real Test Max Duration	1200	Maximum duration of a real test	
GUI	Probe Health Check	1 ▼	Enable/disable the probe health check engine	Probe health check engine is ENABLED
Alarms	Test E2 Available	1 ▼	Test both Endpoint 1 and endpoint 2 availability from Test controller for the test. In network configuration where Endpoint 2 is not available from test controller it might be useful to disable this test	Testing BOTH endpoint 1 and endpoint 2 availability
Maps	Probe Management identification	1 ▼	Use Probe management IP or probe ID to manage unique probe. Serial number of probe is always used by default when available.	Use Probe Management IP as default identifier for probes (default)
Email	Endpoint Autorestart	1 ▼	Enable/disable the autorestart feature for IxChariot endpoint.	IxChariot endpoint autorestart feature is ENABLED
Traffic Port Management	Endpoint Autorestart Interval (minutes)	360	Interval for the endpoint autorestart time.	
	Autorestart Max Duration	30	Maximum duration of endpoint autorestart	
Test Controller	Real Service Port	22	Port required by the test agent to connect to the probes to run real services test types.	
Advanced Options	Alarm on Probe Status Change	0 ▼	Enable alarms (email or SNMP) when probe becomes not available. Send alarm when status changes (available/not available).	Probe status change (available/not available) alarms are DISABLED
Installation Paths	Alarm on Probe Health Fail	0 ▼	Send an alarm when probe is not available (every check)	Alarms for probe not available are DISABLED
logs	Probe Default Login		Probe default Login - overridden by probe specific configuration	
Test Engine	Probe Default Password		Probe default Password - overridden by probe specific configuration	

This configuration is useful when using several interfaces on same probe and allows to give probe control management.

Maximum number of simultaneous tests per probe type and test type

Table below displays the number of max concurrent tests that are allowed on one probe to run.

These metrics can be modified by advanced administrator - contact support for advise and recommendations.

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR-E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
Adaptive Video	1	1	1	1	1	1	1	1	1

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR- E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
Adaptive video with network quality	1	1	1	1	1	1	1	1	1
Citrix	1	1	1	1	1	1	1	1	1
COS line qualification	1	1	1	1	1	1	1	1	1
DNS Response Time	200	200	20	20	20	20	200	20	20
Exchange_ traffic	1	1	1	1	1	1	1	1	1
Flash RTMP	1	1	1	1	1	1	1	1	1
FTP Response Time	5	5	5	5	5	5	5	5	5
HTTP Test	5	5	5	5	5	5	5	5	5
HTTPS Test	5	5	5	5	5	5	5	5	5
Multicast Video over RTP	1	1	1	1	1	1	1	1	1
Netflix	1	1	1	1	1	1	1	1	1
Network KPI	100	500	50	50	50	50	500	50	50
Network KPI 3 COS	5	125	12	12	12	12	125	12	12
Network KPI Advanced	80	320	32	32	32	32	320	32	32
Network KPI bidirectional	25	250	25	25	25	25	250	25	25
Network KPI Low Bandwidth	50	300	50	50	50	50	300	50	50
Network KPI	100	500	50	50	50	50	500	50	50

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR- E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
to->from									
Network loss performance	10	10	10	10	11	13	10	13	10
POP3 Response Time	5	5	5	5	5	5	5	5	5
RTSP	1	1	1	1	1	1	1	1	1
SIP Response Time	5	5	5	5	5	5	5	5	5
Skype4B Traffic	20	80	8	8	8	8	80	8	8
Skype4B Traffic from- >to	40	160	16	16	16	16	160	16	16
SLA Traffic Mix bidirectional	1	1	1	1	1	1	1	1	1
SMTP Response Time	5	5	5	5	5	5	5	5	5
Speedtest bidirectional	1	1	1	1	1	1	1	1	1
Speedtest from->to	1	1	1	1	1	1	1	1	1
Speedtest from->to 2 COS	1	1	1	1	1	1	1	1	1
Speedtest from->to 3 COS	1	1	1	1	1	1	1	1	1
Speedtest from->to 4 COS	1	1	1	1	1	1	1	1	1
Speedtest	1	1	1	1	1	1	1	1	1

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR- E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
from->to 5 COS									
Speedtest to-> from	1	1	1	1	1	1	1	1	1
Speedtest from->to with KPI	1	1	1	1	1	1	1	1	1
TCP Response Time	200	200	20	20	20	20	200	20	20
TCP Throughput Advanced	1	1	1	1	1	1	1	1	1
TCP Throughput bidirectional	1	1	1	1	1	1	1	1	1
TCP Throughput from->to 1 stream	1	1	1	1	1	1	1	1	1
TCP Throughput from->to N streams	1	1	1	1	1	1	1	1	1
TCP Throughput Optimized Window size	1	1	1	1	1	1	1	1	1
TCP Throughput to->from 1 stream	1	1	1	1	1	1	1	1	1
TCP Throughput to->from N streams	1	1	1	1	1	1	1	1	1
Teams Cloud	1	1	1	1	1	1	1	1	1

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR- E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
Call									
Teams WAN Call	1	1	1	1	1	1	1	1	1
Traffic Mix - HTTP - Video - Voice	1	1	1	1	1	1	1	1	1
UDP Throughput Advanced	1	1	1	1	1	1	1	1	1
UDP Throughput bidirectional	1	1	1	1	1	1	1	1	1
UDP Throughput from->to	1	1	1	1	1	1	1	1	1
UDP Throughput from->to - 4 COS	1	1	1	1	1	1	1	1	1
UDP Throughput from->to N streams	1	1	1	1	1	1	1	1	1
UDP throughput from->to with delay/jitter	1	1	1	1	1	1	1	1	1
UDP Throughput to->from	1	1	1	1	1	1	1	1	1
UDP Throughput to->from N streams	1	1	1	1	1	1	1	1	1
Video Stream	1	1	1	1	1	1	1	1	1

	Software	XR2000 / VM	XRPI	Pi4	XR Docker	XR- E1S	XR VM	XR3000	IxProbe, IxTap, IxByPass *
Voice bidirectional	10	200	20	20	20	20	200	20	20
Voice from- >to	50	500	50	50	50	50	500	50	50
Voice N pairs - UDP Data bidirectional	1	1	1	1	1	1	1	1	1
Voice N Pairs bidirectional	1	1	1	1	1	1	1	1	1
Voice N Pairs Unidirectional	1	10	1	1	1	1	10	1	1
Youtube	1	1	1	1	1	1	1	1	1
Zoom meeting	1	1	1	1	1	1	1	1	1

* The maximum number of simultaneous tests with the Trusted Subnet mode enabled is restricted to one.

N2N license cost per Test Types

When considering how many licenses will be required for a User's Hawkeye system, it is important to understand the number of simultaneously running/active users is licensed. Several Node to Node tests require more than one license to run a single test. The table below lists the number of pairs that are required to execute the test based on test types.

Adaptive video	1
Adaptive video + quality	1
COS line qualification	10
DNS Response Time	1
Exchange_traffic	2
Flash RTMP	1
FTP Response Time	1
HTTP Test	1

HTTPS Test	1
Lync Traffic	4
Lync Traffic from->to	2
Multicast video over RTP	1
Netflix	1
Network KPI	1
Network KPI 3 COS	3
Network KPI Advanced	1
Network KPI bidirectionnal	2
Network KPI low bw	1
Network KPI Upstream	1
Network Loss Performance	1
POP3 Response Time	1
SIP Response Time	1
SMTP Response Time	1
Speedtest	1
Speedtest Bidirectional	2
Speedtest N COS M pair	N x M
TCP Response Time	1
TCP Throughput Advanced	1
TCP Throughput bidirectional	2
TCP Throughput from->to 1 stream	1
TCP Throughput from->to N streams	2
TCP Throughput Optimized Window size	1
TCP Throughput to->from 1 stream	1
TCP Throughput to->from N streams	N
Traffic Mix - HTTP - Video - Voice	3

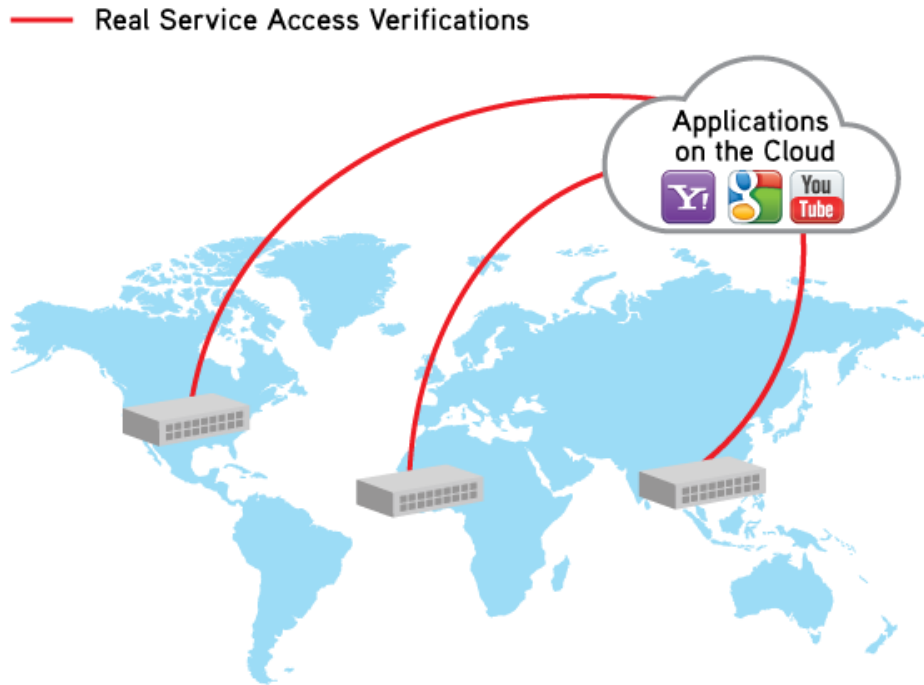
UDP Throughput Advanced	1
UDP Throughput bidirectional	2
UDP Throughput from->to	1
UDP Throughput from->to - 4 COS	4
UDP Throughput to->from	1
Video Stream	1
Voice bidirectional	2
Voice from->to	1
Voice N pairs - UDP Data bidirectional	$N+1$
Voice N Pairs bidirectional	$2N$
Voice N Pairs Unidirectional	N
Youtube (N streams)	N

Real Services

Real service testing is performed between the testing probe (acting as a client) and a server on the network, most of the time in the public Internet.

The probe will access the service and compute key performance indicators for the test.

These tests perform application performance testing: they measure network quality but also application performance.



For distributed sites real service testing, the following endpoints support real service tests:

- [xr2000 hardware endpoint](#)
- [xrpi2 hardware endpoint](#)
- [xr2000 virtual probe in virtual machine](#)

Prerequisites

It is also important to take into account that a lot of the real service tests are done to the public services, therefore they will only be available if the endpoint has access to public internet. DNS settings are set so that public IP addresses can be resolved.

Test types

You can create test details for Real Service through the following test forms:

- [Continuous](#)
- [Advanced](#)

Licensing

The number of Real Services test license features limits the ability to run the Real Service tests. This license count is consumed differently depending on whether a continuous real service test is scheduled or an advanced real service test is running.

Continuous

Continuous Real Service tests consume a real service license for every 20 continuous results per minute. The license is consumed for as long as the test is configured. The algorithm used for calculating Real Service License consumption is given below:

(Number of probes running the test) x (Number of Destinations per probe) x (60 divided by results frequency in seconds)

Following example shows how Continuous real service consume licenses.

Example

Assume TCP Echo test is configured on 3 probes. Each probe tests 5 destinations and results are collected every 90 seconds.

$$3 \times 5 \times (60/90) = 10 \text{ results per minute}$$

This configuration will consume 1 real service license.

NOTE

If the above count was 10.344, Hawkeye would round it off to 10. Counts greater than 10.5 will be round off to 11.

Advanced

Advanced Real Service tests consume 1 Real Service license count while a given test execution is actively in the running state.

Continuous

Ping	
Description	The continuous ping tests to a destination URL or another endpoint.
Purpose	This test is used to continually check the availability of the destination and measure Round Trip Time (RTT).
Available Options	<ul style="list-style-type: none"> • IPv6 • Interval Between Pings (ms) • Packets Per Result • Packet Size • DSCPT • imeout(ms) • TTL • Local Source Address

Ping	
	<div>NOTE</div> <p>The results cannot be reported on an interval less than 2 minutes. Example: 1000 ms Interval Between Pings with 120 Packets Per Result means one result reported to the server every 120 seconds.</p>
Metrics	<ul style="list-style-type: none"> • Average, Max, Min and standard deviation for Round Trip Times (RTT) • TTL • Packet loss rate • Packets sent/received
Advanced Information	<p>This test sends ICMP packets and listens for responses.</p> <div>NOTE</div> <p>Up to 10 destinations can be selected for each endpoint.</p>
Results interpretation	<p>The ICMP packets detect any obvious issues on the network (congestions, drops, long response time, instable response time). It is an interesting data point, because a change in the average of an ICMP test likely reflects some modification of the network average. The results must however be interpreted with care, because the ICMP packets are usually treated with lower priority than data packets by network elements. Therefore, this treatment can result in worst behavior than actual user traffic (prioritized) experiences in some cases.</p>
Potential Errors	<p>See Common Errors - Real Services.htm.</p>

Web Page Download	
Description	<p>The continuous HTTP request packets sent to a destination URL. Up to 10 destinations can be selected for each endpoint.</p>
Purpose	<p>To configure test once, so that the endpoint continuously reports test results.</p>
Available Options	<ul style="list-style-type: none"> • Interval Between Tests • IPv6 • DNS Server • Proxy Server • Proxy Username • Proxy Password • CA Certificate • Client Certificate • Client Key

Web Page Download	
	<ul style="list-style-type: none"> • Client Password • User Agent
Metrics	<ul style="list-style-type: none"> • Average connect time • DNS resolution time • Min/average download rate • Max connect time • Max SSL time • Max time to first byte • The number of files downloaded • Overall download rate/size/time
Advanced Information	<p>This test downloads elements in a web page providing user experience in getting information from the associated URL.</p> <p>NOTE Up to 10 destinations can be selected for each endpoint.</p> <ul style="list-style-type: none"> • CA Certificate is used to verify the peer. If no certificate is entered in the CA Certificate, Peer Certificate Authentication is not performed. • Client Certificate is used to validate the identity of a client (user). It works as a password without any intervention or input from the user. In this way, the server makes sure that it is connecting to the permitted user and the connection is safe to communicate with. • Client Key is the Private Key associated with the Client Certificate. • Client Password is the password for the Client Key. <p>NOTE The Client Certificate and the Client Key can be concatenated into one file and entered into the Client Certificate.</p> <p>To move certificates into the Hawkeye system, use the Upload Files button. This will allow the user to upload file types: pem, key, and crt. Certificates can also be removed from the Hawkeye system from the Upload Files window.</p> <p>After certificates have been moved to the Hawkeye system, they will appear in the certificate Select file pulldown selection menus.</p>
Results interpretation	The result must be reflective as the user experience getting from a browser to the web page.
Potential Errors	See Common Errors - Real Services.htm.

Wi-Fi	
Description	Gathers wireless information on wireless interface of endpoint. No traffic is generated.
Purpose	To configure test once, so that the endpoint continuously reports WIFI information.
Available Options	Interval Between Tests
Metrics	<ul style="list-style-type: none"> • Wifi Available • Wi-Fi Channel • Wi-Fi Frequency • Wi-Fi Link Speed • Wi-Fi RSSI
Advanced Information	Data is collected about the current Wi-Fi Connection.
Results interpretation	RSSI is not reported in dbm. This signal Quality metric is dependent on the wifi device manufacturer. The general rule — higher the RSSI, better is the signal quality.
Potential Errors	See Common Errors - Real Services.htm.

Echo TCP	
Description	Echo TCP tests the operation of echo port at the server. It sends TCP packets of a configured size to a destination (server) on a specified port. It possesses ability to use port other than the standard echo port 7.
Purpose	To configure test once, so that the endpoint continuously reports Echo TCP test metrics.
Available Options	<ul style="list-style-type: none"> • IPv6 • Port • Interval Between Packets (ms) • Packets Per Result • DSCP <div style="background-color: #cccccc; padding: 5px; display: inline-block; margin-top: 10px;">NOTE</div> The results cannot be reported on an interval less than 2 minutes. Example: 1000 ms Interval Between Pings with 120 Packets Per Result means one result reported to the server every 120 seconds.

Echo TCP	
Metrics	<ul style="list-style-type: none"> • Total bytes sent/received • Total packets sent/received • Min/Avg/Max RTT • Packet loss rate • Total time
Advanced Information	<p>This test sends TCP SYN packets and listens for SYNACK responses.</p> <p>NOTE Up to 10 destinations can be selected for each endpoint.</p>
Results interpretation	The TCP response round trip and packet loss provides good information about the network transport to TCP remote ends.
Potential Errors	See Common Errors - Real Services.htm.

Echo UDP	
Description	Echo UDP tests the operation of echo port at the destination Server. It sends UDP packets of a configured size to a destination (server) on a specified port. It possesses ability to use port other than the standard echo port 7.
Purpose	To configure test once, so that the endpoint continuously reports Echo UDP metrics.
Available Options	<ul style="list-style-type: none"> • IPv6 • Port • Interval Between Packets (ms) • Packets Per Result • DSCP <p>NOTE Results cannot be reported on an interval less than 2 minutes. Example: 1000 ms Interval Between Pings with 120 Packets Per Result means one result reported to the server every 120 seconds.</p>
Metrics	<ul style="list-style-type: none"> • Total bytes sent/received • Total packets sent/received • Min/Avg/Max RTT • Packet loss rate • Total time
Advanced	This test sends UDP packets and listens for UDP packet responses.

Echo UDP	
Information	NOTE Up to 10 destinations can be selected for each endpoint.
Results interpretation	The UDP response round trip and packet loss provides good information about the network transport to UDP remote ends.
Potential Errors	See Common Errors - Real Services.htm.

Advanced

	Bittorrent test
Description	Start Downloading a torrent from torrent client- THIS TEST IS ONLY SUPPORTED ON XR2000, NOT ON XRPI
Purpose	Measures Throughput at which a file can be downloaded from a peer-to-peer network.
Available Options	<ul style="list-style-type: none"> • Torrent name (simply for display reasons, not used in test) • magnet link: is the torrent file url that the probe needs to download to get access to torrent <p>Test duration: torrent download duration - after this duration torrent download will stop and result printed out even if torrent is not fully downloaded.</p>
Metrics	<ul style="list-style-type: none"> • downloaded Size: size downloaded during allocated time • Filename: name of the file associated to torrent • Filesize: file size as published by the torrent • Throughput: throughput rate during the time allocated for download
Advanced Information	<p>This test aims at proving capability to do peer to peer traffic from the probe and identify the relevant max throughput.</p> <p>It is recommended to use popular torrent files so that the results are significant.</p>
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	Cloud Test - AWS
Principles	This test verifies key metrics to access AWS (Amazon Web Services) cloud.

	Cloud Test - AWS
	<p>AWS has different regions that can host servers and services. Having good network connectivity from the edge to these data centers is often paramount to the service experience delivered for internal application that is self hosted on Amazon, or for external applications (SaaS) hosted on the cloud. Through this test, you can have monitoring capabilities with network performance characterization from the endpoint to the Cloud. This capability is independent of any potential application responsiveness problems; because the measured performance is purely network related from the endpoint (typically deployed at the edge or at the service delivery location, remote site, home environment, and so on) and the Amazon data center edge.</p> <p>Key metrics that affect the performance of any application hosted by Amazon:</p> <ul style="list-style-type: none"> • Response time: The response time is expected to be as fast as possible. Delay to cloud services adds in responsiveness of the application and typically results in application slow response. The long delays can also impact critically on the time taken to download the content. • Packet loss: As much as possible, the packet loss must be close to none. Dropping packets affect the real time applications (like voice, video), resulting in bad user experience. Packet loss also affects the transactional applications (like web based app); because it creates retransmissions, thus affecting the responsiveness. <p>The test also includes some path discovery. Path discovery identifies the path and service providers involved in the transport of packets from an endpoint to the AWS edge.</p> <p>The protocol used is TCP (on port 443).</p>
Description	<p>Generate TCP ping requests to known AWS servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.</p>
Purpose	Validate availability and response time to selected AWS servers.
Available Options	<ul style="list-style-type: none"> • Destination: known AWS server • Interval: interval between sending packets • Count: number of TCP SYN packets to send and SYNACK packets to receive • Packet Size: length of TCP content • Class Of Service: quality of service • Remote Port: • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms)

	Cloud Test - AWS
	<ul style="list-style-type: none"> Round Trip Time Max (ms) Round Trip Time Min (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	DNS test
Description	Test against DNS server and verify the time it takes to resolve IP address.
Purpose	Validate performance of DNS resolution (in response time) for specified server.
Available Options	<ul style="list-style-type: none"> url to resolve DNS server (default or empty: will use default DNS server as provisioned on probe) IPv4 or IPv6
Metrics	<ul style="list-style-type: none"> DNS resolution Availability (1 for available, 0 for not available) DNS Response time (msec) DNS server IP Resolved Addresses (one or several addresses resolved for url)
Advanced Information	This test will verify availability and response time of DNS service from probe or specific DNS server response time.
Results interpretation	A long response time from DNS by default can result into bad user experience and therefore should be monitored closely.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Dropbox upload/download
Description	Download or upload a file on dropbox account.
Purpose	Measures user experience sharing files on dropbox service.
Available Options	<ul style="list-style-type: none"> File (file size)

	Dropbox upload/download
	<ul style="list-style-type: none"> • Timeout
Metrics	<ul style="list-style-type: none"> • Download or upload rate • Download time • File size
Advanced Information	The files are provided by default. The dropbox account is a dedicated test account provided by Ixia.
Results interpretation	See advanced information.
Potential Errors	<p>Check whether the date on endpoint is valid, that is, the end point is not out of date. This is because, dropbox security policy will reject dropbox use from devices with an old date.</p> <p>See Common Errors - Real Services in <i>Error Description Guide</i>.</p>

	Email
Description	Send and receive email from same or different email accounts.
Purpose	Measures The time taken to relay an email via the configured SMTP servers and reaching a target mail server .
Available Options	Account information for sending and receiving email.
Metrics	Delay (ms) for receiving the email.
Advanced Information	<p>The test works by creating a mail client on the endpoint that sends an email to another address. The endpoint then connects to the inbox of the sent email to verify reception of the sent email.</p> <p>Details: You send email from your mail client (now running on Hawkeye Server) using the configured email address to the outgoing SMTP server using the configured port. The SMTP server first validates security and authentication i.e. connection security (SSL/TLS/25), port, username, password. The SMTP server works like the post office and performs a DNS lookup to find where to send the email (destination domain). The SMTP server may store the actual email on a local server (owned by domain sender) close to the Hawkeye server instead of the main SMTP server (that is Gmail). The SMTP server then sends the email to the destination domain Message Transfer Agent (MTA) server for long term storage. If the email destination domain is the same as the source, (that is both gmail) the SMTP server will act as the MTA server. If different sender/destination email domain and no issues, it can be routed/forwarded. The email is sent by SMTP protocol to the (destination domain) MTA server. The received email is stored on the destination domain</p>

	Email
	<p>MTA (POP3/IMAP) server. The MTA (POP3/IMAP) server uses POP3 or IMAP protocol to transfer email to recipient's inbox (email client on the laptop) when requested.</p> <p>In summary the User is required to enter credentials (username/password/SMTP server IP/server port/type encryption) for the senders and the receivers credentials (username/password/IMAP IP/IMAP server port/protocol) so the endpoint can verify receipt of the test email. The Real Service Email test times different stages, but most important is when the destination POP3/IMAP server receives the sent email. Endpoint will poll every second to check received email.</p>
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	FTP download
Description	FTP server test with login, password and download file.
Purpose	Test user experience downloading files from FTP server. The file downloaded needs to be on the FTP server.
Available Options	<ul style="list-style-type: none"> • test Timeout (sec) • FTP Server address or url • File to download • Authentication mode • FTP mode (active/passive) • Username • Password
Metrics	<ul style="list-style-type: none"> • Download File size • Download Time • Download bitrate
Advanced Information	This test will download the FTP file as fast as possible from the server to the probe.
Results interpretation	<p>This is user experience from probe to download file from specified FTP server</p> <p>If ftp not downloaded before end of timeout defined then the test will error out.</p>
Potential	See Common Errors - Real Services in <i>Error Description Guide</i> .

	FTP download
Errors	

	FTP multistream download
Description	<p>FTP server test with login, password and download file - adding a parameter to enable multiple concurrent streams download.</p> <p>THIS TEST IS ONLY SUPPORTED ON XR2000, NOT ON XRPI</p>
Purpose	Test user experience downloading files from FTP server. The file downloaded needs to be on the FTP server. The experience will be enhanced by multiple parallel streams. If the FTP server access is good enough, multiple FTP download streams are supposedly filling up the transport pipe.
Available Options	<ul style="list-style-type: none"> • test Timeout (sec) • FTP Server address or url • File to download • Authentication mode • FTP mode (active/passive) • Username • Password • Number of Streams : number of parallel streams the FTP will use
Metrics	<ul style="list-style-type: none"> • Download File size • Download Time • Download bitrate
Advanced Information	
Results interpretation	
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Gaming Test - Fortnite
Description	<p>Generate TCP ping requests to known Fortnite servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.</p>

	Gaming Test - Fortnite
Purpose	Validate availability and response time to selected Fortnite servers.
Available Options	<ul style="list-style-type: none"> • Destination: Known Fortnite Server • Interval: interval between sending packets • Count: number of TCP SYN packets to send and SYNACK packets to receive • Packet Size: length of TCP content • Class Of Service: quality of service • Remote Port: • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms) • Round Trip Time Max (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	Gaming Test - League of Legends
Description	Generate TCP ping requests to known League of Legends servers. THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.
Purpose	Validate availability and response time to selected League of Legends servers.
Available Options	<ul style="list-style-type: none"> • Destination: Known League of Legends Server • Interval: interval between sending packets • Count: number of TCP SYN packets to send and SYNACK packets to receive • Packet Size: length of TCP content • Class Of Service: quality of service • Remote Port: • Collect Path Discovery: Yes or No

	Gaming Test - League of Legends
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms) • Round Trip Time Max (ms) • Round Trip Time Min (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	Gaming Test - World of Warcraft
Description	<p>Generate TCP ping requests to known World of Warcraft servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.</p>
Purpose	Validate availability and response time to selected World of Warcraft servers.
Available Options	<ul style="list-style-type: none"> • Destination: Known World of Warcraft Server • Interval: interval between sending packets • Count: number of TCP SYN packets to send and SYNACK packets to receive • Packet Size: length of TCP content • Class Of Service: quality of service • Remote Port: • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms) • Round Trip Time Max (ms) • Round Trip Time Min (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results	See advanced information.

	Gaming Test - World of Warcraft
interpretation	
Potential Errors	See Common Errors - Real Services.htm.

	HTTP Client Certificate Check test
Description	Test to verify the validity of a HTTP Client Certificate, a digital signature. THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRpi, XR-VM, and VisionE1S.
Purpose	Check the validity of HTTP Client Certificates.
Available Options	<ul style="list-style-type: none"> • Destination Server: URL of the Client Server • Certificate File URL: URL of the Client Certificate file • Certificate Password: Password associated with the Client Certificate
Metrics	<ul style="list-style-type: none"> • Availability • DNS Resolution Time (ms) • Network TCP Connection Time (ms) • SSL Connection Time (ms) • Time to First Byte (ms) • Total Download Time (ms)
Advanced Information	Client certificates are used to validate the identity of a client (user). Simply put, it works as a password, but without any intervention/input from the user. This way, the server makes sure that it is connecting to the permitted user and that party is safe to communicate with.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	HTTP response time
Description	Download HTML content from the input url.
Purpose	Check availability of a webpage, check time to download content, compare TCP response time with application level content download time.
Available	<ul style="list-style-type: none"> • Servers address or url - the list can contain up to 10 different servers

	HTTP response time
Options	<ul style="list-style-type: none"> • IPV4 or IPV6 • Protocol http (0) or https (1) • Number of tests to execute in same batch • DSCP setting
Metrics	<p>Per Web server:</p> <p>Application latency (ms) – calculated as the time between endpoint issues the HTTP/Get and the time endpoint receives the first datagram from the server</p> <p>Number of Bytes received from server (size of the url html)</p> <p>TCP latency (ms) – calculated as the time between endpoint issues [SYN] and the time endpoint receives [SYN, ACK]</p> <p>Total download time (ms) – calculated as the time between endpoint issues [SYN] and the time endpoint receives the last datagram [FIN.ACK] from server</p> <p>Resolved IP address for server</p>
Advanced Information	<p>This test will try to download http content on a url. It will simply analyze result of the HTTP GET content - if a HTTP response code differs from 200 information will be displayed (eg REDIRECT)</p> <p>When http code is different from 200 no html is received.</p> <p>It is important to understand the difference between absolute URL's and relative URL's.</p> <p>An absolute URL takes the form protocol://domain/path, such as www.<domain name>.com, which will map specifically to https or http protocol. A relative URL like <domain name>.com can be redirected to either http or https. If test fails due to protocol error the test result reason code will advise user to change ip protocol configured for test.</p>
Results interpretation	The test is useful to understand TCP response time (network) to full html download (server response time).
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	HTTP Server test
Description	Download http pages full content from one or several servers and provide statistics about content and response time.
Purpose	<p>Get user experience information downloading the web page content. this will include all images and JavaScript/css etc...</p> <p>Other information like DNS resolution will help correlate user experience to CDN (Content Data Network) architecture.</p>

HTTP Server test	
Available Options	<ul style="list-style-type: none"> • Servers address or url • Download all page or only html content • IPV4 or IPV6 • Proxy Server • Proxy Username • Proxy Password • CA Certificate • Client Certificate • Client Key • Client Password • User Agent
Metrics	<ul style="list-style-type: none"> • Per Web server: • Download time • Download size • Download bitrate • Total File download size • time to first byte (max for all elements in page) • time to first byte (average for all elements in page) • Number of files in page • Resolved DNS address for http server
Advanced Information	<p>This test will download elements in a web page providing user experience getting information from the associated url. This test will download all elements in page (unless setting prevents it).</p> <p>It is important to understand the difference between absolute URL's and relative URL's.</p> <p>An absolute URL takes the form protocol://domain/path, such as www.<domain name>.com, which will map specifically to https or http protocol. A relative URL like <domain name>.com can be redirected to either http or https. If test fails due to protocol error the test result reason code will advise user to change ip protocol configured for test.</p> <p>URL may have multiple components to download, such as web page, scripts, images, style sheets. Multiple components will involve creating multiple TCP streams for the complete download. When only the page is selected for the download, the Initial time taken to setup connection is excluded from download time. Download time will solely reflect the actual download of the page. This means wireshark trace calculating time between first and last packet will be wrong. Following is the formula for calculating Download time.</p> <p style="text-align: center;">Download time = (Download Size * 8 / KB Rate per sec)</p>

	HTTP Server test
	<ul style="list-style-type: none"> • CA Certificate is used to verify the peer. If no certificate is entered in the CA Certificate, Peer Certificate Authentication is not performed. • Client Certificate is used to validate the identity of a client (user). It works as a password without any intervention or input from the user. In this way, the server makes sure that it is connecting to the permitted user and the connection is safe to communicate with. • Client Key is the Private Key associated with the Client Certificate. • Client Password is the password for the Client Key. <p>NOTE The Client Certificate and the Client Key can be concatenated into one file and entered into the Client Certificate.</p> <p>To move certificates into the Hawkeye system, use the Upload Files button located under the Advanced tab. This will allow the user to upload file types: pem, key, and crt. Certificates can also be removed from the Hawkeye system from the Upload Files window.</p> <p>After certificates have been moved to the Hawkeye system, they will appear in the certificate Select file pulldown selection menus.</p>
Results interpretation	The result should be reflective as the user experience getting from a browser to the web page.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	HTTP Server test-advanced
Description	Download http pages full content from one or several servers and provide statistics about content and response time- provides advanced information with full list of downloaded objects.
Purpose	<p>Get user experience information downloading the web page content. this will include all images and JavaScript/css etc.</p> <p>Other information like DNS resolution will help correlate user experience to CDN (Content Data Network) architecture.</p>
Available Options	<ul style="list-style-type: none"> • Servers address or url • Download all page or only html content • IPV4 or IPV6 • Proxy Server • Proxy Username • Proxy Password • CA Certificate

	HTTP Server test-advanced
	<ul style="list-style-type: none"> • Client Certificate • Client Key • Client Password • User Agent
Metrics	<p>Per Web server and element:</p> <ul style="list-style-type: none"> • Download time • Download size • Download bitrate • Total File download size • time to first byte (max for all elements in page) • time to first byte (average for all elements in page) • Number of files in page • Resolved DNS address for http server <p>Per web page element:</p> <ul style="list-style-type: none"> • Download time • Download size • Download bitrate
Advanced Information	<p>This test will download elements in a web page providing user experience getting information from the associated url. This test will download all elements in page (unless setting prevents it).</p> <p>It is important to understand the difference between absolute URL's and relative URL's.</p> <p>An absolute URL takes the form protocol://domain/path, such as www.<domain name>.com, which will map specifically to https or http protocol. A relative URL like <domain name>.com can be redirected to either http or https. If test fails due to protocol error the test result reason code will advise user to change ip protocol configured for test.</p> <p>URL may have multiple components to download, such as web page, scripts, images, style sheets. Multiple components will involve creating multiple TCP streams for the complete download. When only the page is selected for the download, the Initial time taken to setup connection is excluded from download time. Download time will solely reflect the actual download of the page. This means wireshark trace calculating time between first and last packet will be wrong. Following is the formula for calculating Download time.</p> <p>Download time = (Download Size * 8 / KB Rate per sec)</p> <ul style="list-style-type: none"> • CA Certificate is used to verify the peer. If no certificate is entered in the CA Certificate, Peer Certificate Authentication is not performed. • Client Certificate is used to validate the identity of a client (user). It

	HTTP Server test-advanced
	<p>works as a password without any intervention or input from the user. In this way, the server makes sure that it is connecting to the permitted user and the connection is safe to communicate with.</p> <ul style="list-style-type: none"> • Client Key is the Private Key associated with the Client Certificate. • Client Password is the password for the Client Key. <p>NOTE The Client Certificate and the Client Key can be concatenated into one file and entered into the Client Certificate.</p> <p>To move certificates into the Hawkeye system, use the Upload Files button located under the Advanced tab. This will allow the user to upload file types: pem, key, and crt. Certificates can also be removed from the Hawkeye system from the Upload Files window.</p> <p>After certificates have been moved to the Hawkeye system, they will appear in the certificate Select file pulldown selection menus.</p>
Results interpretation	The result should be reflective as the user experience getting from a browser to the web page.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	ICMP performance
Description	Generates ICMP packets at user defined bit rate and look at network bandwidth performance to receive response.
Purpose	Run quick throughput availability calculation based on ICMP traffic blasting. Is a way to quickly check the available bandwidth against a remote device on layer 3 without deploying advanced endpoints. This test should be considered as a first approximation to determine obvious bottlenecks.
Available Options	<ul style="list-style-type: none"> • Destination servers (IP or url addresses) • Generated throughput (ICMP content) • packet sizes(ICMP content) • Class of Service • test duration
Metrics	<ul style="list-style-type: none"> • ICMP Packet loss (%) • ICMP throughput (layer 4)
Advanced Information	<p>This test sends ICMP packets at defined bit rate and listens for the received packets throughput.</p> <p>Number of packets per second is calculated based on send throughput and</p>

	ICMP performance
	<p>packet size.</p> <p>It is expected that the total bitrate generated will be accurate for large packet sizes up to 200M for xr2000.</p> <p>Received throughput will take into account lags into the network so is expected to be always at least a bit less than the sent rate.</p>
Results interpretation	A loss rate is likely to impact the total received throughput quite dramatically. Results will also get more precision if traffic generation length is longer.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	ICMP test
Description	Generates ICMP ping requests to servers or interfaces.
Purpose	Validate network response time and key metrics (loss/jitter/response time) through very simple and largely supported ICMP protocol.
Available Options	<ul style="list-style-type: none"> • List of destination servers (IP or url addresses) • interval for icmp packets • number of packets to send • packet sizes • IPV4 or IPV6 • Enable Jitter calculation (default yes) • Class of Service
Metrics	<ul style="list-style-type: none"> • Packet loss (%) • Round trip average (ms) • Round trip max (ms) • Round trip min (ms) • Standard Deviation (ms) • Jitter (ms) • Jitter max (ms)
Advanced Information	This test sends ICMP packets and listen for responses. The jitter, round trip, and standard deviation cannot be calculated for packet sizes less than 16 bytes and will return a result of 0.
Results interpretation	The ICMP packets will detect any obvious issues on the network (congestions, drops, long response time, instable response time). It is an interesting data point as a change in the average of an ICMP test would likely reflect some

	ICMP test
	modification of the network average. The results should however be interpreted with care as the ICMP packets are usually treated with lower priority than data packets by network elements, therefore could show worst behavior than actual user traffic (prioritized) would experience in some cases.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	IGMP test
Description	Join a multicast channel and analyze received RTP stream- igmp v2 or v3 will be used depending on the available network. THIS TEST IS ONLY SUPPORTED ON XR2000, NOT ON XRPI
Purpose	Will join a channel (if available) and collect broadcasted stream if available.
Available Options	<ul style="list-style-type: none"> • watch duration: time before joining and leaving the stream • Probe physical interface: this setting is important as the igmp join is allocated to physical interface. Can be eth0 or eth1 (port 0 or port 1) • Multicast address: multicast address for the stream • Source Multicast address: for igmp v3 - will be used to select a specific source address.
Metrics	<ul style="list-style-type: none"> • join latency (ms) • leave latency (ms) • Number Of RTP flows • Average Packet Length • Interpacket arrival average (ms) • Interpacket arrival max (ms) • Interpacket arrival min (ms) • Interpacket arrival standard deviation (ms) • Maximum Loss Burst • Throughput average (Mbps) • Total kBytes Received • Total Packets lost • Total Packets Received • Total stream duration (sec) • Loss rate • IGMP protocol version

	IGMP test
Advanced Information	<p>The RTP stream received is parsed and analyzed. Video is not stored on the probe.</p> <p>Probe will autodetect igmp version (v2 or v3).</p> <p>Leave Source Multicast address empty for v2 or All sources.</p>
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Office365
Description	Office 365 Test Suite.
Purpose	Validate network connectivity performance for Office 365 server suites.
Available Options	<ul style="list-style-type: none"> • Office365 Server lists to choose from <ul style="list-style-type: none"> ▪ login.microsoftonline.com ▪ office.live.com ▪ outlook.office365.com ▪ teams.microsoft.com ▪ broadcast.skype.com ▪ www.onenote.com • Option to collect Path Discovery to trace the path taken • SharePoint Tenant • Test Frequency in Minutes
Metrics	<ul style="list-style-type: none"> • Packet loss (%) • Application latency (ms) • Round trip max (ms) • Round trip Min (ms) • Round trip Avg (ms)
Advanced Information	
Results interpretation	<p>The ICMP packets will detect any obvious issues on the network (congestions, drops, long response time, instable response time). It is an interesting data point as a change in the average of an ICMP test would likely reflect some modification of the network average. The results should however be interpreted with care as the ICMP packets are usually treated with lower</p>

	Office365
	priority than data packets by network elements, therefore could show worst behavior than actual user traffic (prioritized) would experience in some cases.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Office365 using proxy
Description	Office 365 Test Suite through a proxy.
Purpose	Validate network connectivity performance for Office 365 server suites through a proxy.
Available Options	<ul style="list-style-type: none"> • Office365 Server lists to choose from <ul style="list-style-type: none"> ▪ login.microsoftonline.com ▪ office.live.com ▪ outlook.office365.com ▪ teams.microsoft.com ▪ broadcast.skype.com ▪ www.onenote.com • SharePoint Tenant • Test Frequency in Minutes • IP Protocol (IPv4 or IPv6) • Class of Service • Protocol (https or http) • Proxy Host:Port • Proxy User • Proxy Passwd
Metrics	<ul style="list-style-type: none"> • Packet loss (%) • Resolve Hostname Avg, Max, and Min (ms) • Connect Avg, Max, and Min (ms) • Round trip Avg, Max and Min (ms) • (HTTP Server) Process and Respond Avg, Max and Min (ms) • Teardown Avg, Max and Min (ms) • Download Rate Avg, Max and Min (KB/Sec)
Advanced Information	
Results interpretation	The HTTP packets detect any obvious issue on the network (congestions, drops, long response time, unstable response time). It is an interesting data point, because a change in the average of an HTTP test may reflect some modification of the network average. You must interpret the results carefully, because the HTTP packets are usually treated with lower priority than data packets by the network elements. Therefore the result displayed may be of poorest quality than the actual user traffic (prioritized) experienced in some cases.

	Office365 using proxy
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Path Discovery
Description	Discover paths to a destination.
Purpose	Uses a combination of traceroute and ping requests to discover paths from the original probe to the destination server.
Available Options	<ul style="list-style-type: none"> • destination (IP or url addresses) • timeout for request (sec) • traceroutes count • traceroute max hops • traceroute protocol (ICMP, TCP or UDP) • destination port • Quality of service (or DSCP setting) • IPv4 or IPv6
Metrics	
Advanced Information	<p>Although Path Discovery has no configurable metrics there are criteria for Pass/Fail/Error. The criteria for Fail is reached if for all the last hops the destination is unknown.</p> <p>The different servers on the path will be identified and multiple paths to destination can be discovered by increasing the traceroutes count.</p> <p>Graph only shows forward routes. It does not show return routes for any packets used for path discovery. Some nodes may have no measurements as they are configured not to respond to ping. For path discovery mechanism, each traceroute is run for one probe per hop (not as typically the traceroute sends 3 pings or request per probe). Path Discovery sends 100 ICMP packets to each node in the path.</p> <p>If a test is configured and not enough hops are configured to reach the destination, the test will pass without reaching destination assuming all hops were successful.</p> <p>In Path Discovery the traceroute component uses the ping command. The URL used for test is expected to be a value that will find a match in the DNS lookup tables. The URL used for the test cannot have sub-directories as part of the URL if they will not match entries in the DNS lookup tables. Path Discovery test does not massage the URL's entered by the User."</p>
Results interpretation	There are various options in 'Test Results' that can help user to analyze path discovery results:

Path Discovery	
	<ul style="list-style-type: none"> • Traceroute – displays the traceroute style output • Show navigation – (uncheck) enables free zoom/ pan mode • Frequent path – highlights frequent path and line thickness will be proportional to frequency • Loss – if selected, highlights nodes with loss equal or greater than specified value • Avg RTT – if selected, highlights nodes with average round trip delay (RTT) equal or greater than specified value • Cluster – gives user option to cluster Autonomous Systems or unknown nodes • Class of Service (DSCP setting) – identifies where in network path nodes change the QOS setting <p>The following information is retrieved and available for display:</p> <p>Hop info</p> <ul style="list-style-type: none"> • IP • Reverse DNS • Autonomous System • ICMP extensions • QoS Changes <p>When Hawkeye server is connected to internet, following hop info are also retrieved</p> <ul style="list-style-type: none"> • Network name • Prefix • Organization <p>Metrics</p> <ul style="list-style-type: none"> • Frequency • Min/Avg./Max response time • Packet loss
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

Port Scan	
Description	Determines the state of network ports.
Purpose	Can be used to ensure services (for example HTTPS, FTP, etc.) are accessible or blocked by firewalls.

	Port Scan
Available Options	<ul style="list-style-type: none"> • destination (IP or url addresses) • protocol: TCP or UDP • start port • port count • expected port state • IPv4 or IPv6
Metrics	<ul style="list-style-type: none"> • Open ports – shows how many ports from the configured range are open. Available for both TCP and UDP • Closed ports - shows how many ports from the configured range are closed. Available for both TCP and UDP • Filtered ports - shows how many ports from the configured range are filtered (no replies are received). Available for TCP • Open/Filtered ports - shows how many ports from the configured range are open/filtered (no replies are received either because of a firewall or the application listening on the port is not sending any reply). Available for UDP <p>Each of these metrics will only show up in result if at least on port of corresponding state was found.</p>
Advanced Information	
Results interpretation	<p>The Port Scan results will reflect an overall test status and the status of different ranges of ports. For a given range of ports the Metric column represents the state of the port and the value column, represents the port number or port range that is in that state. The Status KPI column represents the comparison with the actual state of the ports compared to the configured “expected state” in the test configuration.</p> <p>The following describes the port state:</p> <ul style="list-style-type: none"> • OPEN: The port (TCP or UDP) on the destination is reachable and we receive reply to our sent packets. • OPEN/FILTERED: Only applies to UDP ports. If no reply is received either because the application listening is not replying or we cannot reach the destination (e.g. due to firewalls blocking the packets). • FILTERED: Only applies to TCP ports. If no reply is received back (e.g. due to firewalls blocking the packets). • CLOSED: If the port on the destination is reachable (TCP or UDP) but there is no application listening on destination (i.e. packets received by destination IP, but packets not processed by intended application). Specifically endpoint received back ICMP Destination Unreachable message.

	Port Scan
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	REST API test
Description	Generates REST HTTP requests. (ONLY SUPPORTED ON VISIONE1S AND XR-VM)
Purpose	Validate RESTful Web Services of a server and the response time supported ICMP protocol.
Available Options	<ul style="list-style-type: none"> • URL: • Key-Value Pairs: Data parameters • Method: GET, POST, PUT, PATCH, DELETE • Response Code: The Response Code is compared to the HTTP Status Code of the response to the query sent • Authentication: None, Cookie based • Session ID: Alpha-numeric identifier to allow multiple cookies
Metrics	<ul style="list-style-type: none"> • Availability (1 for available, 0 for not available) • Response Code (Compare configured Response Code of test with returned HTTP Status Code) • Response time (ms)
Advanced Information	<ul style="list-style-type: none"> • The Response Code has wildcards like 2XX which will match any 200 series HTTP Status Code response. • Can be used to perform both positive and negative testing.
Results interpretation	<ul style="list-style-type: none"> • The availability of the URL being tested. • The round trip time of the request and response. • If the HTTP Status Code of the response matches the desired Response Code
Potential Errors	<ul style="list-style-type: none"> • Missing URL • Unknown Session • Response time threshold failed • Response Code failure

	Skype Network Connectivity Performance
Description	Assesses the set of network performance requirements for Skype for Business Online services.
Purpose	Determines the quality of connection between your network and Skype for Business Online. No actual Skype traffic is exchanged, just performance measurements across the internet to the Skype servers.
Available Options	<ul style="list-style-type: none"> • Class of service
Metrics	<ul style="list-style-type: none"> • Jitter (ms) • packet loss • round trip time avg (ms) <p>The result includes also the path view to get a more clear understanding of where performance issues are located. The metrics for pass/fail criteria are defined by Microsoft so the user cannot define pass/fail criteria for metrics.</p>
Advanced Information	<p>The test sends 150 ping TCP packets 10 milliseconds apart to World Wide Anycast IP of Skype for Business media relay and compare the measurements against Microsoft requirements. Skype network connectivity performance metrics report packet loss to the final IP.</p> <p>See Media Quality and Network Connectivity Performance in Skype for Business Online for more information</p>
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	TCP Ping
Description	Generates TCP SYN ping requests to servers or interfaces.
Purpose	SYN packets are sent to interface and port, and round trip delay is based on SYNACK received. This test is useful especially to measure TCP connection times to http server or when ICMP protocol is blocked to check availability and network response time to server.
Available Options	<ul style="list-style-type: none"> • List of destination servers (IP or url addresses) • interval for TCP SYN packets • number of packets to send • packet sizes(TCP content) • TCP port

	TCP Ping
	<ul style="list-style-type: none"> • DSCP setting • IPv4 or IPv6
Metrics	<ul style="list-style-type: none"> • TCP Packet loss (%) • Round trip average (ms) • Round trip max (ms) • Round trip min (ms)
Advanced Information	<p>This test sends TCP SYN packets and listen for SYNACK responses.</p> <p>Some TCP ports (HTTP for example on some servers) would only allow packet size of 0 (no content) for TCP syn.</p>
Results interpretation	The TCP response round trip and packet loss provides good information about the network transport to TCP remote ends.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Teams
Principles	<p>This test verifies key metrics to access Teams services (gateways in Microsoft cloud).</p> <p>The services of Teams are hosted into different regions. A server is automatically affected to the user for connectivity and voice/video traffic on its infrastructure. The server is typically optimized to be the closest geographic gateway of the first to join a call or a meeting. Having good network connectivity from the edge to the Teams serving gateways are paramount to the service experience.</p> <p>This test possesses monitoring capabilities with network performance characterization from the endpoint to the different points of services of Teams. Predicting Teams serving region(s) for a user is not always possible, because these can change over time. But as a good approximation, it is recommended to verify the performance against two or three closest regions and also against the regions of other team members frequently setting up meetings.</p> <p>Key metrics that affect the performance and Teams user experience:</p> <ul style="list-style-type: none"> • Response time: The response time is expected to be as fast as possible. Delay to cloud services impacts the conversation lags, but is also likely to create delay variations. Therefore it affects the overall performance with some buffering dropping packets. • Packet loss: Packet loss results into real time packets being lost, resulting in breaking of part of conversations or freezing of videos. <p>The test also includes some path discovery. Path discovery identifies the path and service providers involved in the transport of packets from an endpoint to</p>

	Teams
	<p>the Teams service locations.</p> <p>The protocol used is TCP (on port 443).</p>
Description	<p>Generate TCP ping requests to known Teams servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPi, XR-VM, and VisionE1S.</p>
Purpose	Validate availability and response time to selected Teams servers.
Available Options	<ul style="list-style-type: none"> • Destination: known Teams server • Class Of Service: quality of service • IP Protocol: IPv4 or IPv6 • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms) • Round Trip Time Max (ms) • Round Trip Time Min (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	Traceroute
Description	Generates traceroute request.
Purpose	Traceroute request sent from original probe to the destination server or url. Helps understanding the different hops involved and response time of each hop based on used protocol (ICMP or UDP).
Available Options	<ul style="list-style-type: none"> • Destination Server (IP or url addresses) • Timeout for request (sec) • DSCP setting • IP protocol (ipv4 or ipv6) • traceroute protocol (ICMP or UDP)

	Traceroute
Metrics	Per step: <ul style="list-style-type: none"> • server ip and name • response time
Advanced Information	Traceroute is informative for now: there is no check on thresholds therefore the result is always pass. The different servers on the path will be identified. Several packets are sent for discovery and in case of load balancing the list of servers that have been used to reach end destination might show different options per path.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	UDP Ping
Description	Generates UDP packets requests to servers or interfaces.
Purpose	UDP packets can be blasted to remote servers or interfaces. If these are configured with echo port (typically port 7 on routers) packets are sent back.
Available Options	<ul style="list-style-type: none"> • List of destination servers (IP or url addresses) • interval for UDP packets • number of packets to send • packet sizes(TCP content) • Remote UDP port • DSCP setting • IPv4 or IPv6
Metrics	<ul style="list-style-type: none"> • UDP Packet loss (%) • Round trip average (ms) • Round trip max (ms) • Round trip min (ms)
Advanced Information	This test sends UDP packets and listen for UDP packet responses.
Results interpretation	The UDP response round trip and packet loss provides good information about the network transport to UDP remote ends. This test is particularly useful to test routers configured with reflectors. The UDP traffic generation is similar

	UDP Ping
	than TWAMP protocol defines for user plane.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Webex Test
Description	<p>Generate TCP ping requests to known Webex servers. Optionally Download HTML content from the tenant.</p> <p>This test is supported on XR2000, XR2000VM, XR3000, XRPi, XR-VM, XRE1S, and VisionE1S.</p>
Purpose	<p>Validate availability and response time to selected Webex servers.</p> <p>Check availability of a tenant, check time to download content, compare TCP response time with application level content download time.</p>
Available Options	<ul style="list-style-type: none"> • MediaGW Destination: known Webex server • Tenant: a company's common access to Webex, that is mycompany.webex.com • IP Protocol: IPv4 • Class Of Service: quality of service • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • MediaGW Destination Availability • MediaGW Destination Packet Loss • MediaGW Destination Round Trip Time Avg (ms) • MediaGW Destination Round Trip Time Max (ms) • MediaGW Destination Round Trip Time Max (ms) • Tenant Application Latency (ms) • Tenant Bytes from server • Tenant TCP Latency (ms) • Tenant Total http download time (ms) • Resolved IP address
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Wi-Fi Connect
Description	Measure Metrics Connecting To Wi-Fi AP.
Purpose	Wi-Fi connect measures the time taken by the Wi-Fi device to connect to the access point (AP). This test highlights the bottle necks in the various states like (Association, Authentication and DHCP) while connecting to the Wi-Fi AP. This test can be executed to check the connectivity of the device to the service provider by pinging to the Internet or external network. The results are available as part of Metrics status and graphs. For this test to work, the Ixia XRPi probe must be used with the supplied Wi-Fi dongle. This test is also supported on XR3000 with Wi-Fi interface enabled. Note that a valid wired ethernet connection is necessary to run this test.
Available Options	Authentication Method, Passphrase (WPA-PSK), SSID, BSSID, Reset Interface After Test, Custom WPA Content, Username, Password, Test frequency, Ping Address, reset interface after test.
Metrics	<ul style="list-style-type: none"> • Association Time (Ms) • Authentication Time (Ms) • Connect Time (Ms) • DHCP Handshake Time (Ms) • Association Attempt • ICMP Packet Loss • ICMP Round Trip Avg • Signal Strength (%) • Total Connect Time (Ms) • Wi-Fi Signal Level (DBm)
Advanced Information	<p>This test supports Authentication schemes, None, WPA-PSK, EAP-TTLS/MSCHAPv2 and custom. You can also select a particular BSSID to connect to.</p> <p>The default average is to reset the wlan0 interface after each execution of the Wi-Fi Connect test.</p>
Results interpretation	Total connect time gives the entire time for the Wi-Fi connection to the AP. The four stages for connection to the AP are numbered 1,2,3, or 4 and have times reported to complete those stages of total call connect. Bottle necks can be identified by looking at the time taken by individual 802.11 standard Wi-Fi States. ICMP metrics provide the connectivity to internet stats. Historic data can be used to make inference on the Wi-Fi load on the network.
Potential Errors	<p>The error messages that can be displayed are:</p> <ul style="list-style-type: none"> • If Wrong SSID is used – “No Wi-Fi interface detected” • If no Wlan0 interface - “No response from file”

	Wi-Fi Connect
	<ul style="list-style-type: none"> • If Probe is not registered – “Probe not registered or active for real service”

	Wi-Fi Inspect
Description	Measure Metrics Connecting to all available Wi-Fi AP.
Purpose	Measures key metrics of all available Wi-Fi AP that can be detected by probe.
Available Options	<ul style="list-style-type: none"> • SSID
Metrics	<ul style="list-style-type: none"> • Channel • Advertised by AP Max bitrate (Mbps) • Wi-Fi Signal Level (DBm)
Advanced Information	XRPI Wi-Fi Probe makes repeated measurements to ensure that all Wi-Fi AP in range can be detected and reported. All Wi-Fi AP in range (2.4/5 GHz) in range are reported, except limited support for AC networks.
Results interpretation	Results are reported in Wi-Fi Dashboard. Results can be associated with a floorplan.
Potential Errors	<p>Charting Wi-Fi AP over time may show gaps in statistics. This can be caused by several factors such as, Wi-Fi AP is busy and is not sending out the beacon signal used to calculate measurements. Wi-Fi AP signal level drops below necessary signal strength to be detected and reported. Interference from stronger signal level from another Wi-Fi AP using same channel number may cause weaker signal AP to not be reported.</p> <p>If no Wlan0 interface on XRPI Wi-Fi probe - “No response from file”.</p> <p>If Probe is not registered – “Probe not registered or active for real service”.</p>

	Zoom
Principles	<p>This test verifies key metrics to access Zoom services (gateways).</p> <p>Zoom is hosted into different regions. A server is automatically affected to the user for connectivity and voice/video traffic on its infrastructure. The server is typically optimized to be the closest geographic gateway. Having good network connectivity from the edge to the Zoom serving gateways are paramount to the service experience.</p> <p>This test possesses monitoring capabilities with network performance characterization from the endpoint to the different points of services of Zoom. Predicting Zoom serving region(s) for a user is not always possible, because</p>

	Zoom
	<p>these can change over time. But as a good approximation, it is recommended to verify the performance against two or three closest regions.</p> <p>Key metrics that affect performance and Zoom user experience:</p> <ul style="list-style-type: none"> • Response time: The response time is expected to be as fast as possible. Delay to cloud services impacts the conversation lags, but is also likely to create delay variations. Therefore it affects the overall performance with some buffering dropping packets. • Packet loss: Packet loss results into real time packets being lost, resulting in breaking of part of conversations or freezing of videos. <p>The test also includes some path discovery. Path discovery identifies the path and service providers involved in the transport of packets from an endpoint to the Zoom service locations.</p> <p>The protocol used is TCP (on port 443).</p>
Description	<p>Generate TCP ping requests to known Zoom servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.</p>
Purpose	Validate availability and response time to selected Zoom servers.
Available Options	<ul style="list-style-type: none"> • Destination: known Zoom server • Interval: interval between sending packets • Count: number of TCP SYN packets to send and SYNACK packets to receive • Packet Size: length of TCP content • Class Of Service: quality of service • Remote Port: • Collect Path Discovery: Yes or No
Metrics	<ul style="list-style-type: none"> • Availability • Packet Loss • Round Trip Time Avg (ms) • Round Trip Time Max (ms) • Round Trip Time Min (ms)
Advanced Information	For information on Collect Path Discovery, refer to the Path Discovery Real Service test.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

	Zoom Status
Description	Zoom service status of various Zoom systems THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPi, XR-VM, and VisionE1S.
Purpose	Check if Zoom systems are operational.
Available Options	None
Metrics	<ul style="list-style-type: none"> • Zoom Meetings • Zoom Video Webinars • Zoom Phone • Zoom Chat • Zoom Website • Zoom Dashboard & Reporting • Download Center • Web Portal • Web Client • Conference Room Connector • Zoom Cloud Room Connector • Zoom Connector for Cisco • Zoom Connector for Polycom • Cloud Recording • Meeting Telephony Services • Integrations • Live Streaming • Zoom Developer Platform • Web SDK • REST API • Marketplace • Webhooks
Advanced Information	Each system will have a status. The metric passes if the system is Operational.
Results interpretation	See advanced information.
Potential Errors	See Common Errors - Real Services.htm.

Path Discovery

Summary

Hawkeye Path discovery is a methodology to provide visibility into network topology from a location with Hawkeye endpoint to any remote location.

The discovery relies on standard protocols packets being sent to the network to find out about nodes being traversed. There is therefore no need for specific software or hardware being deployed on the path nor at remote location.

Path discovery allows to discover application specific paths by way of configuring the protocol and ports used by an application to discover the route taken by packets to reach destination.

Path discovery leverages Hawkeye test execution framework to allow historical data collection and perform analysis in real time or with retrospective views.

Path Discovery Methodology

The path discovery relies on the following steps for path analysis:

1. Path discovery: packets are sent using TCP, UDP or ICMP protocols with different TTL tags and responses from network elements are captured to indicate information about traversed nodes. This sequence is repeated several times (configurable) so that potential different paths are discovered and displayed in a graph.
2. Nodes network performance analysis: 100 ICMP packets are sent to each identified nodes to find out about basic IP performance metrics using ICMP protocol and report on packet loss rate and round trip times (RTT) to the traversed nodes.
3. Fail criteria is determined if the last two nodes are **unknown nodes**. If the configured number of hops is more than the count of nodes to the destination, it is not uncommon for the nodes beyond the destination node to be marked as unknown nodes. This will result in the test being flagged as **fail**.

Setting up the Path Discovery from an Endpoint

Path discovery is available from Hardware endpoints and XR2000 VM as a real service.

To set it up, go to test execution-real service screen and select your endpoint and Path discovery test type.

The following options are available:

Probe From:	xr2000-0090083672A4 - 10.200.40.81	Test Type:	Path Discovery	Test Identifier:	
Destination Server:	google.com	Traceroute Count:	4	Maximum Number Of Hops:	30
Protocol:	TCP	Class Of Service:	Best Effort	Destination Port:	443
Timeout (Sec):	120				

Destination server: is IP or URL of the remote server that needs to be reached to discover path. It can be hosted in private network, private or public cloud, public internet etc.

Traceroute counts: number of path discovery attempts executed to find out about path. This number must be into 1-20 range.

Maximum number of hops: the traceroute are attempted until destination is reached or for a maximum number of hops between source and destination.

Protocol: protocol used for path discovery. The default is TCP which is recommended as it is the most likely to provide accurate results. Other options available are UDP and ICMP. UDP would function similar to TCP but using a different destination port and without SSL, while ICMP is going to issue pings with TTL. It is important to know that some nodes on the path may react differently to these protocols: some routers/switches are blocked for ICMP responses for example and allow TCP or UDP, so the discovery may provide more information with one protocol or the other.

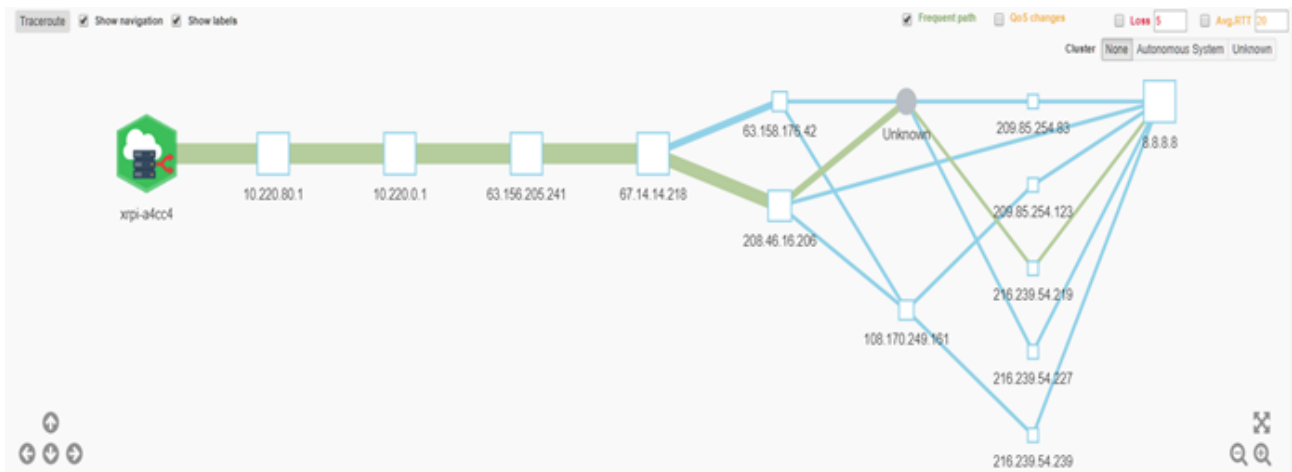
Destination port: this is used if protocol is TCP or UDP. The discovery messages will be sent with destination port set to this value and using a random source port. This can again be important when determining routing/COS management details on the path for specific protocol/port. Using the protocol and destination port a specific application would use allows finding about how the associated packets would be handled by the network.

Timeout (sec): this is the maximum time the path discovery will be allowed to run – in case the overall process exceeds this maximum allowed time the test will error out and free the test execution queue.

Interpreting Test Execution Results

Path discovery display is highly visual allowing quick understanding of the traversed nodes for an endpoint.

The picture below shows an output of the function:



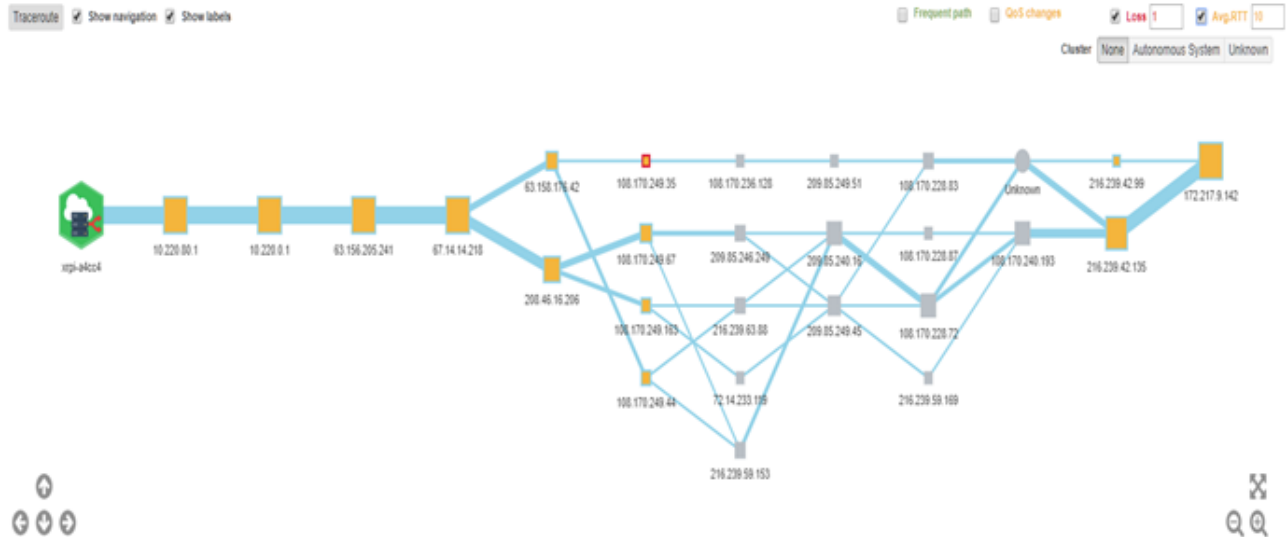
The different nodes detected in the path discovery are shown with squares.

When messages are sent and there is no responses from the network, an unknown square is shown.

This typically happens when packets are dropped on their way back or forth, or when the node that is on the path is configured so that it does not advertise the drop to source.

The links between the nodes are shown with different thickness levels to illustrate the distribution between paths.

As shown in the example below, it is also possible to investigate the packet drops or Round Trip Time (RTT) detected in the path by configuring a threshold.

**NOTE**

The RTT and packet loss are displayed based on ICMP messages being sent to the nodes. The metric is displayed only if at least one ICMP answer is received. The assumption if 100% packets are dropped is that the node is blocked for ICMP responses and therefore no data is displayed.

The ICMP packets are 100 bytes long and 100 of them are sent with 20ms interval for collecting the information. The base ICMP sequence is the starting ICMP sequence number that gets incremented with each packet.

During the path discovery, the information about Autonomous System (AS) to which the node belongs is collected. This information is belonging to an organization having routers on the public internet. It will identify service providers or autonomous entities being traversed to reach destination.

Routes can be displayed with only showing Autonomous System (AS).

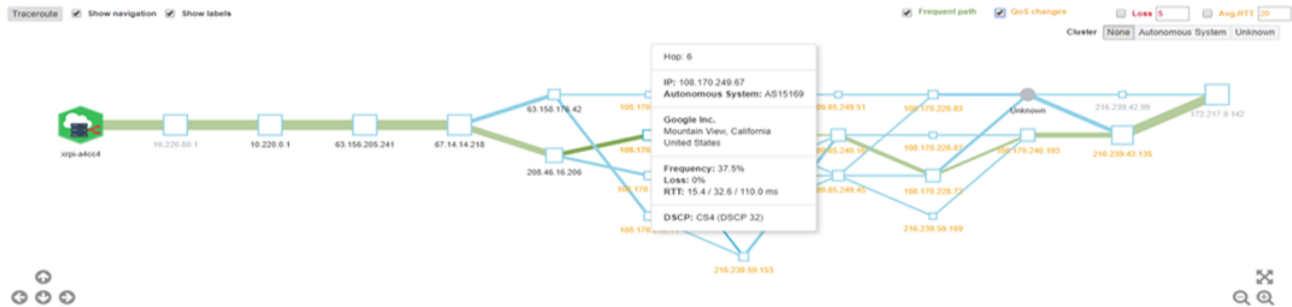
When the Hawkeye server has access to internet it can collect information to what AS code is registered.

Next figure illustrates a path discovery shown with AS grouping.



The next figure illustrates a path discovery showing the changes in QOS. When the Path discovery test was configured the required QOS (DSCP) value was selected. As the packets pass through each network node the specific node can change the QOS setting for each packet. The figure below shows

when the QOS changes box is selected that the user has the ability to select a node to view its details which will include the QOS value assigned to all packets being forwarded to the next network node.



By clicking on any nodes on the graph, full information about the results collected will be displayed:

- Hop defines the path # it was detected at.
- IP if the IP detected or unknown if node does not respond to traceroute packet.
- Network is detected through AS.
- If available the full registered address for AS will be displayed.
- Frequency shows how many times this was detected using this node.
- Loss and RTT (round trip time) are gathered through ICMP messages.
- DSCP is not available for the last node.
- The DSCP information for a node will not be displayed if the TCP/ICMP messages are not responded to by the node.

The traceroute button will display in a table all the information collected for all steps in the path – see example below:

Traceroute style output

Traceroute from xrp1-a4cc4

#	IP	Autonomous System	Min / Avg / Max RTT	DSCP	ICMP Extensions
1	10.220.80.1		5.0 / 14.5 / 75.0 ms	AF13 (DSCP 14)	
2	10.220.0.1		3.8 / 12.2 / 81.2 ms	AF13 (DSCP 14)	
3	63.156.205.241	AS209	9.5 / 20.4 / 77.5 ms	AF13 (DSCP 14)	
4	67.14.14.218		14.8 / 23.5 / 75.6 ms	AF13 (DSCP 14)	
5	63.158.176.42	AS209	15.1 / 23.7 / 77.9 ms	CS4 (DSCP 32)	
6	108.170.249.76 108.170.249.108	AS15169 AS15169	14.9 / 21.9 / 67.3 ms 15.0 / 23.7 / 78.4 ms	CS4 (DSCP 32) CS4 (DSCP 32)	
7	108.170.236.128 209.85.248.183	AS15169 AS15169	_/_/_/_ _/_/_/_	CS4 (DSCP 32) CS4 (DSCP 32)	<MPLS:L=325387,E=4,S=1,T=1> <MPLS:L=26498,E=4,S=1,T=1>
8	209.85.249.51 209.85.240.16	AS15169 AS15169	_/_/_/_ _/_/_/_	CS4 (DSCP 32) CS4 (DSCP 32)	<MPLS:L=24763,E=4,S=1,T=1> <MPLS:L=723925,E=4,S=1,T=1>
9	108.170.228.72 216.239.63.250	AS15169 AS15169	_/_/_/_ _/_/_/_	CS4 (DSCP 32)	
10	* 108.170.240.193	AS15169	_/_/_/_	CS4 (DSCP 32)	
11	216.239.42.135	AS15169	36.0 / 45.0 / 84.2 ms	CS4 (DSCP 32)	
12	172.217.9.142	AS15169	36.0 / 44.2 / 89.3 ms		

This will show the User the different steps and what nodes were involved. The ICMP extensions contain feedback on MPLS network labelling and protocol information.

Path Discovery Failures

If a Path Discovery test has an error message indicating a timeout, follow the following steps in order:

1. Reduce tracecount in configuration of Path Discovery test. This will reduce amount of scans and may potentially reduce number of available routes identified to destination.
2. Reduce maximum number of hops in configuration of Path Discovery test.
3. Increase test timeout in configuration of Path Discovery test. If this is increased above 3 minutes, refer to [Parameters Effecting Performance on page 337](#) for information on how to increase overall timeouts for Real Service tests.

NOTE

Some nodes will respond to the first ICMP message then not respond to any other ICMP messages from the same source for a certain time period, this does not reflect a problem.

If you use an IP for a well-known web site, such as Google, the test may be flagged as a fail although the Path Discovery test was able to successfully reach and map the organization.

If the web site supports IETF defined "anycast routing", IPv4 or IPv6 address will be routed to the nearest operational server, which would have a different IP address to the entered destination IP

defined for the test. Thus, this would be marked as a **Fail** but the traceroute and network map to the destination will be correct.

Real Service Endpoint Support Matrix

Continuous Real Service

	Software Endpoint	XR2000 / VM	XR Pi	Pi4	XR Docker	Vision E1S	XR VM	XR3000	IxProbe IxTap IxBypass
Echo TCP	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Echo UDP	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Ping	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Web Page Download	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Wi-Fi	Supported	Not Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Supported	Not Supported

Advanced Real Service:

	Software Endpoint	XR2000 / VM	XR Pi	Pi4	XR Docker	XR E1S	Vision E1S	XR VM	XR3000	IxProbe IxTap IxBypass
BitTorrent	Not Supported	Supported	Not Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
Cloud Test - AWS	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
DNS Test	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
DropBox	Not Supported	Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported

	Software Endpoint	XR200 0 / VM	XR Pi	Pi4	XR Docker	XRE1S	Vision E1S	XR VM	XR300 0	IXProb e IXTap IXByp ass
Download	Not Supported	Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
DropBox Upload	Not Supported	Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
Email	Not Supported	Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
FTP Download	Not Supported	Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
FTP Multistream Download	Not Supported	Supported	Not Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
Gaming Test - Fortnite	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Gaming Test - League of Legends	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Gaming Test - World of Warcraft	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
HTTP response time	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
HTTP Server	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

	Software Endpoint	XR200 0 / VM	XR Pi	Pi4	XR Docker	XRE1S	Vision E1S	XR VM	XR300 0	IXProbe IXTap IXBypass
Test	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
HTTP Server Test - Advanced	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
HTTPS Client Certificate Check	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
ICMP performance	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
ICMP Test	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
IGMP Test	Not Supported	Supported	Not Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
Office3 65	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Office3 65 using proxy	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Path Discovery	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Port Scan	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
REST API	Not Supported	Supported	Not Supported	Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported

	Software Endpoint	XR200 0 / VM	XR Pi	Pi4	XR Docker	XRE1S	Vision E1S	XR VM	XR300 0	IXProb e IXTap IXByp ass
Test	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Skype Network Connectivity Performance	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
TCP ping	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Teams	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Traceroute	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not Supported
UDP ping	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Webex	Not Supported	Supported	Supported	Not Supported	Not Supported	Supported	Supported	Supported	Supported	Not Supported
Wifi Connect	Not Supported	Not Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Not Supported
Wifi Inspect	Not Supported	Not Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Not Supported
Zoom	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Zoom Status	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Replicating Tests Across Multiple Endpoints

Hawkeye allows you to create a test template for all test types. The advantage of this is that when assigning tests to endpoints a saved test template can be assigned. Test templates offer the ability to create pre-canned test suites. For instance combining several Node to Node tests for an "office_suite" test template or combining several tests for a "voice_suite" test template. This saves user time in test creation and allows for thresholds for test metrics to be set to expected values once for the users network. For example threshold metrics for expected round trip delays.

In **Probe Management** there is a web GUI for **Test Templates**. You can create a test template and give it a name for referencing in test execution. You can configure all properties of a test except the endpoints to be used. You can create a test suite by adding multiple tests of the same test type (N2N/Mesh/Real Services) to each test template. For each test type added to the template all usual configuration of a regular test can be configured, such as thresholds, email for alarms, schedule frequency of tests. For each test the you have a flag to enforce the test is scheduled at correct synced time. Each test template can be restricted to be available to only certain user groups. Once all tests have been added to the new test template it is "added" and is available for use in **Test Execution**.

In **Test Execution** for each test type such as **Test Execution Node to Node** if a test template is available then a button is presented to the user allowing the selection of "normal" test or using a previously saved test template. A pull down menu allows for the selection of a test template then the User only has to select the endpoints to assign for the test template. When tests are running an icon identifies normal tests and tests based on test templates.

Under **Test Execution** there is a web page **Test Execution Templates**, which is used to manage tests running using a test template (for example, voice_suite). From this web page individual tests on endpoints can be paused and deleted.

NOTE

A test template can only be deleted once all scheduled tests using that specific test template have been removed.

NOTE

The name of the test template (test identifier) does not support special characters such as quotes.

Test Types Reporting Wi-Fi Statistics

This feature displays the statistics of the tests that are executed for the Wi-Fi devices. The tests results are displayed based on the combination of the **Probe From** and **Probe To** with the TCP and UDP tests that you execute.

The system displays the statistics when you execute any TCP XR2000/XRPi/SW EP test the **Probe From** must be Wi-Fi(interface) and when you execute any UDP transport test the **Probe To** must be Wi-Fi.

The table below provides information on the various combinations when a Wi-Fi enabled endpoint or non-Wi-Fi enabled endpoint in the **TO/FROM** position for TCP and UDP traffic tests will provide Wi-Fi statistics.

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
N2N			
Voice 1 Pairs Unidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Voice 1 Pairs Unidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Voice 1 Pairs bidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Voice 1 Pairs bidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Voice 1 pairs - UDP Data bidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Voice 1 pairs - UDP Data bidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Voice from->to	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Voice from->to	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Voice bidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Voice bidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Video Stream	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Video Stream	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
UDP Throughput to->from	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
UDP Throughput to->from	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
UDP Throughput from->to - 4 COS	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
UDP Throughput from->to - 4 COS	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
UDP Throughput from->to	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
UDP Throughput from->to	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
UDP Throughput bidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
UDP Throughput bidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
UDP Throughput Advanced	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
UDP Throughput Advanced	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Traffic Mix - HTTP - Video - Voice	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Traffic Mix - HTTP - Video - Voice	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
TCP Throughput to->from N streams	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
TCP Throughput to->from N streams	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
TCP Throughput to->from 1 stream	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
TCP Throughput to->from 1 stream	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
TCP Throughput Optimized Window size	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Throughput Optimized Window size	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
TCP Throughput from->to N streams	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Throughput from->to N streams	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
TCP Throughput from->to 1 stream	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Throughput from->to 1 stream	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
TCP Throughput bidirectional	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Throughput bidirectional	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
TCP Throughput Advanced	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Throughput Advanced	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
TCP Response Time	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Response Time	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
SMTP Response Time - SMTP.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
SMTP Response Time - SMTP.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
SIP Response Time - SIP_Registration.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
SIP Response Time - SIP_Registration.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
POP3 Response Time - POP3.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
POP3 Response Time - POP3.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Network KPI to->from	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Network KPI to->from	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Network KPI Low Bandwidth	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI Low Bandwidth	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI bidirectionnal	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Network KPI bidirectionnal	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
Network KPI Advanced	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI Advanced	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI 3 COS	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI 3 COS	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Skype4B Traffic from->to	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Skype4B Traffic from->to	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Skype4B Traffic	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Skype4B Traffic	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
HTTPS Test - HTTPS_Secure_Transaction.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
HTTPS Test - HTTPS_Secure_Transaction.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
HTTP Test - HTTPtext.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
HTTP Test - HTTPtext.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
FTP Response Time - FTPget.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
FTP Response Time - FTPget.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Exchange_traffic	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Exchange_traffic	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
DNS Response Time - DNS.scr	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
DNS Response Time - DNS.scr	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
COS line qualification	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
COS line qualification	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
HTTP Video	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
HTTP Video	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Multicast video over RTP	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Multicast video over RTP	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Mesh			
Voice from->to	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Voice from->to	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
TCP Response Time	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
TCP Response Time	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Network KPI to->from	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	Yes
Network KPI to->from	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	No
Network KPI Low Bandwidth	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI Low Bandwidth	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI Advanced	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI Advanced	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI 3 COS	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI 3 COS	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes
Network KPI	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Network KPI	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes

Test Name	Probe From	Probe To	Wi-Fi Statistics Availability
Skype4B Traffic from->to	Android/XRPi Wi-Fi	XR2000/XRPi/SW EP	No
Skype4B Traffic from->to	XR2000/XRPi/SW EP	Android/XRPi Wi-Fi	Yes

Supported Protocols and Standards

This section covers supported protocols and standards by Hawkeye.

Node to Node Tests

Transaction traffic Types	Supported Traffic
Throughput measurements	UDP / TCP
Voice	G711, G729, AMR
Video	MPEG2/MPEG4 – SD and HD
Signalling Voice	SIP - H323
Emails	POP3, SMTP, Exchange
WWW	HTTP, HTTPs, FTP, DNS, Telnet
Office 365	Exchange, Skype4B media

Real Service Tests - One Arm

One arm traffic	Details
Bittorrent	Download torrent
DNS	Verify DNS server response time
DropBox	Download/upload files
Email	Send/receive emails (SMTP, IMAP, POP3)
FTP	Download/upload files to server
HTTP/HTTPS	Download/check page availability
ICMP	Advanced ping metrics
IGMP v2/v3	Join/leave Multicast and measure metrics

SpeedTest	Validate Speedtest up/down from 4000+ servers
TCP/UDP ping	Ping using TCP or UDP protocols
Traceroute	Trace routes to remote hosts

Supported Standards

Node to Node	
Protocol	Standard
IP TOS	RFC 791 y RFC 1349
Diffserv	RFC 2474, RFC 2597, RFC 2598
UDP	RFC 768 or proprietary
TCP window scale	RFC1323
TCP window retransmission	RFC1122
RTP	RFC3550
Real Services	
Protocol	Standard
HTTP	RFC2616
HTTPS	RFC2818
FTP	RFC959
DNS	RFC1034, RFC1035
ICMP	RFC792
Traceroute	RFC1393
Peer to Peer	RFC5694
SMTP	RFC821, RFC2821
POP3	RFC1939
Testing	
Metric	Standard
Throughput (goodput)	RFC2647
Jitter	RFC1889

video MDI (DF, MLR)	RFC 4445
MOS	ITU.G107
R Factor	ITU.G107 (E-model)
Benchmarking, service activation	RFC2544
Web Server notification	
Protocol	Standard
SMTP (email notification)	RFC821, RFC2821
SNMP	RFC1157

Supported Voice over IP Codecs

Codec	Data Rate	Default Datagram Size	Frame Size	Jitter Delay	Look Ahead Delay	Theoretical Max MOS
G.711u	64 kbps	20	1	2 datagrams (40 ms)	0 ms	4.41
G.711a	64 kbps	20	1	2 datagrams (40 ms)	0 ms	4.40
G.726	32 kbps	20	10	2 datagrams (40 ms)	0.125 ms	4.22
G.729	8 kbps	20	10	2 datagrams (40 ms)	5.0 ms	4.07
G.723.1 MPMLQ	6.3 kbps	30	30	2 datagrams (60 ms)	7.5 ms	3.87
G.723.1 ACELP	5.3 kbps	30	30	2 datagrams (60 ms)	7.5 ms	3.69
AMR NB	4.75 kbps ¹	14	20	2 datagrams (40 ms)	5 ms	3.16
	5.15 kbps	15	20	2 datagrams (40 ms)	5 ms	3.40
	5.9 kbps	16	20	2 datagrams (40 ms)	5 ms	3.55
	6.7 kbps	18	20	2 datagrams (40 ms)	5 ms	3.71
	7.4 kbps	20	20	2 datagrams (40 ms)	5 ms	3.82
	7.95 kbps	22	20	2 datagrams (40 ms)	5 ms	3.87
	10.2 kbps	27	20	2 datagrams (40 ms)	5 ms	4.07
	12.2 kbps	32	20	2 datagrams (40 ms)	0 ms	4.18
	6.6 kbps	18	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	8.85 kbps	24	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
AMR WB	12.65 kbps	33	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	14.12 kbps	37	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	15.85 kbps	41	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	18.25 kbps	47	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	19.85 kbps	51	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	23.05 kbps	59	20	2 datagrams (40 ms)	5 ms	MOS Score not supported
	23.85 kbps	61	20	2 datagrams (40 ms)	5 ms	MOS Score not supported

This page intentionally left blank.

CHAPTER 7

Outlier detection

Hawkeye detects outlier through the following options:

- Machine learning by using Auto Learned Threshold: Thresholds are the baselines to decide if tests are passing or failing. Set up correct thresholds to understand the test results. Auto Learn Threshold helps to calculate threshold values. Auto Learn Threshold reads the metric data for a specific scheduled test case in set of batches and calculate threshold to be set for the metric.
- Configuring Outlier per test: Often, a few isolated failed cases are normal and there is no reason to issue an alert. Hawkeye detects an outlier if a set of failed cases occurred in a configured time frame.

How do I...

This section covers the tasks that you can perform on outlier:

Configure Auto Learn Threshold	313
Configure Auto Learn Threshold Global	314
Configure Outlier	314

Configure Auto Learn Threshold

To configure Auto Learn Threshold per test, do the following:

1. Turn on **Auto Learn Threshold** for the test.
2. Configure the **Auto Learn Tolerance** percentile. The percentile is based on the probability that a measurement value can be abnormal. The percentile can be estimated from observing the data, or from domain expertise, or a combination of the two. For example, if you estimate that one in every thousand measurements is an abnormal, set the percentile to 99.9 by using the formula $(1-1/1000) * 100$. See the following table for examples:

Outlier Frequency	Percentile	Formula
1 in 100,000	99.999	$(1-1/100000) * 100$
1 in 1,000,000	99.9999	$(1-1/1000000) * 100$
5 in 100,000	99.995	$(1-5/100000) * 100$
3 in 1,000,000	99.9997	$(1-3/1000000) * 100$
P in Q	See the Formula column	$(1-P/Q) * 100$

NOTE

The default value is **Medium sensitivity Percentile 99**.

Auto Learn Threshold				Auto Learn Tolerance ⓘ		☐ Enable Outlier ⓘ
KPI From->To	Datagrams Out Of Order	1	<=	☒ On	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Delay (Ms)	100	<=	☒ On	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Jitter (Ms)	5	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Jitter Max (Ms)	5	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Loss	0.2	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>

Configure Auto Learn Threshold Global

You can set Auto Learn Threshold globally for a metric from **Administration > Global Threshold Management**. To set Auto Learn Threshold globally, do the following:

- Select  to automatically select the threshold. By default, Auto Learn Threshold is turned off.

RealTest		ICMP Test		ICMP Test		Standard deviation		20		<=		0		OFF		Autorefresh ON	
Showing 1 to 50 of 485 entries																	
Test Type:	ICMP Test			Pair Name:	ICMP Test			Metric:	Round trip time max (ms)								
Measurement Unit:	ms																
Threshold Value	400			Threshold Type	<=			Auto Learned Threshold	<input type="button" value="Off"/>								
<input type="button" value="Update Threshold"/>																	

NOTE

Outlier and Auto Learn Threshold are supported for a node-to-node topology or real service scenario only. We do not recommend to configure it for Mesh and Template. It may cause unexpected results in Threshold Calculation and Outlier dashboard.

Configure Outlier

To configure Outlier per test, do the following:

1. Select the **Enable Outlier** check box.
2. Toggle to make the **Outlier Parameters** option available.
3. Select **Outlier Parameters** to set the following outlier parameters:
 - Analysis Interval
 - Outlier Percentage

Auto Learn Threshold				Auto Learn Tolerance ⓘ		☐ Enable Outlier ⓘ
KPI From->To	Datagrams Out Of Order	1	<=	☒ On	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Delay (Ms)	100	<=	☒ On	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Jitter (Ms)	5	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Jitter Max (Ms)	5	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>
KPI From->To	Loss	0.2	<=	☐ Off	Medium sensitivity- Percentile 99	<input type="button" value="Outlier Parameters"/>

- a. Specify the time interval window (in minutes) in **Analysis Interval (minutes)** to detect a set of failed or abnormal cases as an outlier. The default interval is **30** minutes.

- b. Set the percentage value of failed cases to be considered as outlier in the specified interval. The default percentage is **50**.

KPI from->to : Datagrams Out of Order

Analysis interval (minutes):

Outlier Percentage:

Cancel
Save changes

If you want to be alerted whenever there is a five-minute window containing all failed cases, set duration to 300 seconds and level to 100 percent.

Quantization and Fudge Factors

Due to quantization, irregular measurement intervals, and round-off error, you should allow for some error when configuring the duration and level. For example, if your scheduled test interval is one minute and you want to have a better chance of having at least five items in a five minute window, set the duration to more than five minutes.

Things to consider:

- More failed cases for first few weeks: For first few weeks, the process is learning and setting the threshold by collecting data on regular basis. The more data that Hawkeye collects, more accurate is the threshold value.
- More Outliers: Outlier window moves from left to right and there are chances that outlier windows overlap for same failed cases.

This page intentionally left blank.

CHAPTER 8

Server and Probe Communications

This chapter describes the routing and ports management.

In this chapter:

Server and Probe Communications Overview	318
Hawkeye Ports for Automatic Endpoints	319
Hawkeye Scenarios for Endpoints	321
Debugging Routing Issues	326
Troubleshoot Connectivity between Endpoints	326

Server and Probe Communications Overview

The server, upon installation or upgrade, runs a script to enable required ports. This script updates the Linux system files in `/etc/sysconfig/iptables` and `etc/sysconfig/ip6tables` directories and enables the following ports for both IPV4 and IPV6:

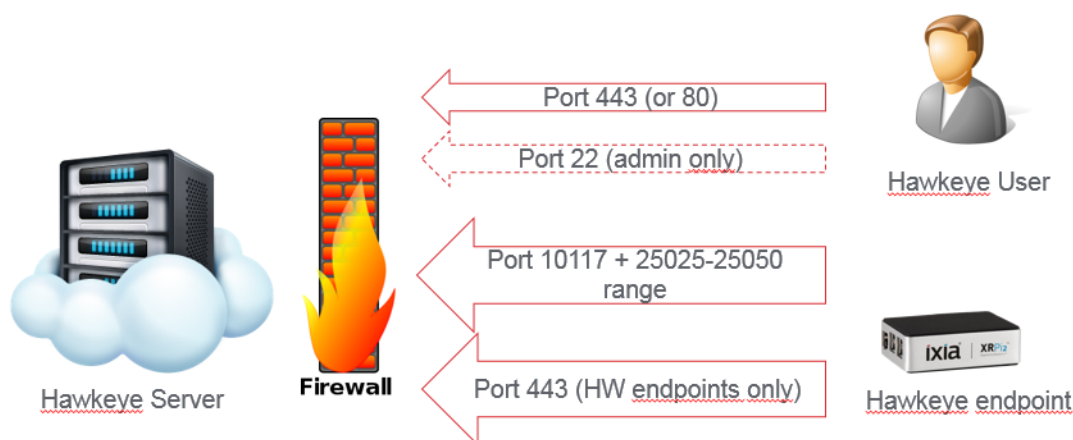
- TCP: 22, 80, 123, 443, 546, 25025-25050, 10117, 10118, 10119, 4501-4502, 27000-27009
- UDP: 123

NOTE

Port 123 is for the NTP service for accurate clock timing.

Hawkeye Ports for Automatic Endpoints

The following image displays information about the ports that are required for management and traffic for the probes/endpoints:



Description	Port(s)	Port or Port Range Modification Policy	Protocol	Directions	Description
Probes to Hawkeye server for node to node and mesh	10117, 25025-25050	Not modifiable.	TCP	From probes to server (hardware and software).	Mandatory for node to node and mesh testing.
Probes to Hawkeye server for Real Services	443	Modifiable with advanced configuration.	TCP	From probes to server (hardware probes only).	Mandatory for advanced probes administration and real services executions.
Probes to Hawkeye server for Continuous Services	10118 , 10119	Not modifiable	TCP	From probes to server (hardware and software).	Mandatory for Continuous Services executions.
Probe to probe management	10115, 10116	Not modifiable.	TCP AND UDP	Probe to Probe, bidirectional or private to public only.	Mandatory for node to node and mesh testing.

Description	Port(s)	Port or Port Range Modification Policy	Protocol	Directions	Description
				10116 port is opened by first probe (if private) to second public probe for second probe to send management packets to first probe.	UDP port is only required for tests with synchronization (network KPI, any real time traffic). Direction is always private to public in case of mix in same pair.
Probe to Probe traffic	User defined	Modifiable from administrator console in preferences.	TCP	From Probes to server.	Default to AUTO which picks any port available on probes. Need to be enforced in Hawkeye configuration in case of FW between Probes.

NOTE

When the first endpoint is private as defined in **Probe Management** web page, the first endpoint will open port 10116 to the second endpoint so the second endpoint can use this port for sending test results (plus other management information) back to the first probe.

Hawkeye Scenarios for Endpoints

When a firewall is involved in a test, the following possible testing scenarios appear, with respect to the Hawkeye server, source and destination endpoint localization in private/enterprise networks or public networks/Cloud. Each of these scenarios is detailed in a separate topic below.

For these scenarios, the source and destination endpoints are determined by the direction of the traffic. When using a reversed traffic direction, the source and destination endpoints for the scenarios are in reversed order as compared to how they appear in the user interface.

While adding the source (from) and destination (to) endpoints to the test in the test execution configuration, check that they are in the relevant network for the use case being tested. If it is not located in the correct network for that particular use case, you can change that in the endpoint management dialog:

1. Select probe management (endpoint management).
2. Select the relevant automatic endpoint.
3. Edit and change the public/private to ensure it is correctly configured.

Assumptions

Unless otherwise specified, the following assumptions are made for firewall testing:

- The Hawkeye server (Hawkeye server and the registration server) are accessible to all endpoints in a test.
- The virtual image that hosts the Hawkeye server comes with a pre-installed Registration Server. Although virtually any endpoint can act as Registration Server, we recommend to use the pre-installed one. The Hawkeye server and Hawkeye registration server may have different IP addresses.
- When multiple system components are located in a private/enterprise network, we assume that they are in the same network, with full network connectivity between them.
- When exiting the enterprise network, a device may be encountered, acting as a firewall, performing address translation and, for the most part of the testing scenarios, port translation.
- When entering the cloud, a device may be encountered, performing only 1:1 Network Address Translation (NAT), without any port translation. If a firewall is also present, the ports specified in each of the test scenarios are opened.
- The Registration Server is usually able to detect if an endpoint is located behind a firewall in an enterprise or in the public space/cloud.

Operational Concepts

For the purpose of running tests involving firewall, we consider the following working concepts:

- **Hawkeye server:** is the main server for Hawkeye, that includes Hawkeye test engine server and Registration server.
- **Hawkeye Server (C):** Central point of test execution. It is delivered as a virtual image.
- **Registration Server (RS):** A service that handles endpoints management and acts as a mediator between the Hawkeye Server and endpoints at runtime.

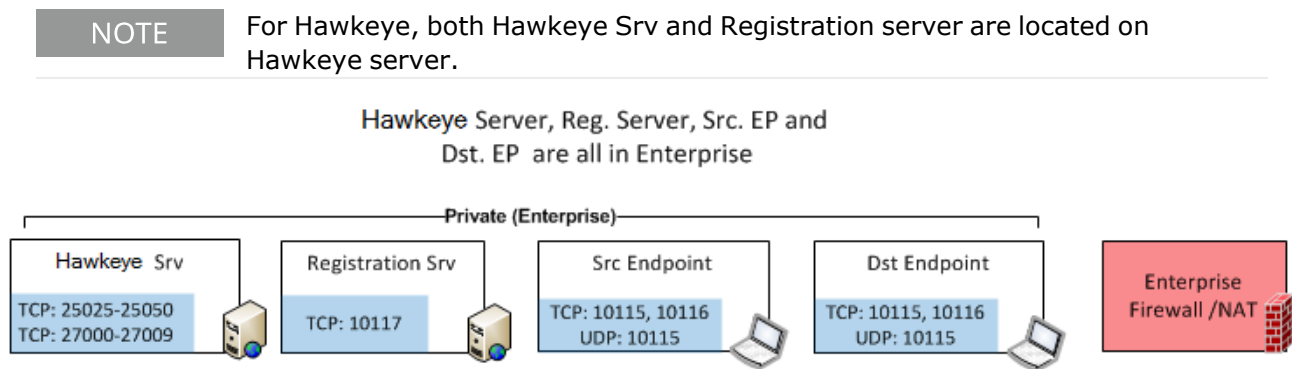
- **(Source and Destination) Endpoints:** Performance Endpoints that are installed and run on the clients' device(s).
- **Private/Enterprise:** A private, usually enterprise network, located behind a firewall, whose address is not Internet-routable and thus, needs Network Address Translation (NAT).
- **Public:** A public (and fully routable IP address) network.
- **Cloud:** A network with a private/non-routable address, yet exposed as a public IP by way of a 1:1 TCP/UDP IP-mapping (NAT) rule.

Hawkeye Server, Source and Destination Endpoints in Private/Enterprise

In this case, all types of traffic are supported.

Given that all Hawkeye components are located in the same private/enterprise network (and, as such, there is no firewall or NATing between them), no special settings must be configured. The endpoint should appear as public and/or be configured as such.

The following image illustrates the use case referencing the underlying components from Hawkeye control engine that are involved and which ports are used.



Source and Destination Endpoints in Private/Enterprise and Hawkeye Server in Public

In this case, all types of traffic are supported.

We assume that both endpoints are in the same private network and that no device is present that can alter the traffic or IPs.

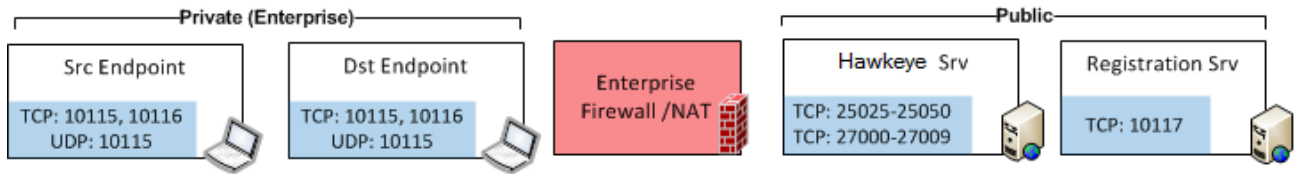
- NOTE** Make sure that the private/enterprise firewall allows for outbound connections to the public ports shown in the figure below.

The endpoints need to be set to private mode for this use case.

The following image illustrates the use case referencing the underlying components from Hawkeye control engine that are involved and which ports are used.

- NOTE** For Hawkeye, both Hawkeye Srv and Registration server are located on Hawkeye server.

Src. EP and Dst. EP in Enterprise, Hawkeye
Server, Reg. Server in Public Space



Source Endpoint in Private/Enterprise and Destination Endpoint, Hawkeye Server in Public

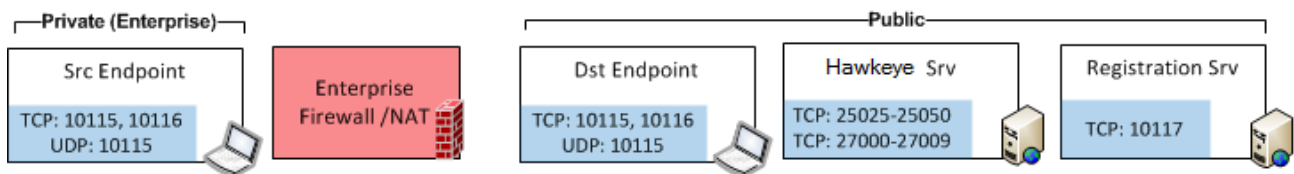
In this case, all types of traffic are supported.

NOTE

Make sure that the private/enterprise firewall allows for outbound connections to the public ports shown in the figure below

The endpoint in private (enterprise) must be configured as private, the endpoint in public must be configured as public.

Src. EP in Enterprise, Dst. EP, Hawkeye Server,
Reg. Server are in Public Space

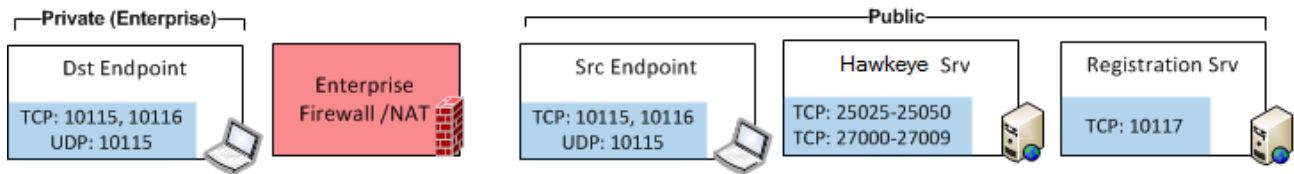


Destination Endpoint in Private/Enterprise and Source Endpoint, Hawkeye Server in Public

NOTE

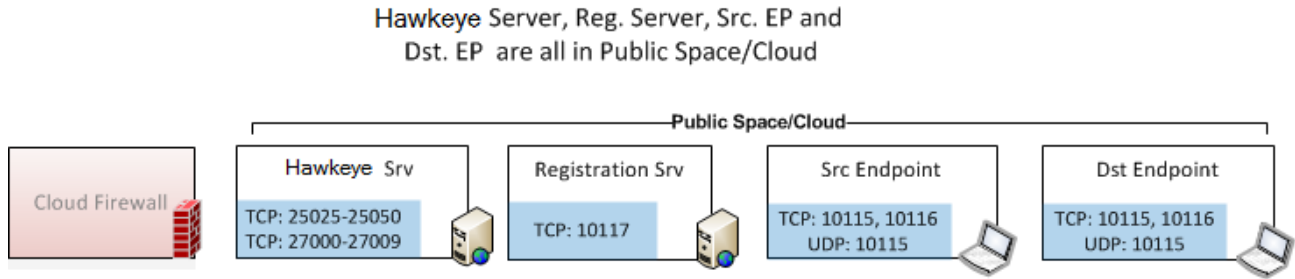
Make sure that the private/enterprise firewall allows for outbound connections to the public ports shown in the figure below.

Dst. EP in Enterprise, Src. EP, Hawkeye Server,
Reg. Server are in Public Space



Hawkeye Server, Source and Destination Endpoints in Public

No special requirements in this case.



Source and Destination Endpoints in Private and Hawkeye Server in Cloud

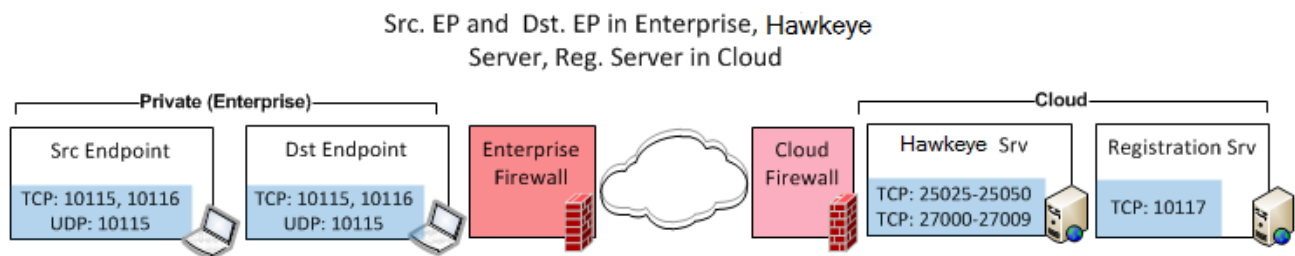
In this case, all types of traffic are supported.

For the firewall at the entry point into the cloud, make sure to open the following ports:

- TCP management ports (for the Registration Server): 10117
- TCP reporting ports (for the Hawkeye Server): 25025-25050
- TCP licensing ports (for the Hawkeye Server, only if an external license server is used): 27000-27009

NOTE

Make sure that the private/enterprise firewall allows for outbound connections to the Cloud ports shown in the figure below.



Source Endpoint in Private/Enterprise and Destination Endpoint, HawkeyeServer in Cloud

In this case, all types of traffic are supported, except for non-streaming flows over UDP.

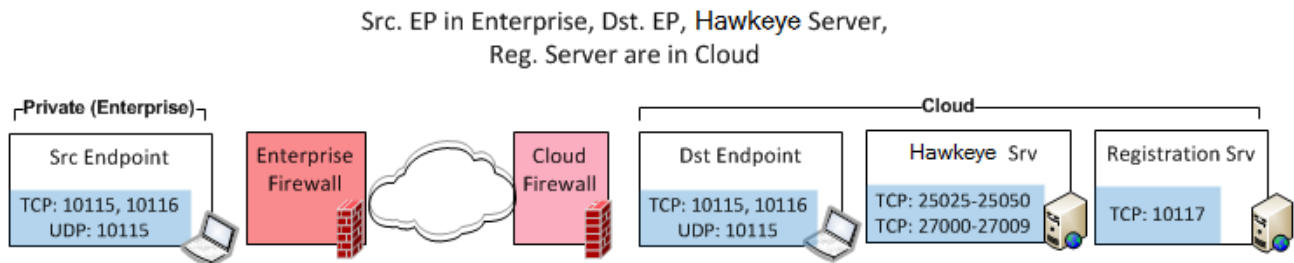
For the firewall at the entry point into the cloud, make sure to open the following ports:

- TCP management ports:
 - 10115 (for the destination endpoint)
 - 10116 (for the destination endpoint)
 - 10117 (for the Hawkeye Server)
- TCP reporting ports (for the Hawkeye Server): 25025-25050
- TCP licensing ports (for the Hawkeye Server, only if an external license server is used): 27000-27009
- UDP port: 10115

- Open into the Cloud firewall the TCP/UDP ports that you plan to use for test traffic, then go to User Preferences and configure the same range there in the port management in preferences section.

NOTE

Make sure that the private/enterprise firewall allows for outbound connections to the Cloud ports shown in the figure below.



Destination Endpoint in Private/Enterprise and Source Endpoint, Hawkeye Server in Cloud

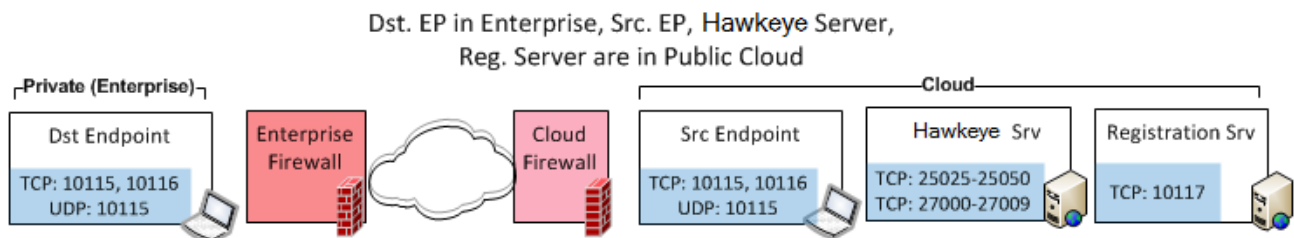
In this case, non-streaming flows over UDP and AppMix traffic are supported only if the actions mentioned in the Limitations section are performed.

For the firewall at the entry point into the cloud, make sure to open the following ports:

- TCP management ports:
 - 10115 (for the source endpoint)
 - 10116 (for the source endpoint)
 - 10117 (for the Registration Server)
- TCP reporting ports (for the Hawkeye Server): 25025-25050
- TCP licensing ports (for the Hawkeye Server, only if an external license server is used): 27000-27009
- UDP port: 10115
- Open into the Cloud firewall the TCP/UDP ports that you plan to use for test traffic, then go to User Preferences and configure the same range there in the Ports opened for the test traffic into the public / cloud firewall section.

NOTE

Make sure that the private/enterprise firewall allows for outbound connections to the Cloud ports shown in the figure below.



Limitations

By default, when the destination endpoint is behind a firewall (enterprise or Cloud), application mixes traffic fails at test run unless the following actions are performed:

- In the firewall, make sure to open the ports corresponding to the applications that you want to emulate. The table below lists the corresponding TCP ports set by default for the test traffic as defined in the port management preferences.
- If the NAT is activated, an entry must be added in the NAT table to make sure that the traffic is routed to the private IP of the destination endpoint(s). This is for test traffic only.

Debugging Routing Issues

Registering XRPi/XR2000 Endpoint to Hawkeye Server

If endpoint does not register:

1. Check routing to Hawkeye server.
2. Check ports open to Hawkeye server.
3. Use nmap (linux command) to check ports open.

```
nmap -d -p 10117,25025-25050,443 <Hawkeye server>
```
4. Confirm able to ping Hawkeye server from endpoint.
5. Confirm on the Hawkeye Server in Probe management that the new endpoint can be seen.
6. Confirm in Probe management for the cloud endpoint that a private corporate network IP and a public internet IP can be seen.
7. Confirm on the Hawkeye server in Probe Health Check that the endpoint is in a state of link up.

Troubleshoot Connectivity between Endpoints

SSH to the XRPi/XR2000 endpoint or Hawkeye server and confirm routes with “ifconfig” and “route -n” commands. The ping and traceroute commands may be helpful.

```
ifconfig
route -n
ping -I wlan0 <peer endpoint>
ping -I wlan0 www.google.com
ping -I eth0 <peer endpoint>
```

Issues with Node to Node tests can be caused by connectivity issues. Check routes and no port blocking.

SSH to endpoint and use nmap to verify path between endpoints.

```
nmap -d -p 10115,10116,10117 <peer endpoint>
nmap -d -sU 10115,10116 <peer endpoint>
```

The output will identify if a port is open or closed.

The suggested ports to verify are the following:

- Port 22 - TCP - traffic for ssh. Debugging for Admin users
- Port 123 - UDP - NTP clock source
- Port 80 – TCP – HTTP and HTTPS traffic
- Port 443 - TCP - HTTP/HTTPS traffic. Real service traffic
- Port 10115-6 - TCP – management. Hawkeye server to Endpoint. Endpoint to Endpoint management
- Port 10115 - UDP - Endpoint to Endpoint sync timing traffic for RTP traffic like Skype4B, Voice services, Network KPI
- Port 10117 - TCP - Endpoint auto-registers with Hawkeye
- Port 25025-25050 - TCP - Endpoint reporting test results
- Skype4B traffic port ranges are configurable. Vary with test traffic type. Example for Skype4B is given below:
 - UDP ports 49751 – 49999 (default Skype4B audio)
 - UDP ports 59751 – 59999 (default Skype4B video)

Verify traffic ports used in Hawkeye server in **Preferences – Traffic Port Management**. To verify routes correct run N2N traffic test between two endpoints (UDP/TCP bidirectional tests). First run ipconfig on endpoint, then run test, then run ipconfig after test and this will show packets increasing for RX/TX on interface used.

Troubleshoot Endpoints/Hawkeye Server in the Cloud

In this case, non-streaming flows over UDP and test traffic are supported only if the actions mentioned in “port limitations” are performed.

For the firewall at the entry point into the cloud, make sure to open the following ports:

TCP management ports:

- 10115 (for the source endpoint)
- 10116 (for the source endpoint)
- 10117 (for the Registration Server)

TCP reporting ports (for the Hawkeye Server): 25025-25050

UDP port: 10115

Open into the Cloud firewall the TCP/UDP ports that you plan to use for test traffic, then go to User Preferences and configure the same range there in the **Administration > Preferences > Traffic Port Management**.

Probe Bouncing IPs in Probe Management

The Hawkeye server appears to track each probe by its name in **Probe Management**. However, in **Preferences > Test Controller** table, **Probe Management Identification** allows the user to track the probe by its management IP or the UID (MAC address of interface on probe). There are cases where probes such as XR2000 VMs have been cloned at Customer sites and in Probe Management it appears that the probe is bouncing as the IP appears to keep changing in Probe Management. This happens when the multiple XR2000 VMs send the keep alive every 2-4 seconds to

the Hawkeye server, the **Probe Management** entry for the probe keeps changing its IP addresses for the probe. As the XR2000 VMs have been cloned the UID (MAC address for eth0) is always the same.

NOTE

All XR2000 VM images posted contain a blank UID.

Debugging Test Management Routing Issues

Probe overview for Routing

The probe has two separate services running that depend upon routes and ports. The first is the probe process that is used for management with the Hawkeye Server and executes node to node tests. The second process executes real service tests (if probe supports Real Services).

Probe process - Register with Hawkeye Server and Node to Node tests

Configuration script is run to register the probe with the Hawkeye server. Either the Hawkeye Server IP or Hawkeye hostname is provided. If user chooses the Hawkeye hostname, a DNS lookup is performed to obtain the IP address and from this point onwards, the saved Hawkeye Server IP is used for the 'keep alives' sent every 2-4 seconds to the Hawkeye Server. The Hawkeye Server will update the management IP for the probe each time a keep alive is received. If NAT or a gateway is involved the IP and port for the probe can change dynamically.

Every time the Real Service communicates to the Hawkeye Server when Hawkeye Hostname is configured a DNS lookup occurs before packets are sent in case Hawkeye Server VM has been moved to a different IP address.

Check NTP clock synchronization process is running on the probe if Node to Node tests fail. This can be done by ssh to the endpoint and executing the following command:

```
# ntpq -pn
```

Probe Management – Status Indicator

Key point is probe originates packets to Hawkeye Server, Hawkeye Server does not initiate communication to probe (unless manual probe). The Hawkeye Server stores the IP from the 'keep alives' and uses this IP and port for the probe for all management traffic.

Every 2-4 seconds, the probe (random TCP port) communicates to the Hawkeye Server (port 10117/TCP unencrypted) to update the probe health status web UI. Any change in the IP address of the probe will also be updated in Auto probe management.

Probe originates management (including registration) to Hawkeye Server, Hawkeye Server records this route (IP + port) then uses this for management packets back to probe. Specifically test commands and configuration and additionally reboot requests.

Real Service Command Manager process

Hawkeye Server sends the Real Service test command information to the management IP ('keep alives') defined for the probe in probe management (Server port 443/TCP encrypted). The real service command manager process (running on probe) will execute the test and then send the results back to the Hawkeye Server. The test results will be stored in the Results database and any logs from the test will be stored in the Real Service manager log files on the Hawkeye Server.

Every time the Real Service command manager process communicates to the Hawkeye Server when Hawkeye Hostname is configured. A DNS lookup occurs before packets are sent in case Hawkeye Server VM has been moved to a different IP address.

Node to Node test

When the User runs a node to node test, management communication takes place between the Hawkeye Server and the two probes. In the Test Execution UI on the Hawkeye server the user selects the 'FROM' probe and the 'TO' probe. The user selects the interface (IP) to be used for the test traffic but the actual commands and configuration are sent to the probe management IP ('keep alives' are received on).

There are three key concepts to know what ports are used when:

- All tests fall into the category of either being classified as UDP tests or TCP tests. The test results for UDP tests are sent from 'TO' and TCP tests are sent from 'FROM' probe.
- Probe is listed as **Private** or **Public** in Probe Management.
- Bi-directional tests.

The Hawkeye Server sends commands to both probes at the start of a test on port 10117. Between the two probes (port 10115 and possibly port 10116) are opened for exchange of test statistics and management of tests. The test traffic between the probes will use different ports. Once the test is complete the test results (stored in .csv files) are sent to the Hawkeye Server. If the test is a UDP test, the 'TO' probe will send the test statistics (.csv file) and log file to the Hawkeye Server. If the test is a TCP test, the 'FROM' probe will send the test statistics (.csv file) to the Hawkeye Server. The Hawkeye Server will store these log files (log rotated) and record test results in the Hawkeye Server Results database.

In Probe Management UI, for each probe a field identifies if the probe is 'private' or 'public'. If in a Node to Node test both probes are 'private' or both are 'public' only port 10115 is used between the two probes for management. Specifically the 'FROM' probe will open port 10115 to the 'TO' probe. If the probes are a mix of 'private' and 'public', the additional port of 10116 is also opened for management. If one probe is Private and the other is Public, the Private probe will open connections for ports 10115 and 10116 to the other probe for Management.

All Bidirectional tests are different in that both probes send statistics and log files back to the Hawkeye Server. This can be viewed as running two separate uni-directional tests, with each probe in both the 'FROM' and 'TO' logical position. As a result, for example if running a UDP Bi-directional test, each probe will generate traffic for one test and calculate statistics for the other test.

How to Debug Routing issues – Example: Node to Node Bi-directional test on Linux probe

The XR2000, XRPi and XR2000 VM are Linux based probes. The following identifies Linux debugging commands.

When the probe 'from' registers with the Hawkeye Server (it sends 'keep alive' message every 3-4 seconds to the Hawkeye Server), this IP (referred to as 'keep alive IP') will be used by the Hawkeye Server to send the test command information to the 'probe from' using port 10117 (this can be different to IP chosen for test). The 'probe from' then sends the test configuration to the 'probe to' using the IP addresses defined when creating the test. The probe IP sent in the test command will either be the IP selected from the pull-down menu when creating the test, or if set to 'default', will be the IP used to communicate management messages to/from the Hawkeye Server.

For the test duration, the probe 'from' and the probe 'to' will send traffic to each other. Once the test is over each probe will process its test results. Based on the rules above one probe will collect statistics and results and send to the Hawkeye Server on port 10117. The probe 'from' will wait to collect the test results from the probe 'to', then the 'probe from' will send the combined test results to the Hawkeye server using port 10117. If the 'probe from' does not receive the test results from the 'probe to' within a defined timeout period (System preferences – Test Engine – Statistics receive timeout) the probe 'from' will send its test results to the Hawkeye Server (without results from probe 'to'). If the Hawkeye server only gets test results for one direction of traffic it will report the test as an 'Error', but still report received test results. The test results will reflect the IP used for the 'probe from' and 'probe to' for the transmission of test results.

If the test results are not received by the Hawkeye Server and the test is reported as an Error, this could be due to a routing problem. Each probe can have multiple addresses assigned to it. If NAT and gateways are involved, a probe can easily have 3 different IPs and more. There can be the local physical IP, the public IP, a NAT IP and even an IPv6 address (per single interface). The user will have to know which IP to use when creating the test. If the 'default' is used for the test it is possible that this will not be correct to route traffic between each probe.

Many steps are available to identify where the routing issue is occurring.

If a Real Service license has been purchased, the real service tests of 'Port Scan', 'Path Discovery', traceroute, TCP Ping and UDP Ping can easily be used to assist in identifying the routing issue. For example, the Real Service test of 'Port Scan' could be used where the IP for each probe in the Node to Node test would run the Port Scan test where the destination would be the other probe. It has been found that the 'Path Discovery' test is particularly powerful, which includes traceroute output and calculated network delays.

For each Node to Node test ran, the Hawkeye Server has a log file of the test results. The log file (/opt/hawkeye/logs/Chariot/<testID>.log) can be checked to confirm the test results are present. A key tip is to stop/pause all other tests so the log files can easily be identified.

If a Real Service license has not been purchased, a number of commands can be run from the command line interface of each probe. The below commands will capture all management packets between probe and Hawkeye server using port 10117 and all management packets between probe to probe on port 10115, and send output to a file (-w trace_10115.pcap). Either leave out the log to file options and view in realtime or view .pcap file in wireshark.

```
# yum install tcpdump
# tcpdump -X -e -n -w trace_10115.pcap port 10115
# tcpdump -X -e -n -w trace_10117.pcap port 10117
```

The above will identify exchange of packets on port 10117 and the IP for the sent/received packets.

Confirm management port for probe to Hawkeye server and management port between probe to probe is open:

```
# nmap -d -p 10115 <IP other probe>
# nmap -d -p 10117 <IP Hawkeye Server>
```

Confirm port for management can be used between probes:

```
# traceroute -p 10115 10.146.4.238
```

While a Node to Node Bi-directional test is running the following command will constantly repeat and identify the established/transmitting connections for ports 10115 and ports 10117 every 5 seconds:

```
# netstat -atnc 5
# netstat -tc 1
Protocol Local address remote address state
tcp 0 0 10.36.32.29:43932 10.36.34.191:10117 ESTABLISHED
tcp 0 0 10.36.32.29:10115 10.36.33.18:51796 TIME_WAIT
tcp 0 0 10.36.32.29:10115 10.36.33.18:51798 TIME_WAIT
```

The remote address contains the IP for the Hawkeye Server and the other probe for the test. The state will alternate between Wait/Listen/Established when sending packets.

In order to confirm what route will be taken for a given destination IP, view the configured routes on each probe for its routing tables:

```
# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.36.32.0 0.0.0.0 255.255.252.0 U 0 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
0.0.0.0 10.36.32.1 0.0.0.0 UG 0 0 0 eth0
```

You will see routes for specific IPs such as the Hawkeye Server IP, and a route for default traffic.

To find all probes communicating to on Hawkeye server:

Run command for a minute then end with control-C.

```
# netstat -tc 4 > /tmp/10117_trace
# grep 10117 /tmp/10117_trace > /tmp/10117_trace_a
```

Same `netstat` command on probe should match entry on Hawkeye server file above.

This page intentionally left blank.

CHAPTER 9

System Optimization

The following section explains how to optimize the performance of the Hawkeye Server. It is important to understand that the Hawkeye software upgrade brings in required Debian updates compatible with the Hawkeye Server and all necessary security upgrades.

NOTE

You must not run `apt` commands on the Hawkeye server in case required libraries are changed. Contact Keysight customer support to update a package for a specific requirement.

In this chapter:

Hawkeye Services	334
Manage Configuration Database	335
Report Generation	337
Parameters Effecting Performance	337
Example of optimization of a running system	339
FPM tuning	340

Hawkeye Services

The Hawkeye system is based on a Debian (version of Linux) system. The Hawkeye server consists of following services:

- OutlierDetection
- DataCollection
- VE1Sstats
- RealServices
- ReportScheduler
- PhantomJS
- ServerDaemon
- TestEngine
- RegistrationServer
- hawkeye-fpm
- nodedv3
- httpd
- mariadb

The Hawkeye server has these services turned on. You must restart these services before you make any of the following changes:

- Change a Service configuration file (Hawkeye, Nginx, and MariaDB database)

This is required for the changes to take effect. You must ssh to the Hawkeye server to restart these services from the command line.

```
# hawkeyeServices restart
```

The Hawkeye server is constantly updating the MariaDB database and often stores information in RAM because recording a single test result will involve updating several tables in MariaDB database.

To shut down the Hawkeye Server VM in the preferred controlled way, complete the following steps:

1. ssh to Hawkeye server so command line can be used.
2. Execute the follow at the command line for immediate shutdown:

```
# shutdown -h now
```

NOTE

If a configuration file was changed, use the following commands to restart the Hawkeye server. :

```
# hawkeyeServices restart
```

Hawkeye Service

The Hawkeye service configuration file is located at `/opt/hawkeye/conf/configuration.txt`. We do not recommend you to change any values in this file without contacting Keysight Customer support.

You can change some settings from **Administration > Preferences**. Passwords are defined in a file but refer to [Change Passwords](#) to change passwords safely.

Ngix Web Server Service

You should not change the Nginx (web server) service configuration file without consulting with Ixia Customer support. The configuration files are located in the `/etc/nginx/` and `/etc/nginx/snippets/` directories. We recommend you modify the file after contacting Keysight Customer support.

MariaDB Service

The MariaDB service configuration file is located at `/etc/mysql/mariadb.conf.d/99_tuning.cnf`. Refer to [Customize MariaDB configuration](#) for instructions to change the amount of RAM allocated to the MySQL service. You must contact Keysight customer support before modifying this file. Do not modify that database manually.

Manage Configuration Database

Check Configuration Database integrity

Some organizations like to perform weekly database integrity checks. Additionally, if a sudden power loss is encountered a test may not have fully completed in updating all tables in the MariaDB database, and upon powering back up may detect an issue. In such a case the MariaDB database integrity would need to be checked and auto-corrected.

You can verify and repair the integrity of the MariaDB database by using the following command (ssh to Hawkeye server):

```
# mysqlcheck Hawkeye --user=hawkeye --password=hawkeye --auto-repair
```

A number of organizations using MariaDB for other products have a Linux cron job to schedule this command to be run once a week or month to protect the integrity of their data. We recommend you to run this command following a power outage as many activities such as, recording a test result involve updating several tables in the MariaDB database and a sudden shutdown due to loss of power would leave this updating in a partial state of completion.

Customize MariaDB configuration

When the Hawkeye Server virtual machine was created, a certain amount of RAM was allocated to it. All Hawkeye services and the MariaDB server share this RAM.

The MariaDB service is configured to use 1GB of RAM by default. This is considered insufficient for most Corporate environments.

The MariaDB database configuration parameters are located on the Hawkeye server in the file `/etc/mysql/mariadb.conf.d/99_tuning.cnf` directory and the user with privilege escalation can modify these.

Refer to the section [Hawkeye Services](#) for information on how to start and stop services safely to implement the changes mentioned below.

The most important parameter that needs to be adjusted is the parameter that sets the max amount of RAM to be used by MariaDB. The default Hawkeye server settings is to save all test results for 1 year, the amount of RAM required for processing this much data for multiple users may result in slow performance of the system. In addition to the work of saving and recycling of test results in MariaDB.

Parameter: **innodb_buffer_pool_size=1G**

The default is to limit the MariaDB to 1GB. For large systems, Keysight recommends setting this to 25% of available RAM on the Hawkeye server. For a Hawkeye Server with 16GB of allocated RAM, Keysight recommends setting this to **innodb_buffer_pool_size=4G**.

MariaDB transactions per hour

Default value for **max_connections** parameter for MariaDB database in `/etc/mysql/mariadb.conf.d/99_tuning.cnf` is 151. This defines the maximum number of concurrent connections opened against MariaDB. In the case of numerous endpoints/tests per hour (above 1000 per hour), Keysight recommends to increase this number to 1000.

Control Size of Configuration Diskspace

Available disk space was allocated to the Hawkeye server virtual machine during its creation. The MariaDB database can grow to a very large size. For large systems running a high number of tests per hour, if this goes unchecked all disk space could become used which will prevent the Hawkeye server from running tests. The size of the MariaDB database is a combination of how many endpoints/tests per day are executed and the number of days configured to retain MariaDB tests and metrics for report generation.

The default settings for Hawkeye Server will result in one year of tests results to be saved. The user is highly recommended to configure the number of days to store test results to keep the system manageable. There are two suggested ways to calculate how much disk space will be used by the system daily:

1. A rough rule to calculate disk space required: An approximate estimate will be 1 test = 2 kilobytes (KB) of data. So, 1,000 tests per day will generate 2 MB of data and 1,000,000 tests will generate 2GB of data.
2. Once system configured with all endpoints and scheduled tests, the daily use of disk space can be calculated. By using ssh to Hawkeye server, then running the command "df -h", then 24 hours later run the same command and see what the daily growth of the MariaDB database is.

If the disk space is growing rapidly at 100 MB a day and the Hawkeye server virtual machine was created with a virtual disk space of 30 GB this means after 300 days the available disk space will be filled.

On the Hawkeye server under **Administration > Preferences** there are two parameters:

- **Number of days for database retention: 365**
- **Number of days for database retention for detailed metrics: 180**

These two parameters define the recycling and retention period for keeping test results and metrics. For the example above, Keysight recommends you to set the **Number of days for database retention** and **Number of days for database retention for detailed metrics** to 180 days (6 months) to allow for a large safety margin.

The **Number of days for database retention for detailed metrics** are disk intensive and the retention period should be less than the **Number of days for database retention**. For systems under heavy load (>100000 tests a day) it is recommended to change this metric to less than 30 days, if possible less than 10 days is highly recommended.

The parameter for **Number of days for database retention** of admin elements can be reduced to as low as 5 days as it is mostly used for log tracking.

Report Generation

Generating and scheduling reports can be very CPU intensive.

There are many configurable **preferences** that will impact report generation.

The parameter **Max report generation time** sets a maximum amount of processing allowed to generate a report. If this time is exceeded the report is abandoned.

In the **Advanced** section of **preferences**, the parameter **Maximum number of graphs in a saved or scheduled report** sets the maximum number of graphs to be included in a report. After the maximum limit is reached, the report generation is complete.

Manage Disk Storage for Saved Reports

Presently, it is the responsibility of the user to manage disk storage on the Hawkeye Server being used by reports. Over time the disk space of saved reports has been seen at several Customer sites to use substantial amounts of disk space.

Once a user has a SSH session to the Hawkeye server the following Linux command can be useful to maintain deletion of all reports older than 365 days. Changing the value 365 below will change the number of days that reports are kept.

NOTE

This is a temporary process that will not survive a Hawkeye Server restart but will automatically delete all files older than the configured number of days.

```
# find /opt/hawkeye/WebServer/SavedReports/ -mtime +365 -exec rm -rf {} \;
```

Parameters Effecting Performance

Hawkeye Timeout for Receiving Statistics

In the **Test Engine** section of **Preferences** the parameter **Statistics receive timeout (seconds)** defines the max amount of time the Hawkeye server will wait for an endpoint to send the test results once a test has completed.

Test Timeouts

In the **Test Controller** section of **Preferences** there are many parameters defining max test durations. After a timer expires Hawkeye server ends the test and cleans up.

In the **Advanced Options** section, the parameter **Maximum time processing Node to Node and Mesh tests** specifies how many seconds after test duration is over before the Hawkeye server ends the test and cleans up.

There are two parameters for Real Services. In the **Test Controller** section the parameter **Real Test Max duration** defines how long the endpoint processes the test, after which time the endpoint terminates the test. In the **Advanced Options** section, the parameter **Maximum time processing Real Service tests** specifies how many seconds after test duration is over before the Hawkeye server ends the test and cleans up.

Auto Refresh of Web Pages

The user needs to be aware that the autorefresh of web pages impacts CPU usage and must not be too frequent. There are three autorefresh timers, one for the main dashboard, one for the map display, and one for other web pages such as floorplans and test execution pages.

There are two parameters in the **Main** section of preferences.

The parameter **Dashboard autorefresh** enables or disables the automatic refresh of the main dashboard statistics. The second parameter is **Dashboard autorefresh interval**, which defines how often the statistics for the main dashboard are re-calculated and displayed. We recommend you to keep this above 30 seconds.

The parameter **Refresh Execution List Timer** specifies how many seconds between updating the test execution web pages. It is recommended to keep this value above 10 seconds for system performance.

The parameter **Map update frequency in seconds** impacts how frequently the maps are re-calculated. It is recommended to keep this above 30 seconds. The parameter **Refresh list timer value** impacts other web pages that support autorefresh. We recommend you to keep this above 10 seconds.

Max Concurrent Tests in GUI

There is a parameter **Max Concurrent Tests in GUI** in the **Main** section of **Preferences** that defines how many tests are allowed to be running concurrently. This parameter, when set correctly, will ensure no issues with tests failing to run because the number of licensed tests has been reached. This parameter effectively manages the maximum number of simultaneous tests and will queue up those tests that need to run. This also indirectly allows the user to define how much CPU processing is allocated to processing test results.

Map Refresh

The frequency for updating maps can be CPU intensive. There are two parameters under **Preferences** in **Administration** that defines this. First the parameter **Map Report** must be enabled or disabled. If disabled no processing of maps to be displayed will take place. In the GUI section of **preferences** the parameter **Map update Frequency in seconds** defines how frequent the processing or refreshing of maps will be performed. As this impacts the CPU we advise not setting this value to less than 30 seconds.

Probe Healthcheck Polling Interval

In the **Advanced Options** section, the parameter **Test Controller: Polling interval** defines how often the test controller process will poll each endpoint to check its status. We recommend you to keep this above 4 seconds. This impacts **Probe healthcheck** feature and reporting alarms for endpoint down (email/SNMP traps).

Log Retention Minutes

In the **Logs** section, there are two parameters used to define the test log retention time on the Hawkeye server. The **Log Retention minutes** specifies how many minutes to retain Hawkeye test logs in the directory /opt/hawkeye/logs/Hawkeye. The parameter **Test Engine Log retention** specifies how many minutes to retain the endpoint test logs in /opt/hawkeye/logs/Chariot.

Automatic Endpoint Retry of Tests

Hawkeye has a feature to automatically retry a test that fails to execute. This is useful in unstable networks. However if a Customer has limited licenses and has carefully scheduled a number of tests to maximize the available licenses enabling this feature may result in increased licenses being used at once.

Under **Administration** in **Preferences** for the **Test Engine** there is a parameter **allow_pair_reinit_run** which is used to enable/disable the automatic retry of failed tests. If enabled and a test fails to start due to connection issues, the test will retry in **pair_reinit_retry_interval** seconds. The test will be tried a further **pair_reinit_max_run** number of times. The retry interval after the first attempt is defined by **pair_reinit_retry_interval_run** seconds.

Example of optimization of a running system

After Hawkeye server has been running for a while, it helps to review Optimization. Confirm system resources and adjust configuration.

From the command line on the Hawkeye server (ssh or bitwise) determine resources used matches configuration:

```
# cat /proc/meminfo
```

The value for **MemTotal** identifies allocated space example. 4 Gb.

The value of **MemFree** identifies how much free RAM is available, example 256 Kb. This shows with a running system how much RAM is used to run current scheduled tests and how much RAM is available for other activities such as generating reports.

```
#df
```

This command identifies how much disk space is being used, for example 54 Gb used out of 256 Gb disk drive.

For test results stored (in this example 54 Gb) and having only 4 Gb of available RAM is undersized.

```
# lscpu
```

This indicates for example we have 2 Core CPU's

This example has two CPU's, 4 Gb RAM, and a 54 Gb database. To process reports for such a large database this is considered undersized.

As the Hawkeye server has an approximate 54 Gb database to process the default MariaDB configuration needs to be changed. It is advised to configure 25% RAM for MariaDB and to increase the number of concurrent accesses to the MariaDB database. This will help report generation. The following changes will be made for this example:

Increase RAM allocated to MariaDB database and increase allowed concurrent connections.

```
# nano /etc/my.cnf.d/tuning.cnf
max_connections=1000
innodb_buffer_pool_size=1G
```

In this example due to limited processing resources reduce number of days metrics kept for so reports can be generated more quickly.

On the Hawkeye Server UI, in the **System Preferences > Main**, make the following changes to keep just 6 months of test results.

- Set **Number of days for database retention** to 180.
- Set **Number of days for database retention for detailed metrics** to 180.

If the number of scheduled tests are close to maxing out the number of licenses, we recommend you to disable automatic retries of failed tests with the following change. In the **System Preferences > Test engine**, make the following change:

- Set **Allow_pair_reinit_run** to 0.

To reduce amount of individual log files for N2N tests, complete the following:

- In the **System Preferences > Logs**, set **Log retention Minutes** to 120.

When creating or scheduling a report, select specific metrics using **options** feature instead of all metrics by default. This will allow you to customize the metrics to be included in the report. Fewer the metrics means less processing resources. Thus, less time is needed to generate the reports.

FPM tuning

Starting with Hawkeye 4.0 php-fpm thread, tuning is available. This allows the Hawkeye system to scale performance better and to balance both the load of the system and the resources available to it. Tuning of the php-fpm process can be performed with the following file:

```
/opt/hawkeye/conf/fpm.d/tuning.conf
```

The tuning file you will edit by uncommenting (" ; ") the variables listed below and changing them to the following tuning starting points based on the following table. Use the table with the following logic to find the correct starting points:

If your system has A number of endpoints connected or B number of tests running per hour and has C for system resources, use the following values as starting points for tuning your system.

After making the changes, run the `hawkeyeServices` command to restart the services for your changes to take effect.

#Endpoint	Tests / Hour	Sys. Resources	pm.max_children	pm.start_servers	pm.min_spare_servers	pm.max_spare_servers
25	<150	4 vCPU 8GB RAM	10	2	2	5
100	<1000	6 vCPU 16GB RAM	20	6	2	10

400	<10000	8 vCPU 24GB RAM	30	7	5	10
-----	--------	--------------------	----	---	---	----

NOTE

For systems with 8 GB of RAM, if your MariaDB innodb_buffer is set above 4GB, reduce it to 4GB before modifying the FPM tuning file. Otherwise, you will be at risk of running into an Out of Memory Error.

Example Config file:

```
[root@hawkeye-server ~]# cat /opt/hawkeye/conf/fpm.d/tuning.conf
[hawkeye]
; Choose how the process manager will control the number of child processes.
; Possible Values:
; static - a fixed number (pm.max_children) of child processes;
; dynamic - the number of child processes are set dynamically based on the
; following directives:
; pm.max_children - the maximum number of children that can
; be alive at the same time.
; pm.start_servers - the number of children created on startup.
; pm.min_spare_servers - the minimum number of children in 'idle'
; state (waiting to process). If the number
; of 'idle' processes is less than this
; number then some children will be created.
; pm.max_spare_servers - the maximum number of children in 'idle'
; state (waiting to process). If the number
; of 'idle' processes is greater than this
; number then some children will be killed.
; Note: This value is mandatory.
;pm = dynamic
; The number of child processes to be created when pm is set to 'static' and the
; maximum number of child processes to be created when pm is set to 'dynamic'.
; This value sets the limit on the number of simultaneous requests that will be
; served. Equivalent to the ApacheMaxClients directive with mpm_prefork.
; Equivalent to the PHP_FCGI_CHILDREN environment variable in the original PHP
; CGI.
; Note: Used when pm is set to either 'static' or 'dynamic'
; Note: This value is mandatory.
pm.max_children = 10
; The number of child processes created on startup.
; Note: Used only when pm is set to 'dynamic'
; Default Value: min_spare_servers + (max_spare_servers - min_spare_servers) / 2
pm.start_servers = 2
; The desired minimum number of idle server processes.
; Note: Used only when pm is set to 'dynamic'
; Note: Mandatory when pm is set to 'dynamic'
pm.min_spare_servers = 2
; The desired maximum number of idle server processes.
; Note: Used only when pm is set to 'dynamic'
; Note: Mandatory when pm is set to 'dynamic'
pm.max_spare_servers = 10
; The number of requests each child process should execute before respawning.
; This can be useful to work around memory leaks in 3rd party libraries. For
```

```

; endless request processing specify '0'. Equivalent to PHP_FCGI_MAX_REQUESTS.
; Default Value: 0
;pm.max_requests = 500
; The timeout for serving a single request after which the worker process will
; be killed. This option should be used when the 'max_execution_time' ini option
; does not stop script execution for some reason. A value of '0' means 'off'.
; Available units: s(econds)(default), m(inutes), h(ours), or d(ays)
; Default Value: 0
;request_terminate_timeout = 0
; The timeout for serving a single request after which a PHP backtrace will be
; dumped to the 'slowlog' file. A value of '0s' means 'off'.
; Available units: s(econds)(default), m(inutes), h(ours), or d(ays)
; Default Value: 0
;request_slowlog_timeout = 0
; The log file for slow requests
; Default Value: not set
; Note: slowlog is mandatory if request_slowlog_timeout is set;
;slowlog = /var/logs/php/slow.log
; Set open file descriptor rlimit.
; Default Value: system defined value
;rlimit_files = 1024
; Set max core size rlimit.
; Possible Values: 'unlimited' or an integer greater or equal to 0
; Default Value: system defined value
;rlimit_core = 0
; Chroot to this directory at the start. This value must be defined as an
; absolute path. When this value is not set, chroot is not used.
; Note: chrooting is a great security feature and should be used whenever
; possible. However, all PHP paths will be relative to the chroot
; (error_log, sessions.save_path, ...).
; Default Value: not set
;chroot =
; Chdir to this directory at the start. This value must be an absolute path.
; Default Value: current directory or / when chroot
;chdir = /var/www
; Redirect worker stdout and stderr into main error log. If not set, stdout and
; stderr will be redirected to /dev/null according to FastCGI specs.
; Default Value: no
;catch_workers_output = yes
Defaults:
pm.max_children 10
pm.start_servers 2
pm.min_spare_servers 2
pm.max_spare_servers 5
Servers running 100-250 tests per hour.
pm.max_children 20
pm.start_servers 6
pm.min_spare_servers 2
pm.max_spare_servers 10
Vision Appliance running 12,000 tests per hour
pm.max_children 30
pm.start_servers 7
pm.min_spare_servers 5
pm.max_spare_servers 10

```

CHAPTER 10

Security

This section provides information on the corporate security that Hawkeye provides.

Another layer of security is the use of firewalls to block specific ports for ingress/regress to the endpoints and Hawkeye server which is explained in the Routing section.

The administrator can set the timeout period for the Hawkeye client (User's web access to Hawkeye server) by setting a parameter on the web page **Administration > Preferences > GUI > Max Idle Timer**.

The Hawkeye server by default uses HTTP (port 80) for web access. This can be changed to secure HTTPS (port 443) access if required. If a user wants to do this they are recommended to contact Keysight Customer Support for the steps as it involves changing two configuration files and possibly disabling port 80 in iptables.

In this chapter:

Secure Access to Hawkeye Server	344
Hawkeye User Authentication	347
Change Passwords	350
Security Audit Logging of Users	350
Hawkeye Server SSL customization	350

Secure Access to Hawkeye Server

Hawkeye Server by default is enabled for HTTP access using port 80. Some organizations prefer to block HTTP (port 80) access and only allow HTTPS (port 443). The Hawkeye Server has a configuration file `/opt/hawkeye/conf/configuration.txt` which has the parameter `WebServerPort` set to 80. You can edit this file and change this to 443 to enforce HTTPS for browser access. This will force all web browser access to the Hawkeye server to use HTTPS but Hawkeye server can still use port 80 by the Nginx process. In order to prevent all HTTP access you must edit the file `/etc/nginx/snippet/hawkeye-server.conf` and comment out the first two lines, `listen 80 default_server;` and `listen [::]:80 default_server;`, by preceding it with `#` symbol.

After you change either one or both files, stop the Hawkeye service and restart it to apply the changes. Refer to the section [Hawkeye Services](#) on how to do this.

It is not recommended, but for the advanced security conscious organization the SSL protocol and the cipher algorithms to be used can be configured/restricted by changing the `/etc/httpd/conf.d/ssl.conf` file. Examples of changes are to exclude SSL protocol 1.0 and 1.1 and only use 1.2. Another example is to prioritize a list of ciphers to be used (negotiated) for the connection. Important to note as this is a Linux system file not maintained by Hawkeye it can be replaced by an upgrade thus requiring the user to restore any previously saved changes to the file following the upgrade.

Customer Certificates for Hawkeye Server

When using secure access to a Hawkeye Server (HTTPS), you can avoid a certificate warning when logging into the Hawkeye Server web page by using a certificate. The Organization may have port 80 blocked for security or may have a Corporate requirement only to use HTTPS for the Organizations web servers. There are two steps:

- Generate a signed SSL certificate for the Hawkeye Server.
- Configure the Hawkeye Server to use the certificate.

The following sections describe this process.

Create Certificate Signing Request (CSR) on Hawkeye Server

Users seeking to purchase a signed SSL certificate from a Certification Authority will require a Certificate Signing Request be generated by the Server with both a Public and Private key. While pursuing, the signed SSL certificate, a customer will need to generate a Certificate Signing Request (CSR) file to be provided to the Certification Authority (CA) as part of their application.

To generate the CSR from the Hawkeye server you will need to log into the server via SSH and generate a configuration file (for the now required SAN extension) and run a command to generate the certificate request to be sent to a CA authority.

```

root@xrpi-auto-qa-1:/tmp# cat san.crf
[req]
prompt = no
default_bits=2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
C = US
ST = NC
L = Raleigh
O = yourOrganization
CN = hawkeye.yourorganization.com
emailAddress = sam.smith@yourorganization.com
[v3_req]
subjectAltName = @alt_names
[alt_names]
DNS.1 = hawkeye.yourOrganization.com
DNS.2 = www.hawkeye.yourOrganization.com
DNS.3 = anotherCert.yourOrganization.com
root@xrpi-auto-qa-1:/tmp#

```

```

openssl req -new -newkey rsa:2048 -nodes -out YourServerName.csr -keyout
YourServerName.key

```

NOTE

Some attributes may be changed to meet the customer security standards or the recommendations or requirements of the CA. For example, `rsa:2048` indicates 2048 bit key.

Upon completion, your system will have two new files in the directory from which you ran the `openssl` command. `YourServerName.csr` and `YourServerName.key`. Please move `YourServerName.key` to `/etc/pki/tls/private/` for use later.

The `YourServerName.csr` contains your Certificate Signing Request to be submitted to the Certification Authority of your choice.

You can view the contents of your certificate request before sending with the following command:

```

# openssl req -noout -text -in YourServerNameServer.csr

```

```

root@xrpi-auto-qa-1:/tmp# openssl req -noout -text -in YourServerName.csr
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=US, ST=NC, L=Raleigh, O=yourOrganization, CN=hawkeye.yourorganization.com/emailAddress=sam.smith@yourorganization.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:de:b3:6c:62:52:4b:9a:f6:66:32:30:94:76:f3:
      fb:bd:32:0b:29:b8:f2:7e:ac:3f:ac:cb:f3:2b:4c:
      f5:75:ba:e7:65:8f:a3:5e:66:1b:c7:e4:e5:7e:af:
      47:3b:20:01:30:29:48:6b:0e:55:38:74:52:a7:58:
      be:5c:1f:97:14:cd:c4:58:8e:6a:48:e3:18:c3:5a:
      dc:c4:1c:3c:3f:29:67:72:5d:00:72:aa:ac:b7:70:
      53:1e:17:4d:cf:bf:bb:81:bf:8b:bb:d8:57:9d:07:
      78:dc:63:fe:13:ba:68:17:24:d4:c2:15:69:4f:b9:
      34:24:7f:a4:f2:4e:94:e5:9b:68:98:99:35:2a:d1:
      ed:b4:1c:67:3e:c2:d6:f5:20:82:f3:bf:fc:01:61:
      95:88:e7:6c:41:9c:d1:84:57:30:04:5f:45:73:1a:
      5d:f7:75:44:3d:b2:6f:e7:b7:47:e1:c9:ad:7e:9e:
      ab:18:6c:83:38:7e:33:61:eb:8f:f5:77:b0:a7:d1:
      07:da:da:f8:67:fa:86:31:00:6a:82:e1:63:a7:52:
      6f:74:1b:a0:c7:76:69:c7:72:ca:d3:bb:34:f4:de:
      88:da:e9:1c:83:b4:7f:2b:db:63:9f:53:59:03:82:
      d0:71:0c:f6:8b:53:c3:06:40:7a:f6:12:f3:c9:72:
      e7:7d
    Exponent: 65537 (0x10001)
  Attributes:
  Requested Extensions:
    X509v3 Subject Alternative Name:
      DNS:hawkeye.yourOrganization.com, DNS:www.hawkeye.yourOrganization.com, DNS:anotherCert.yourOrganization.com
  Signature Algorithm: sha1WithRSAEncryption
    20:54:8a:61:53:0c:69:95:94:74:15:1a:e0:87:af:e4:03:7b:
    7d:b9:41:2e:14:35:05:de:0f:be:9c:b0:ea:f8:c2:4b:c0:ef:
    f4:0d:94:ae:bc:ff:4f:21:44:94:24:2a:76:e7:4c:fb:9e:38:
    77:36:62:c3:e6:08:ce:9d:bb:ad:2a:91:4f:74:00:6b:fa:1f:
    50:1e:b3:9b:b3:27:cc:1a:dc:80:fe:4f:b1:61:69:8f:f0:41:
    fa:59:d2:fa:4c:27:e3:a8:15:4a:78:e2:2a:53:9f:f3:48:c4:
    c7:1f:c4:dd:08:18:47:ec:01:c4:55:0c:59:99:0c:b1:a0:3a:
    65:9f:08:7e:e0:57:bc:66:ec:fa:9b:39:e6:21:51:2f:10:84:
    03:31:cd:39:d2:4d:cb:db:83:34:28:f1:84:80:58:78:12:be:
    d3:d9:c3:4d:50:2f:d3:05:30:6e:30:de:38:b5:df:69:c8:e8:
    62:78:00:06:60:63:a7:06:a8:97:67:a1:45:92:31:6b:2e:92:
    6e:34:3c:38:7c:c5:ef:1a:c7:a8:c1:ec:e6:65:1c:a2:49:55:
    f2:77:83:4b:a5:12:2e:b9:4a:d1:54:0d:da:e6:47:d9:50:e8:
    bf:62:cc:2b:7f:96:11:83:87:f6:3b:c0:e3:09:76:eb:c4:c2:
    99:fc:eb:df
root@xrpi-auto-qa-1:/tmp#

```

Add signed SSL certificate to Hawkeye Server

If your certificate was delivered with the Root certificate and Intermediate certificate as separate files from the Server certificate, the files must be bundled into a single file. You can do this with the following command by replacing the file names with the names of your certificates.

```
# cat your_domain.crt intermediate.crt root.crt >> hawkeye-bundle.crt
```

The CA Signed SSL Certificate (.crt file) will need to be copied in /etc/ssl/certs/. The associated key file must be copied to /etc/ssl/private/

NOTE

Use cp (copy) to place the files in their new directories. Do not use mv (move) for this purpose.

After the files are in the correct directories, edit the following file with vi or your favorite Linux text editor:

```
vi /etc/nginx/snippets/hawkeye-ssl.conf
ssl_ciphers HIGH:!3DES:!aNULL:!MD5:!SEED:!IDEA;
ssl_protocols SSLv3 TLSv1.2 TLSv1.3;

# select our certificates.
# We default to the ones created
# during install (snakeoil),
# but should be replaced
# with proper customer certs as:
#ssl_certificate <path_to_pem>;
#ssl_certificate_key <path_to_key>;
include snippets/snakeoil.conf;
```

Uncomment the following lines and update the path to point to your signed files:

```
ssl_certificate <path_to_pem>;
ssl_certificate_key <path_to_key>;
```

NOTE

Do not remove the ; at the end of each line.

Comment out the following line to stop using the provided self-signed certificates.

```
# include snippets/snakeoil.conf;
```

Add the following lines to the bottom of /usr/local/Ixia/endpoint.ini

```
NG_SSL_CERTIFICATE_FILE_PATH /etc/ssl/certs/<file.crt>
NG_SSL_PRIVATE_KEY_FILE_PATH /etc/ssl/private/<file.key>
```

NOTE

If endpoint.ini does not exist in /usr/local/Ixia, it can be created by running `cp /usr/local/Ixia/endpoint.ini.newest /usr/local/Ixia/endpoint.ini` command.

After editing both files, restart the Hawkeye Services with the `hawkeyeServices` command.

Following the restart of all services you should be able to reload the Hawkeye website by going to <https://www.YourServerName.com>. This time you should not be prompted about having an unsigned certificate.

Hawkeye User Authentication

You can authenticate Hawkeye users in the following ways:

- Users defined locally;
- Users defined in a LDAP Server;
- Users defined in a secure (Keysight) login server.

There is a parameter in **Administration > Preferences**, which defines the **system Authentication Mode** to be used.

Users Defined Locally

The administrator can define new users in **Administration > System Users Management**. The **System Authentication Mode** is set to **Local** for this authentication type.

The administrator can enforce complex passwords by setting a parameter in **Administration > Preferences > Main > Enforce Complex Password**.

New users will be prompted to change their password on first log in.

Sysadmin can force user password changes on next log in by enabling the **Force Change Password** option in a user profile under **System Users Management**.

Accounts will be locked out for 5 minutes after 5 unsuccessful log in attempts.

If password complexity is enabled, users will be forced to comply with complexity standards on next password change.

Users Defined in LDAP Server

In **Administration > Preferences**, the administrator can configure an LDAP server for authenticating users. Hawkeye supports using both regular LDAP and secure LDAP servers. The **System Authentication Mode** is set to **LDAP** for this authentication type.

In **Administration > Preferences**, define the following parameters to use the LDAP server:

Preference	Description	Example
LDAP server address	LDAP Server (hostname or ip address) or a list of comma delimited servers.	dc1.hawkeye.labs
LDAP Domain DN	Domain DN in the format of either example.org or dc=example,dc=org	hawkeye.labs
LDAP - Users Path	The user account folder in the LDAP tree. Example - CN=Users	ou=Users
LDAP - User Attributes	The comma separated list of user attributes to search for and compare the login against in the LDAP element.	uid,cn,sAMAccountName
LDAP - Enable secure LDAP (LDAPS)	0 - sets regular LDAP connection 1 - sets LDAPS connection	1
LDAP - Auto create Hawkeye	0 - Users must be created in Administration > Users before they can	1

user	authenticate using the LDAP server. 1 - Auto create Hawkeye user (if it does not exist already) when Authentication Mode is set to LDAP and user is authenticated successfully	
LDAP - Enable group based authentication	0 – If the user exists in LDAP they can login. 1 - Authenticate users based on their existence in the LDAP Group Path specified.	1
LDAP Group Path	Defines the group path as defined in the LDAP tree. (Used only when LDAP group based authentication preference above is set to 1)	cn=QualityControl,ou=Groups
LDAP Bind DN	Bind DN for connecting to LDAP. Leave it as empty for anonymous bind. (Used only when LDAP group based authentication preference above is turned on)	CN=read-admin,DC=hawkeye,DC=labs
LDAP Bind DN Password	Password of LDAP Bind DN. Leave it as empty for anonymous bind (Used only when LDAP group based authentication preference above is turned on)	Hard2Guess

Refer to your Organizations LDAP server configuration to know the DN parameters that you must specify. These can include a combination of: OU, UID, CN and DC/DC. The values are not case sensitive.

Users Defined in Keysight Login

The Keysight **Login** is a service allowing users to be authenticated (email/password validation) for using a Hawkeye server. The Keysight Login service manages and validates passwords for an email address. The user will still have to be pre-added to the local Hawkeye server by sysadmin. If Keysight Login is enabled, and a user attempts to login to the Hawkeye server. First the user is confirmed to be defined in the local Hawkeye database, then the Hawkeye server queries the Keysight Login service to confirm the user entered a valid password (authentication).

The Keysight login feature for authenticating users is applied when the **system Authentication mode** is set to **Ixia**. To use the Keysight Login service, the administrator defines a new user in the **Administration > System Users Management** and the user is defined with an email address that ends in **engineer@ixiacom.com**. This allows a defined user to access the Hawkeye server. The user **engineer** must then access the Keysight login server and register, which means providing an email address and password. The Keysight Login service will then send an email to the email address provided requiring confirmation to make the user active.

When the user **engineer** attempts to login, the Hawkeye server contacts Keysight to validate the password provided for the login. If the username and password match in the secure Keysight Authentication server, the user **engineer** is allowed to login. The privileges allowed to the engineer is determined by the sysadmin **administrator** that defined the account for the engineer in the **Administration > System Users Management** (refer to [Users and Groups Management](#)).

NOTE

In the **Login** you must provide a valid email address registered at <https://login.ixiacom.com>.

Change Passwords

Modify MySQL Password

The MySQL database for the Hawkeye server uses a default username/password of **hawkeye/hawkeye**. For Corporate security, we recommend you to change the default passwords.

To change the password for the MySQL database for Keysight and root to access mySQL to run the Hawkeye server do the following:

1. Shutdown Hawkeye services from Hawkeye server console. Use the command below to stop the services:

- `# systemctl stop httpd`

NOTE

Stopping the httpd service, stops Apache, which is the mechanism to access MySQL.

2. Change your password with MySQL command line using the following commands:

- `# changeDBpasswd`

NOTE

You have changed the root and hawkeye database account passwords.

Change System Administrator Password

Use a web browser to log into the Hawkeye server. Select the web page for **system users management** under **Administration**. There will be a user entry for sysadmin. Select the pencil to edit the settings for sysadmin. Once the edit button is selected the bottom pane will allow the password for sysadmin to be changed.

Change Hawkeye Server Virtual Machine Passwords

The default password for the Hawkeye server virtual machine is ksuser/keysight. Privilege escalation is available with the `su -` command and the password keysight.

To change the ksuser password, ssh to the Hawkeye server and run the `passwd` command. While logged in to the cli as ksuser, you can escalate privileges with `su -` and then run the `passwd` command.

Security Audit Logging of Users

Many organizations require audit logs be kept of users activities on systems for security purposes. Hawkeye maintains an audit trail of all users logging in and logging out of the Hawkeye Server. It also tracks which user made changes to which system parameters. These audit logs can be seen from the Hawkeye Server web GUI under **Administration > User Trail**.

Hawkeye Server SSL customization

The Hawkeye Server utilizes SSL in its operations. The user can configure Hawkeye server to use only the highest protocols. The configuration file, `/etc/nginx/snippets/hawkeye-ssl.conf`, can only be

edited with privilege. Use `su -` to escalate privilege.

The example below will force Hawkeye Server to only use TLS 1.2 and 1.3.

```
# vi /etc/nginx/snippets/hawkeye-ssl.conf
ssl_ciphers HIGH:!3DES:!aNULL:!MD5:!SEED:!IDEA;
ssl_protocols TLSv1.2 TLSv1.3;

# select our certificates.
# We default to the ones created
# during install (snakeoil),
# but should be replaced
# with proper customer certs as:
#ssl_certificate <path_to_pem>;
#ssl_certificate_key <path_to_key>;
include snippets/snakeoil.conf;
```

To apply the changes please run that `hawkeyeServices` command.

NOTE

After the service restarts, the Hawkeye email client will be blocked from using SSL and is forced to only allow TLS. You have to modify the email preferences to use TLS. This also applies to web browsers and all communication on port 443.

This page intentionally left blank.

CHAPTER 11

Advanced Administration Guide

This section covers the advanced administration steps of Hawkeye server. You should have administrator access to the server hosting Hawkeye to be able to use this.

The Hawkeye system is currently based on the Debian 12 OS. The main hawkeye software is installed in /opt/hawkeye . The status of the assorted services can be shown by issuing the hawkeyeStatus command. They can then be restarted by issuing the hawkeyeServices command.

The associated config files, which allow you to fine tune and better integrate the hawkeye server are outlined in this chapter.

In this chapter:

MariaDB Database Management	354
Hawkeye Configuration Database Structure	354
Elasticsearch Management	355
OSS (Operations Support System) Integration	356
Backup and restore Hawkeye databases	357
Probe Management - Probe Busy	360
Hawkeye Folder Structure	362
Set up e-mails with Hawkeye server	362
SNMP Configuration and Verification	364
SNMP Traps	364
How to use SNMP Traps	364
Verify Hawkeye Server MIBs file can be interpreted by the User's SNMP server	365
Configure Hawkeye Server to send SNMP trap to a specific SNMP server	365
Configure your SNMP server to receive Hawkeye server originated SNMP traps	365
Enable SNMP traps to be triggered for endpoint scheduled tests	366
Verify SNMP trap successfully received and decoded by SNMP server	366
Advanced Troubleshooting – Debug SNMP packet routing issues	366
Rest API	367
REST examples	371
Server upgrade	378
Configure Time Zone and NTP	383
Configure Time Zone	383
Configure NTP Client	383

Configure Hawkeye as NTP Server	384
Configure UI Time Zone	385

MariaDB Database Management

Hawkeye Database

The tuning file for the Hawkeye Database is `/etc/mysql/mariadb.conf.d/99_tuning.cnf`. This file contains the tuning parameters for the server as well as defining where the MySQL server stores its data files.

For larger installations, you should consult Keysight Support to determine if any of the values here should be modified to accommodate the requirements of the specific installation.

Example of configuration for a server with 16G RAM:

```
#####
# mariaDB System optimizations can be made utilizing this file
# Edit this file using your favorite text editor.
# vi /etc/mysql/mariadb.conf.d/99_tuning.cnf
#
# Uncomment the settings you wish to set and update the associated values.
#
#####
[mariadb]

#####
# innodb_buffer_pool_size=1G This should be set to be 25% of the
# total system RAM. Example for a system with 16GB of RAM you should
# allocate 4G to the innodb_buffer_pool_size
#####

innodb_buffer_pool_size=4G

#####
# Default max-connections=151 This defines the maximum number of
# concurrent connections opened against MySQL. In the case of numerous
# endpoints/tests per hour (above 1000 tests per hour), Keysight recommends
# to increase this number to 1000
#####
```

`max-connections=1000`

MariaDB runs as a service:

- Do not attempt to terminate mariadb service as this can corrupt the database.
- Use `hawkeyeServices` command to restart MariaDB service.

Hawkeye Configuration Database Structure

Hawkeye utilizes MariaDB to store:

- System information and administration management
- Test execution Queue Management

Elasticsearch Management

Elasticsearch advanced configuration for performance tuning

The tuning file for Elasticsearch is `/opt/hawkeye/conf/elastic/jvm.options.d/jvm_tuning.options`. This file contains the tuning parameters for Elasticsearch. For larger installations, it is recommended to consult Keysight support team to determine if any of the values must be modified to accommodate the requirements of the specific installation.

NOTE

Heap Size should never exceed 49% of total system RAM. This can lead to Memory Utilization Alarms and system instability. We recommend to implement 45% of total system RAM.

Example of increment heap size from default 1GB to 4GB:

```
[root@Hawkeye-Server ~]# cat /opt/hawkeye/conf/elastic/jvm.options.d/jvm_tuning.options
#####
-Xms4g
-Xmx4g
#####
```

To apply the new changes made, you must restart **HawkeyeElasticsearch.service**.

HawkeyeElasticsearch runs as a service on which other services depend. To properly restart the service, use the `hawkeyeServices` command.

OSS (Operations Support System) Integration

Hawkeye is designed to be an open framework for easy integration into service providers OSS.

It supports a range of northbound and southbound interfaces that are designed to :

- Export or collect key information and alarms generated by Hawkeye to third party system.
- Automate some tasks from third party tools (generate automatic tests for example).
- Generate customized actions.

Hawkeye SNMP Alarms

Based on test results Hawkeye can trigger an Hawkeye SNMP trap to a third party.

The mib is based on SNMPv2 and is easily imported into supervision systems.

Alarms are generated based on pass fail criteria generated by thresholds.

Hawkeye Email Notifications

Hawkeye can generate automatic emails to configurable recipients (configurable per alert) with alarms based on test results or thresholds.

Automatic emails can also be sent with content result of aggregated report – these are user defined and can be scheduled over time (every hour/day/week).

Hawkeye REST API

Hawkeye REST API allows you to work on the hawkeye server through scripts. This is especially useful for integration in OSS. REST API can be used to integrate the following:

- Manage user/group
- Create tests
- Access user trail
- Update status of probes connected to the system
- Manage Mesh
- Manage IxProbe/Tap/Bypass
- Create and execute test template
- View test results

Keysight also provides the Hawkeye Data Extraction Tool (HDET), which you can download from the support page as a sample set of scripts, which can be run outside of the Hawkeye server to export the test results and audit logs. HDET utilizes python to export data in .json or .csv format for ease of integration with other tools.

Backup and restore Hawkeye databases

Hawkeye Results Data

Hawkeye Results are stored in a NoSQL database for faster response times and to facilitate future expansion. Hawkeye Results data is backed up every night at midnight server time. System administrators are also presented with the option to create a backup of the Hawkeye Results data as part of a server update.

Hawkeye Configuration Data

Hawkeye Configuration data is stored in a SQL database. System Administrators are presented with the option to create a backup of the Hawkeye Configuration data as part of a server update. Otherwise a backup can be manually triggered from the Hawkeye UI.

Creating a Backup

Backing up during an update

The most common time for System administrators to want to create a back up is right before an update to the system. Knowing this information, during the upgrade dialog the System Administrator is presented with the option to create backups of Configuration data, Results data, or both. By setting the corresponding slider to "ON" a backup of the data will be created before any changes are made to the system.

Update Server

Good to know:

- Update could take from 1 hour to many depending on your hardware capabilities.
- It is recommended to leave "Backup Configuration" and "Backup Results" set on.
(In case o failure you can restore your system.)
- During update your system will be unavailable to use.
- After update your system might require a reboot.

Required:

- Make sure your system is connected to internet.
- **DO NOT** interact with system during the update.
(The only one interaction allowed is to access system from a web browser.)
- **DO NOT** power off system during update.

Backup Configuration

On

Backup Results

On

 Update

Manual Backup

If for any reason you want to create a backup of the configuration data, results data, or both you can do so by navigating to the System page on the side bar and select the Backup button in the Data Pane. This will open the backup dialog:

Backup Data ✕

Good to know:

- Backups could take from few minutes to hours depending on your "Results" size(if selected) and hardware capabilities.
- Backups are executed in background, after process is finished you will receive a notification with status.

Required:

- **DO NOT** reboot / power off system during process.

Configuration ☐

Results ☐



Set the slider to **ON** next to the data you want to create a backup for and then select **Backup Now**.

NOTE

Hawkeye Server only stores one backup for the Configuration data and one backup for the Results data. Each subsequent backup will overwrite the existing backup.

Backup Storage locations

Backups are stored in `/opt/backup/`

The configuration backup is a single bzip file with the name: `Hawkeye_Configuration_backup.sql.bz2`

NOTE

Restore process expects the exact file name for configuration backups.

The results data backup is an entire directory. All the files in `/opt/backup/elasticsearch/` are required to be in this exact path for the restore process.

You can store copies of these backup files in the database by using the **Upload** option in Hawkeye. You can copy `Hawkeye_Configuration_backup.sql.bz2` without any additional steps.

To move the results data backup, compress it into a single bzip2 file and then run the following commands on the cli:

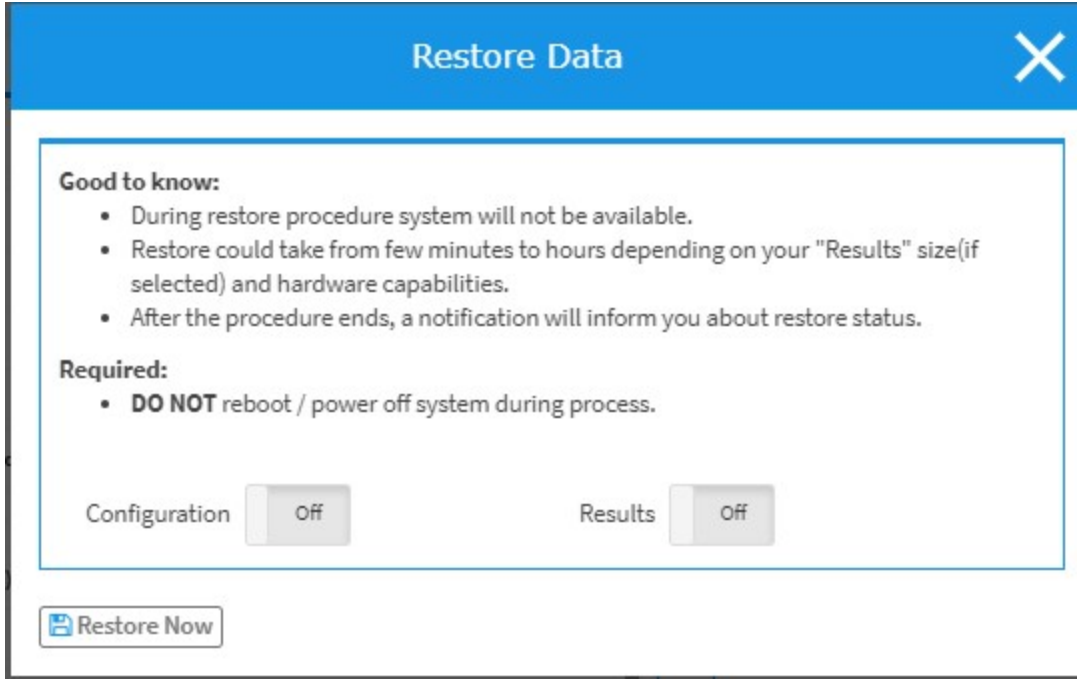
```
sudo cd /opt/backup/elasticsearch/
sudo tar -jcvf /tmp/hawkeye-results_<Date>.bz2 *
```

This will extract the bzip2 file to `/tmp/hawkeye-results_<Date>.bz2`. You can then move it to your off device storage for later use.

Restore Backups

The Hawkeye restore process expects the backups will be located where the backup process creates them. If files were saved to an off-server location, they will need to be returned to the original location for the restore process to work.

To start the restore process navigate to the System page on the side bar and select the Restore button in the Data Pane. This will open the restore dialog box.



The image shows a 'Restore Data' dialog box with a blue header bar containing the title 'Restore Data' and a close button (X). The main content area is white and contains the following information:

Good to know:

- During restore procedure system will not be available.
- Restore could take from few minutes to hours depending on your "Results" size(if selected) and hardware capabilities.
- After the procedure ends, a notification will inform you about restore status.

Required:

- **DO NOT** reboot / power off system during process.

At the bottom of the content area, there are two toggle switches: 'Configuration' and 'Results', both currently set to 'Off'. Below the content area is a button labeled 'Restore Now' with a document icon.

Set the slider to **ON** next to the data you want to restore and then select **Restore Now**.

Probe Management - Probe Busy

Hawkeye supports the ability for a custom script on an endpoint to determine when the probe is busy and therefore unavailable for tests. The Hawkeye Server in **Probe Management** indicates when an endpoint is down or up. This feature introduces a third state of busy for the endpoint. When a probe becomes busy, the state will be reflected in **Probe Management** in blue for that probe and it will not be available to run tests. All scheduled tests will remain in a queued state until endpoint leaves the busy state.

To turn on this feature, go to **Preferences> Advanced Options** and select **Probe Busy** parameter. A user defined script is placed on all endpoints that the probe busy feature is intended for. The purpose of the endpoint probe busy script is to determine when the probe is busy and not available for tests. You should define the script on the probe that determines when a probe is busy. The Hawkeye server will send a command down to each endpoint every so many seconds to execute the script and retrieve the busy status. The frequency of requesting probe busy status is determined by the Hawkeye System **Preference** parameter **Real services: default interval time for automatic endpoints** in **Advanced Options** tab.

When the feature probe busy is turned on, it is not necessary for all endpoints to contain the busy script. For all endpoints not containing the busy script, a result of not busy will be returned.

Below a sample script indicates a probe is busy for a defined period each day.

Use case

This is an example probe busy script which indicates a probe is busy during the peak network busy time of early evening.

NOTE

Use ssh to connect to the endpoint and create the probe busy script as below. The script must be in the specified directory and use the specified filename.

1. Create a file on the endpoint named **testIfProbeBusy** with the following script.

```
# cd /home/ixia/

# nano testIfProbeBusy.py
#!/usr/bin/python
import datetime
import sys
# use format HHMM
simulate_unavailable_start_time = "1326
simulate_unavailable_end_time = "2100
debug = 0
test_start_time = datetime.datetime.now()
test_start_time_str = test_start_time.strftime('%d-%b-%y %H:%M:%S')
test_start_hhmm = test_start_time.strftime("%H%M")
if test_start_hhmm >= simulate_uanavailable_start_time and test_start_hhmm <= simulate_
uanavailable_end_time:
    endpoint_busy = 1
else:
    endpoint_busy = 0
if debug > 0:
    sys.stdout.write('\nDEBUG: %s endpoint_busy=%s unavailable from %s to %s
\n' %
                        (test_start_time_str, endpoint_busy, simulate_uanavailable_start_
time,
                        simulate_uanavailable_end_time))
sys.exit(endpoint_busy)
```

2. Next ensure script is available for executable

```
# chmod +x /home/ixia/testIfProbeBusy
```

3. On the Hawkeye server UI, under **Administration > Preference > Advanced Options**, turn on the **Probe Busy**.

The Hawkeye server will now send frequent commands (default every 5 seconds) down to each endpoint to run the testIfProbeBusy script. The script will return "1" if busy or "0" if available for tests. The Probe status for the endpoint will reflect busy with a blue color when busy. If an endpoint does not contain the script it will always return a not busy status.

When a test runs and the probe is blue indicating busy, the test will enter a queued state. If the test is scheduled to run every minute only one instance of that test will be queued. The scheduled test will continue as normal when probe becomes available. If three different tests are scheduled to run each minute against the probe only one instance of each of the three tests will be queued until probe becomes available.

NOTE

Probe Busy functions are only supported on XR endpoints.

Hawkeye Folder Structure

The Hawkeye application is installed in `/opt/hawkeye`. The Hawkeye application generates a number of log files which are automatically rotated to manage disk space. The user does not need to refer these log files unless advised by Keysight Customer Support.

The following directories contain log files:

- System log files are in `/var/log` directory.
- Individual Node to Node and Mesh test details or statistics files from endpoints are in `/opt/hawkeye/logs/Chariot` directory.
- Hawkeye system files and real service test logs are in `/opt/hawkeye/logs/Hawkeye` directory.

Set up e-mails with Hawkeye server

Hawkeye server supports the use of emails in three ways.

- Deliver generated reports though e-mails.
- Deliver error notification e-mails of test results including failure or error reasons.
- Deliver real service test e-mails for XR probes

To send reports and test results in e-mails, you must make available a mail client and configure it for the Hawkeye server. You do not need to configure mail client for Hawkeye server for real service tests.

Configure e-mail for reports and test results

Configure **Email** section in **Administration > Preferences** of Hawkeye server UI to set up a mail client. You will need to configure your SMTP server settings and your organization's e-mail account credentials in this section for the Hawkeye server to send e-mails.

Configure an Email SMTP server in **Preferences**. Following is a sample configuration.

SMTP server: mail.smtp2go.com

SMTP Authentication: Enable

SMTP Security: SSL (match whatever your email service uses SSL/TLS?)

Port: 465

NOTE

Configure port 465 for SSL, 587 port for TLS or 25 default SMTP port for no security, no other value is supported. Port 25 was the most commonly used port, but for security many email providers now block it as it is used by spammers.

Username: fred_s_fish_n_chips@gmail.com

NOTE

This e-mail address is for reference.

Password: *****

Email address: fred's_fish_n_chips@gmail.com

Full name: fred's_fish_n_chips@gmail.com

NOTE

These are the credentials from e-mail server.

Max Email attempts: 3

NOTE

The e-mail process is abandoned after maximum attempt is attained.

Workflow of sending and retrieving e-mails

Outgoing and incoming mail are handled by two different types of server.

- SMTP server to send e-mail
- POP3/IMAP server to retrieve e-mail

You send email from your mail client (now running on Hawkeye server) by using the configured email address to the outgoing SMTP server using the configured port. The SMTP server first validates security and authentication, that is, connection security (SSL/TLS/25), port, username, password. The SMTP server works like the post office and performs a DNS lookup to find where to send the email (destination domain). The SMTP server may store the actual email on a local server (owned by domain sender) close to the Hawkeye server instead of the main SMTP server (that is, gmail in the above sample configuration). The SMTP server then sends the email to the destination domain Message Transfer Agent (MTA) server for long term storage. If the email destination domain is the same as the source (that is, gmail in the above sample configuration), the SMTP server will act as the MTA server. If different sender/dest email domain and no issues, it can be routed or forwarded. The email is sent by SMTP protocol to the (destination domain) MTA server. The received email is stored on the destination domain MTA (POP3/IMAP) server. The MTA (POP3/IMAP) server uses POP3 or IMAP protocol to transfer email to recipient's inbox (email client on the computer) when requested.

Workflow of real service test e-mail

Real service test e-mail works by using an email client on the probe. Only the XR2000 currently supports an email client. Configuring the **Email** section of **Preferences** is not used in this case.

Configure real service test email

Configure the following parameters to send and receive real service test emails.

- Sending email server credentials
- Email address
- Outgoing Mail server
- Outgoing Mail port
- SMTP authentication: SSL
- SMTP Authentication user

- SMTP Authentication password
- Receiving email server credentials
- Incoming mail server
- Incoming mail port
- Incoming mail protocol
- Mail user
- Mail Password

The real service test e-mail times different stages, but most important is when the destination POP3/IMAP server receives the sent email. Probe will poll every second to check received email.

SNMP Configuration and Verification

You can configure and verify the Simple Network Management Protocol (SNMP). This section explains how to configure and verify the SNMP.

SNMP Traps

Hawkeye server supports the generation of SNMP traps for tests originated from endpoints. Tests configured to generate SNMP traps on certain error/failure conditions sends the SNMP traps in MIB format to a designated SNMP server.

There are six steps involved:

- How to use SNMP traps
- Verify Hawkeye Server MIBs file can be interpreted by the User's SNMP server
- Configure HawkeyeServer in **Preferences** to send SNMP trap to a specific User's SNMP server
- Configure User's SNMP server to receive Hawkeye server originated SNMP traps
- Enable SNMP traps to be triggered for endpoint scheduled tests
- Verify SNMP trap successfully received and decoded by SNMP server
- Advanced Troubleshooting – Monitor Hawkeye server SNMP debug logs

How to use SNMP Traps

SNMP traps can be configured to be triggered by test results on end points. The time between tests and consequently the possible reporting time between SNMP traps is Customer configurable. The shortest time between tests on an endpoint is one minute.

SNMP traps are supported for all test types. When configuring a test, select **Show Alarm options** to see the SNMP configuration.

Each test can be enabled to trigger SNMP traps, based on a failure or error result. There is the option to only report an SNMP trap on a **change**. This means if a test on an endpoint is scheduled to run every 5 minutes and it is failing every time, it is only reported as an SNMP trap the very first time it fails, then it generates another SNMP trap once the endpoint test result changes to be an error or passes.

Verify Hawkeye Server MIBs file can be interpreted by the User's SNMP server

Hawkeye SNMP traps encoding is identified by three files. Retrieve the following three MIBs files from the Hawkeye server so that they can be verified:

- /usr/share/snmp/mibs/NET-SNMP-MIB.txt
- /opt/hawkeye/includes/MIBS/Hawkeye-MIB.txt
- /opt/hawkeye/includes/MIBS/IXIA-SMI.txt

There are a number of independent free web sites that verify that custom MIB files confirm to correct standards.

Suggested free independent web sites to verify Hawkeye MIBs format:

```
http://www.simpleweb.org/ietf/mibs/validate/upload.php
http://www.muonics.com/Tools/smichk.php
```

From these web sites pull in the retrieved two Hawkeye files and validate to MIBs standards. There are three supported versions of MIB files (v1, v2 and v3).

Configure Hawkeye Server to send SNMP trap to a specific SNMP server

Enable SNMP traps to be generated by the Hawkeye server.

To enable the SNMP traps, do the following:

Go to **Administration > preferences > Alarms** toggle the **Enable/disable the alarms received using SNMP**.

Also configure the IP address of the your SNMP trap server, to which the SNMP traps are to be sent to.

Multiple SNMP trap receivers can be supported by using a third party application that will forward received UDP packets from the Hawkeye Server IP address/port to a defined list of destination SNMP trap receivers (IP/port). There are many free applications that are available for this purpose, such as the free linux **samplicator** application. The SNMP server IP defined on the Hawkeyeserver to achieve this will be the IP of the third party application doing the forwarding.

Configure your SNMP server to receive Hawkeye server originated SNMP traps

There are many SNMP servers (receiver) available but the required basic configuration is as follows:

1. Load in the two Hawkeye MIB modules identified and retrieved from the Hawkeye server in the above steps (NET-SNMP-MIB.txt, IXIA-SMI.TXT and Hawkeye-MIB.txt). This enables your SNMP trap server to decode the Hawkeye SNMP traps.
2. Configure the host address of the Hawkeye server that will be the source of the SNMP traps.
3. Set the host port used to generate and be monitored for the SNMP traps to **162**.
4. Set the **community** to **ixia**.

- Following a Hawkeye Server upgrade, remove, flush, or delete any Hawkeye MIB files from the SNMP server (receiver) and pull in the latest version as new test types. Else, changed test metrics will cause decode issues.

Enable SNMP traps to be triggered for endpoint scheduled tests

- Schedule a test (example, node to node Skype4B traffic test) on probes expected to generate SNMP traps on error/failure conditions.
- When configuring the test, set thresholds to expected values additionally select **Show Alarm Options**.
- Go to **Show Alarm Options** and enable the **SnmpTrap**.
- Also select the conditions for the alarm to be triggered that generates the SNMP Trap (Error/Failed/Status change).

Verify SNMP trap successfully received and decoded by SNMP server

Invoke SNMP trapviewer from your SNMP server. Generate SNMP trap by running Hawkeye test that fails. Confirm that the SNMP trap received in the trap viewer is as expected and can be decoded.

Advanced Troubleshooting – Debug SNMP packet routing issues

Putty (ssh) to Hawkeye server and monitor SNMP trap logs to confirm that tests are triggering sending of SNMP traps to SNMP server.

On the Hawkeye server go to directory **/opt/hawkeye/logs/Hawkeye** and monitor server daemon logs with the following command.

```
tail -f ServerDaemon.log
```

Confirm able to see logs such as the one below where the first IP address is the IP address of the SNMP server to receive the SNMP trap.

```
20:24:58 UTC (Alarm send) sending snmptrap -
snmptrap -M /usr/share/snmp/mibs/:/opt/hawkeye/includes/MIBS -c ixia -v 2c 10.220.120.11
"" HAWKEYE-MIB::hawkeye-notification trapID s "xr2000autoqa2xrpiWi-
Fiqa2Skype4BTrafficDelaysmsAudioRTPfromto12kbpsFAIL" summary s "xr2000autoqa2 to xrpiWi-
Fiqa2 Skype4B Traffic Audio RTP fromto 12 kbps Delay ms Failed" runID s "8285" TimeStamp
s "2016-11-30 20:24:57" TestType s "Skype4B Traffic" TestStatus s "Failed" From s
"xr2000-auto-qa-2" To s "xrpi-Wi-Fi-qa-2" PAIRNAME s "Audio RTP from->to 12 kbps"
MetricName s "Delay (ms)" METRICVALUE s "2.5" DefaultThresholdType s "1" THRESHOLD s
"9000" METRICSTATUS s "Failed" FailReason s "Threshold failed on Audio RTP from->to 12
kbps Delay (ms) "
```

Additionally use TCP dump command to confirm that the SNMPtrap packet is not being blocked in the network. The TCP logs below (taken from Hawkeye server) show that a SNMP trap is generated from Hawkeye server (10.220.120.127) and sent to the SNMP trap server/receiver (10.220.20.45) but is blocked as unreachable.

TCP dump from Hawkeye server:

```
tcpdump -n -i eth0 | grep -i "10.220.120.127"
21:11:38.246127 IP 10.220.120.127.52365 > 10.220.20.45.snmptrap: C=ixia V2Trap(183)
.1.3.6.1.2.1.1.3.0=148999358 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.8072.2.1.0.3
.1.3.6.1.4.1.8072.2.1.2.1=3 .1.3.6.1.4.1.8072.2.1.2.2="Amazon-KFFOWI"
```

```
.1.3.6.1.4.1.8072.2.1.2.3="Amazon-KFFOWI" .1.3.6.1.4.1.8072.2.1.2.4="0"
.1.3.6.1.4.1.8072.2.1.2.5="TestAgent1"
21:11:38.247491 IP 10.220.20.45 > 10.220.120.127: ICMP 10.220.20.45 udp port snmptrap
unreachable, length 234
```

In the above example, unlike the Network Unreachable and Host Unreachable messages which come from routers, the Port Unreachable message comes from the SNMP server/receiver. The primary implication for troubleshooting is that the frame was successfully routed across the communications infrastructure, the last router ARP'ed for the host, got the response, and sent the frame. Furthermore, the intended SNMP server (destination host) was on-line and willing to accept the frame into its communications buffer. The frame was then processed and an attempt was made to send the data up to the destination port number (UDP port 162) and the port process (SNMP server) did not exist. The protocol handler then reports Destination Port Unreachable.

For SNMP traps generated by Hawkeye Server to reach a third party SNMP trap receiver the UDP ports 161 and 162 need to be open for UDP traffic on the Hawkeye server and switches between the two parties. One way to open the ports on the Hawkeye Server is to putty to the Hawkeye Server then using the following CLI commands to open the firewall for SNMP traffic:

NOTE

You need privilege escalation for the following steps.

```
ksuser@he-qa-deb:~$ su -
Password:
root@he-qa-deb:~# firewall-cmd --add-service=snmp --permanent
success
root@he-qa-deb:~# firewall-cmd --add-service=snmptrap --permanent
success
root@he-qa-deb:~# firewall-cmd --reload
success
```

Hawkeye SNMP MIB Information

This section covers information about SNMP MIB provided by Hawkeye

MIB file location

MIB files can be found into the following directory /opt/hawkeye/includes/MIBS

Associated MIB Descriptors

Associated MIB descriptors can be needed to import MIB. The associated MIB descriptor are available in the same subdirectory:

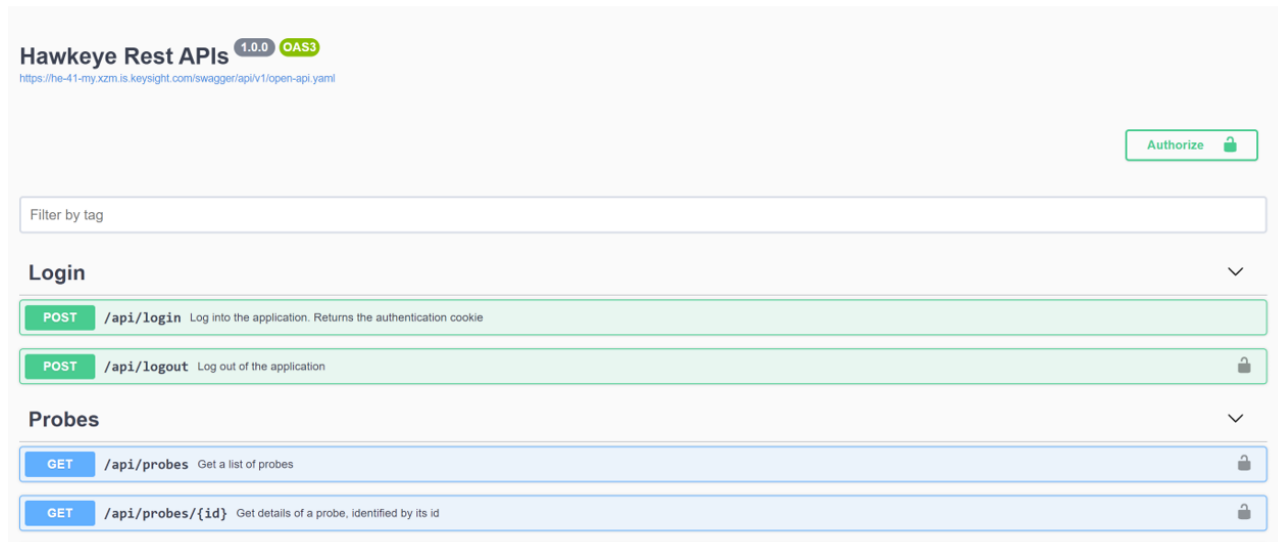
/usr/share/snmp/mibs

Rest API

Hawkeye solution has a web-based GUI. You can access functions of Hawkeye without the web user interface using Rest APIs directly.

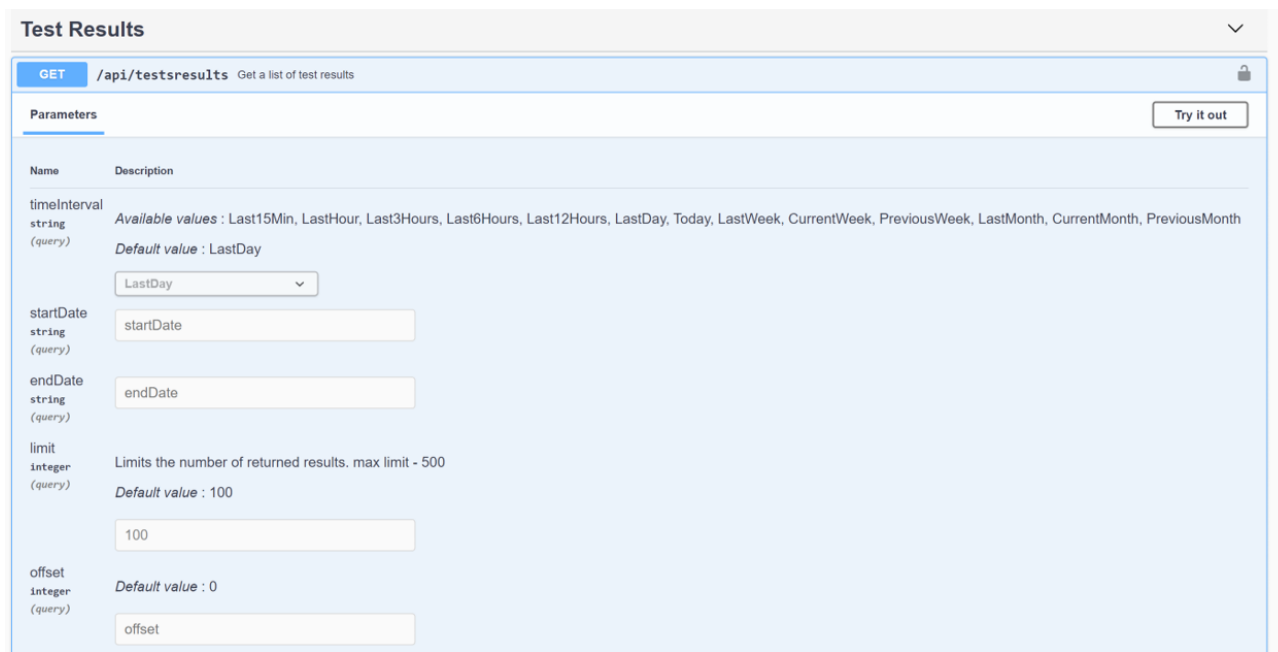
List of supported Rest APIs are available under Documentation > Rest API. Swagger is a tool, which is used to visualize and interact with the API's resources without applying any implementation logic.

You can download open API spec from the <open-api.yaml> link at the top of Documentation > Rest API and use it in any other tool.



Example: Rest API to get a list of test results.

Below is the image of test result request. Select **Try it out** button on the tool to run it without implementing on client side for testing.



Below is image of **test result response** showing JSON format to be returned on the request call.

Responses		
Code	Description	Links
200	Tests Results	No links
	<div>Media type application/json</div> <div>Controls Accept header.</div> <div>Example Value Schema</div> <div><pre>{ "total_count": 0, "count": 0, "limit": 0, "offset": 0, "has_more": 0, "records": [{ "id": "string", "date": "2020-08-03T18:10:38.977Z", "duration": 0, "meshid": 0, "mesh": 0, "module": "N2N", "probeFrom": "string", "probeTo": "string", "reasonCause": "string", "status": "Passed", "testId": 0, "testOptions": "string", "testTag": "string", "testType": "string" }] }</pre></div>	
400	Parameters or body were in an incorrect format	No links
	<div>Media type application/json</div> <div>Example Value Schema</div> <div><pre>{ "error": "string", "code": "404 Notfound" }</pre></div>	

To check the schema of response and its elements click on schema link as highlighted below

Responses		
Code	Description	Links
200	<p>Tests Results</p> <p>Media type <input type="text" value="application/json"/></p> <p>Controls Accept header.</p> <p>Example Value Schema</p> <pre> TestsResultsList { total_count integer count integer limit integer offset integer has_more BooleanType integer Enum: [0, 1] records { TestsResults { id string date date-time string(\$date-time) duration integer meshId integer mesh BooleanType integer Enum: [0, 1] module string Enum: [2] probeFrom string probeTo string reasonCause string status string Enum: [2] testId integer testOptions string testTag string testType string } } }</pre>	No links
400	<p>Parameters or body were in an incorrect format</p> <p>Media type <input type="text" value="application/json"/></p> <p>Example Value Schema</p> <pre> { "error": "string", "code": "404 NotFound" }</pre>	No links

How to create a new test:

The Tests **topology** field (NodeToNode, RealService, Mesh) in a request defines the type of test that is going to be created.

Example requests for each test topology are available in [REST examples](#) section.

The **parameters** array contains list of basic and pairs (for NodeToNode and Mesh) of a testtype. Use `/api/testtypes/{id}/parameters` API where {id} is testtype Id to fetch list of supported test parameters for a specific test type.

The **threshold** and **alarm** are optional data. Use it if client wants to change alarm or threshold's default settings. Outlier under threshold is also optional.

The **startDate** and **endDate** fields are in UTC time format **YYYY-MM-DDTHH:MM:SSZ**

REST examples

NodeToNode Request:

```
{
  "identifier": "",
  "isMesh": "0",
  "testtypeId": "5163",
  "fromProbeId": "2",
  "toProbeId": "3",
  "meshId": "2",
  "enforceSchedule": "0",
  "frequency": "2",
  "startDate": "2020-08-11T18:30:44Z",
  "endDate": "2120-08-11T18:16:48Z",
  "testTemplateExecutionId": "0",
  "topology": "NodeToNode",
  "fromIps": "Default",
  "toIps": "Default",
  "parameters": {
    "basic": [
      {
        "id": "1",
        "value": "30"
      },
      {
        "id": "4",
        "value": "5"
      }
    ],
    "pairs": [
      {
        "id": "15175",
        "parameters": [
          {
            "id": "105",
            "value": "BestEffort"
          }
        ]
      },
      {
        "id": "15176",
        "name": "TCP from->to N pairs COS 2",
        "parameters": [
          {
            "id": "105",
```

```

    "value": "BestEffort"
  }
]
},
{
  "id": "15177",
  "name": "TCP from->to N pairs COS 3",
  "parameters": [
    {
      "id": "105",
      "value": "BestEffort"
    }
  ]
},
{
  "alarm": {
    "trigger": {
      "failure": "0",
      "error": "0",
      "change": "0",
      "outlier": "0"
    },
    "notification": {
      "email": {
        "enabled": false,
        "address": ""
      },
      "snmp": {
        "enabled": false
      }
    }
  },
  "thresholds": [
    {
      "pairId": "15175",
      "pairName": "TCP from->to N pairs COS 1",
      "metric": "Throughput from->to (Mbps)",
      "value": "5571508.445",
      "operator": "1",
      "unit": "Mbps",
      "factor": "1",
      "autoLearnEnabled": "0",
      "sensitivity": 95,
      "outlier": {
        "enabled": "0",

```



```

    "windowSec": "1740",
    "windowPct": "52"
  },
  {
    "pairId": "15176",
    "pairName": "TCP from->to N pairs COS 2",
    "metric": "Throughput from->to (Mbps)",
    "value": "5229714.123",
    "operator": "1",
    "unit": "Mbps",
    "factor": "1",
    "autoLearnEnabled": "1",
    "sensitivity": 99,
    "outlier": {
      "enabled": "1",
      "windowSec": "1800",
      "windowPct": "50"
    }
  },
  {
    "pairId": "15177",
    "pairName": "TCP from->to N pairs COS 3",
    "metric": "Throughput from->to (Mbps)",
    "value": "4844271.8789",
    "operator": "1",
    "unit": "Mbps",
    "factor": "1",
    "autoLearnEnabled": "1",
    "sensitivity": 99.9,
    "outlier": {
      "enabled": "1",
      "windowSec": "1800",
      "windowPct": "50"
    }
  }
]
}

```

RealService Request:

```

{
  "identifier": "api call",
  "isMesh": "0",
  "testtypeId": "7148",
  "fromProbeId": "1",

```

```

    "toProbeId": "0",
    "meshId": "0",
    "enforceSchedule": "0",
    "frequency": "4",
    "startDate": "2020-08-14T15:43:32Z",
    "endDate": "2120-08-14T15:43:32Z",
    "testTemplateExecutionId": "0",
    "topology": "RealService",
    "parameters": {
      "basic": [
        {
          "id": "202",
          "description": "Destination Servers",
          "value": "www.test.com"
        },
        {
          "id": "203",
          "description": "Interval",
          "value": "0.02"
        },
        {
          "id": "204",
          "description": "Count",
          "value": "100"
        },
        {
          "id": "205",
          "description": "Packet Size",
          "value": "100"
        },
        {
          "id": "227",
          "description": "ip protocol",
          "value": "ipv4"
        },
        {
          "id": "3006",
          "description": "Class of Service",
          "value": "0"
        },
        {
          "id": "3007",
          "description": "Jitter Calculation",
          "value": "1"
        }
      ]
    }
  ]

```

```

},
"thresholds": [
{
"pairId": "7148",
"pairName": "ICMP Test",
"metric": "Availability",
"value": "1",
"operator": "1",
"unit": null,
"factor": "1",
"autoLearnEnabled": 0,
"sensitivity": 100
},
{
"pairId": "7148",
"pairName": "ICMP Test",
"metric": "Jitter (ms)",
"value": "8",
"operator": "0",
"unit": "ms",
"factor": "1",
"autoLearnEnabled": 0,
"sensitivity": "0"
},
{
"pairId": "7148",
"pairName": "ICMP Test",
"metric": "Jitter Max (ms)",
"value": "8",
"operator": "0",
"unit": "ms",
"factor": "1",
"autoLearnEnabled": 0,
"sensitivity": "0"
},
{
"pairId": "7148",
"pairName": "ICMP Test",
"metric": "Jitter standard deviation",
"value": "2",
"operator": "0",
"unit": null,
"factor": "1",
"autoLearnEnabled": 0,
"sensitivity": "0"
},
}

```

```

{
  "pairId": "7148",
  "pairName": "ICMP Test",
  "metric": "Packet loss",
  "value": "1",
  "operator": "0",
  "unit": null,
  "factor": "1",
  "autoLearnEnabled": 0,
  "sensitivity": "0"
},
{
  "pairId": "7148",
  "pairName": "ICMP Test",
  "metric": "Round trip time avg (ms)",
  "value": "300",
  "operator": "0",
  "unit": "ms",
  "factor": "1",
  "autoLearnEnabled": 0,
  "sensitivity": "0"
},
{
  "pairId": "7148",
  "pairName": "ICMP Test",
  "metric": "Round trip time max (ms)",
  "value": "400",
  "operator": "0",
  "unit": "ms",
  "factor": "1",
  "autoLearnEnabled": 0,
  "sensitivity": "0"
},
{
  "pairId": "7148",
  "pairName": "ICMP Test",
  "metric": "Round trip time min (ms)",
  "value": "300",
  "operator": "0",
  "unit": "ms",
  "factor": "1",
  "autoLearnEnabled": 0,
  "sensitivity": null,
  "outlier": {
    "enabled": "1",
    "windowSec": "1800",

```

```

    "windowPct": "50"
  }
},
{
  "pairId": "7148",
  "pairName": "ICMP Test",
  "metric": "Standard deviation (ms)",
  "value": "20",
  "operator": "0",
  "unit": "ms",
  "factor": "1",
  "autoLearnEnabled": 0,
  "sensitivity": "0"
}
] }

```

create a Test using Mesh Id:

```

{
  "identifier": "MeshTestFromAPI",
  "isMesh": "1",
  "testtypeId": "5129",
  "meshId": "1",
  "enforceSchedule": "0",
  "frequency": "5",
  "startDate": "2020-08-14T15:50:18Z",
  "endDate": "",
  "testTemplateExecutionId": "0",
  "topology": "Mesh",
  "parameters": {
    "basic": [
      {
        "id": "1",
        "description": "Traffic Duration",
        "value": "30"
      },
      {
        "id": "105",
        "description": "DSCP Setting",
        "value": "BestEffort"
      }
    ]
  }
}

```

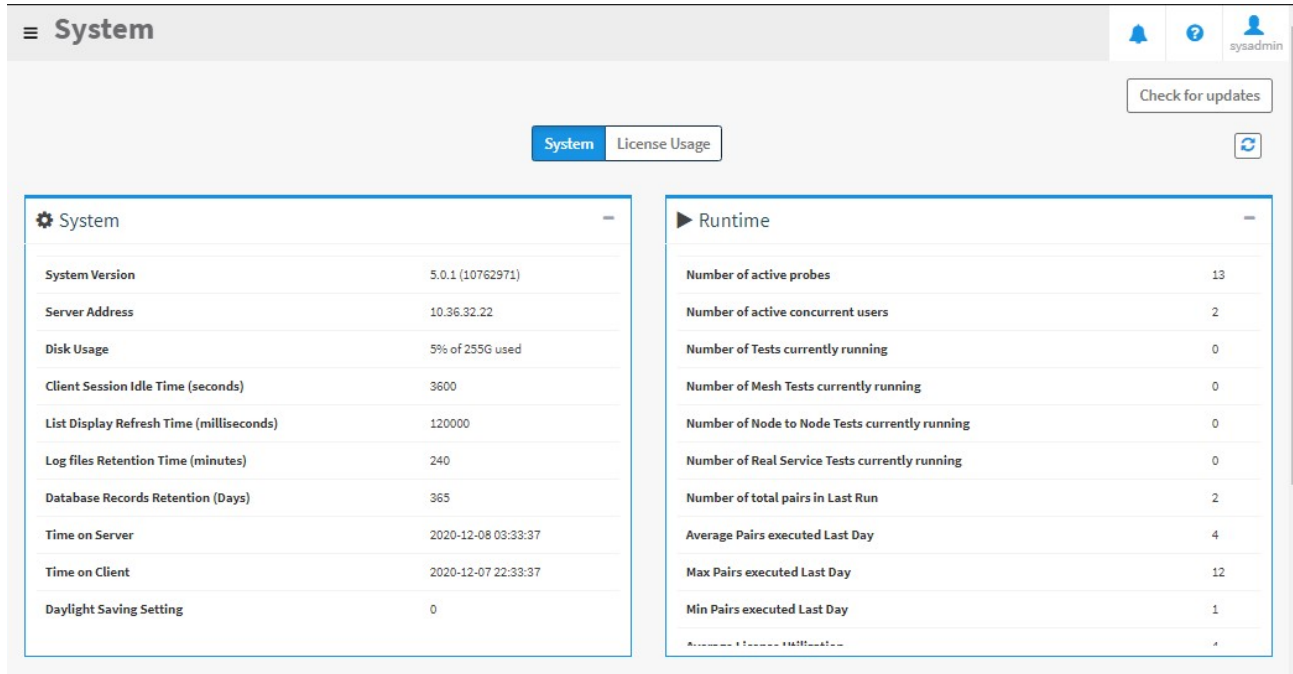
Server upgrade

You can upgrade the Hawkeye server in both online and offline processes.

Online upgrade

You can upgrade the Hawkeye server running Hawkeye 5.0.1 or later versions with a connection to the internet to the latest release of Hawkeye from the UI:

Select **System** from the side bar and select the **Check for updates** button:



The screenshot shows the Hawkeye System configuration page. The top navigation bar includes a hamburger menu, the word "System", and user icons for notifications, help, and "sysadmin". A "Check for updates" button is located in the top right. Below the navigation bar, there are two tabs: "System" (selected) and "License Usage". The "System" tab displays a table of system configuration parameters.

System	
System Version	5.0.1 (10762971)
Server Address	10.36.32.22
Disk Usage	5% of 255G used
Client Session Idle Time (seconds)	3600
List Display Refresh Time (milliseconds)	120000
Log files Retention Time (minutes)	240
Database Records Retention (Days)	365
Time on Server	2020-12-08 03:33:37
Time on Client	2020-12-07 22:33:37
Daylight Saving Setting	0

The "Runtime" tab displays a table of runtime statistics.

Runtime	
Number of active probes	13
Number of active concurrent users	2
Number of Tests currently running	0
Number of Mesh Tests currently running	0
Number of Node to Node Tests currently running	0
Number of Real Service Tests currently running	0
Number of total pairs in Last Run	2
Average Pairs executed Last Day	4
Max Pairs executed Last Day	12
Min Pairs executed Last Day	1

If an update is available, the **Update Server** button will appear. Select **Update Server** button to start the update dialog.

Update Server
✕

Good to know:

- Update could take from 1 hour to many depending on your hardware capabilities.
- It is recommended to leave "Backup Configuration" and "Backup Results" set on.
(In case o failure you can restore your system.)
- During update your system will be unavailable to use.
- After update your system might require a reboot.

Required:

- Make sure your system is connected to internet.
- **DO NOT** interact with system during the update.
(The only one interaction allowed is to access system from a web browser.)
- **DO NOT** power off system during update.

Backup Configuration

On

Backup Results

On

 **Update**

Here you have the option to have either your configuration or your results or both backed up prior to the upgrade. Once your selections are made select **Update** button. You will be asked to confirm that update by selecting **OK** to start you update.

After the Update has started you will be redirected to an Update Status page. This page report when each step in the update is done and will check to see if the system will need to be rebooted once the update is complete. If a reboot is required, you will be prompted to reboot by selecting the **Reboot Now** button otherwise you will be redirected to the login page when the update completes.

Updating Hawkeye in progress ...

Start checking basic requirements ...
DONE: Basic requirements for update have been met.
Configuration backup in progress ...
DONE: Configuration backup was executed with success.
Results backup in progress ...
DONE: Results backup executed with success.
Upgrading server in progress ...
Dependency checking ...
DONE: Dependency checking
Downloading packages ...
DONE: Downloading packages
Installing updates ...
DONE: Installing updates
Cleaning Up ...
DONE: Cleaning Up
Verifying updates ...
DONE: Verifying updates
DONE: Server was updated with success.
Check if reboot machine is needed ...
Now you have to reboot the system ...

[Reboot Now](#)**NOTE**

During the update the system will not be available for tests or access by other users.

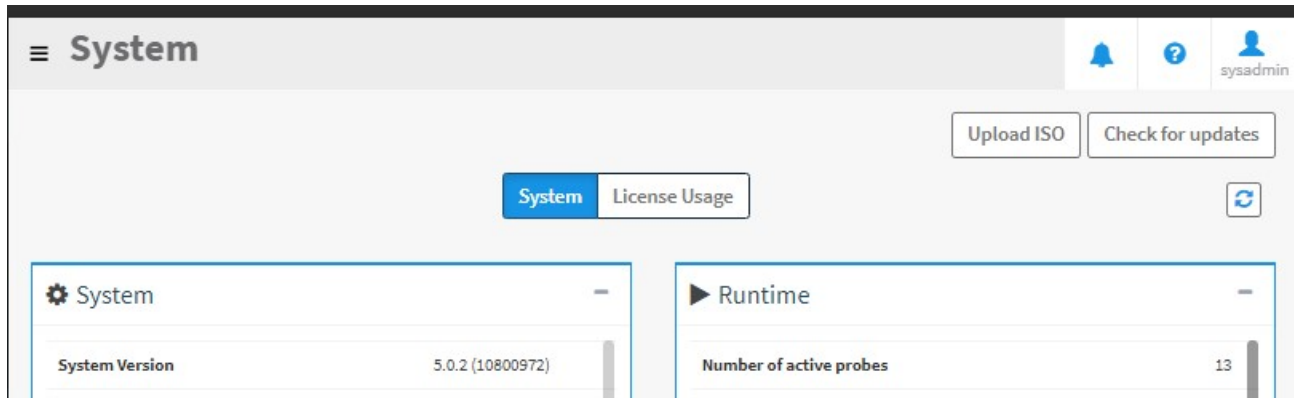
Offline upgrade

You can upgrade Hawkeye server in offline mode either from user interface (UI) or from the command line program (CLI). Both these processes are mentioned in this section.

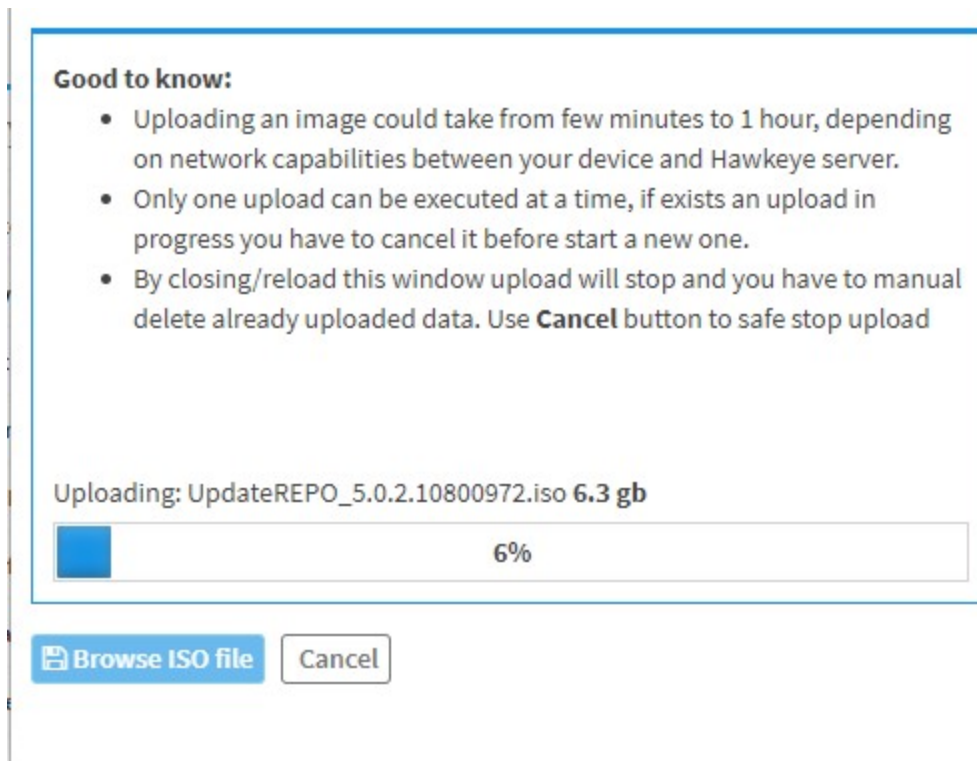
UI process

Hawkeye Servers running Version 5.0.2 or later support offline upgrade from the UI. This does require you to have already downloaded the UpdateRepo .iso file from support.ixiacom.com to your local machine ahead of time. After the file has been downloaded, you can perform the following steps to upload it to your Hawkeye server and upgrade your server.

Select **System** from the side bar and select the **Upload ISO** button.



The **Upload** dialog will open in a new browser window, select the **Browse ISO File** button and select the UpdateRepo.iso file that you previously downloaded. After you select **Open** the upload will start immediately. If you do not refresh or close this browser window, the update will continue while you continue to use Hawkeye.



After the upload completes the system will validate that it is a Keysight update repository ISO file and show a notification in the Hawkeye UI.

Notifications Details

Id	24
Type	ISO image validation success
Content	Image: UpdateREPO_5.0.2.10800972.iso was validated with success. Please refresh your browser.
Is Active	yes
Is Read	no
Login	sysadmin
Created At	2021-02-08 15:34:26

After Hawkeye validates the image, it will display the image available offline for update on the System page. Then you can select the **Update Server** button to start the update process and continue the process similar to online update.



CLI process

You can upgrade the Hawkeye server running Hawkeye 5.0.1 or higher versions offline to the latest release of Hawkeye from the CLI. To do this, you must download the .iso image from support.ixiacom.com.

After you have downloaded the .iso file, transfer it to the /tmp directory of your Hawkeye server and run the following command:

```
#updateServer --offline <path to .iso file>
```

If a reboot is required, Hawkeye will prompt you to reboot the system after the upgrade.

Note:

NOTE

The updateServer command can also perform backups and check for available updates if the server has an internet connection. To see other options available, run the following command:

```
#updateServer -h
```

Configure Time Zone and NTP

Configure Time Zone

When configuring the time zone for various devices in your Hawkeye environment please follow the table below for the commands required.

Action	Hawkeye Server/XR-E1S/XR-VM/XR3000	Xr2000/xrpi
List available time zones	timedatectl list-timezones	ls /usr/share/zoneinfo/
Set time zone	timedatectl set-timezone ZONE	ln -sf /usr/share/zoneinfo/ZONE /etc/localtime
Example set time zone	timedatectl set-timezone America/New_York	ln -sf /usr/share/zoneinfo/America/New_York /etc/localtime

NOTE

Changing the Time Zone in the Hawkeye Server after recording the test results leads to incorrect display of previously recorded results in the current time zone. There is either a gap in results or results into the future that equals to the offset between the prior and current time zones.

Configure NTP Client

All probes when connected to a Hawkeye Server will configure their NTP solution to sync time with the Hawkeye Server by default you can configure additional NTP servers to help keep probe time in sync. When configuring the Network Time Protocol (NTP) on various devices in your Hawkeye environment please follow the table below for the configuration file to use and the Service to restart after making the configuration change.

Action	Hawkeye Server/XR-E1S/XR-VM/XR3000	Xr2000/xrpi
Configuration File	/etc/chrony/chrony.conf	/etc/ntp.conf
Restart Service	systemctl restart chronyd	Xr2000: service ntpd restart XRpi: service ntp restart
Example server key	server your.ntp.server iburst	server your.ntp.server iburst

To Configure NTP on your device find your devices configuration file above and add a server key at the bottom of the file using the format presented above. Following is an example of the config file for an XR-VM:

```
# Welcome to the chrony configuration file. See chrony.conf(5) for more
# information about usable directives.

# Include configuration files found in /etc/chrony/conf.d.
```

```

confdir /etc/chrony/conf.d

# Use Debian vendor zone.
pool 2.debian.pool.ntp.org iburst

# Use time sources from DHCP.
sourcedir /run/chrony-dhcp
.
.
.
# Log files location.
logdir /var/log/chrony
.
.
.
# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
leapsectz right/UTC

```

After editing this file to add your servers, restart the time service using the appropriate restart service command from the above table.

Configure Hawkeye as NTP Server

By default, the Hawkeye Server denies all NTP sync requests it gets from other NTP clients. The system supports allowing client connections by subnet, IP , or allow all client connections. To configure this, add allow statements to the /etc/chrony.conf file in the section by using the following command:

```
# Allow NTP client access from local network.
```

Allow Statement	Description
allow 1.2.3.4	Allows the IP address 1.2.3.4 to connect as client
allow 1.2	Allows any IPv4 Address that start with 1.2 to connect as a client
allow 192.168.22.0/24	Allows the 192.168.22.0 class c subnet to connect as a client
Allow 265d:dc10::/64	Allows IPv6 265d:dc10:: with a 64 bit prefix connect as client
allow 0/0	Allows all IPv4 addresses to connect as a client
allow ::/0	Allows all IPv6 addresses to connect as a client
allow	Allows all addresses to connect as a client

Configure UI Time Zone

Each user can assign the required time zone. The required time zone and the time zone used for creating the reports requested by a user, is available in the Graphical User Interface (GUI).

For users with the System Administrator role, this preference is found in the **Preferences > Administration > GUI** tab. Select the required time zone in the **Timezone** drop down list.

<div>Main</div> <div>GUI</div> <div>Alarms</div> <div>Maps</div> <div>Email</div> <div>VisionE15</div>	Parameter Name	Value	Description	Details (Current Setting)
	Timezone	America/New_York	User Timezone	America/New_York
	Default Calendar Range	LastDay	This parameters may take the following values; LastDay, LastHour, LastWeek. It defines the default time scale for the system when the user logs in. For best performance, use LastHour or LastDay.	Default calendar range is LAST DAY
	Refresh Table Interval (seconds)	120	Refresh table timer (in seconds). This will allow refreshing any table with autorefresh option on every defined interval. It is recommended to keep it above 10 seconds for optimized system performance.	
	Allow URL	1	Set it to 1 to allow probe to have url instead of IP	Allow probe to have URL instead of IP

For Users with any other role this preference is found in the **Preferences > Administration > General** tab. Select the required time zone in the **Timezone** drop down list.

Notification Alerts Silent Mode

0

Silence the notification alerts (bell icon in the top right corner)

Disable Notification alerts silent mode

Timezone

America/New_York

User Timezone

America/New_York

Save

Cancel

Restore To Default

This page intentionally left blank.

CHAPTER 12

Server CLI Commands

The Hawkeye Server supports the following CLI Commands:

Command	Options	Description
backupConfigurationData		Back up the Configuration Database (sql)
	-m , --memberid	Member Id, required when calls are mde from UI
	-n , --notificationType	Notification type, required when calls are mde from UI
	-h , --help	Prints help menu
	-v , --verbose	Verbose output
backupResultsData		Back up the Results Database (elastic)
	-m , --memberid	Member Id, required when calls are mde from UI
	-n , --notificationType	Notification type, required when calls are mde from UI
	-h , --help	Prints help menu
changeDBpasswd		change the SQL database password
changeRepo		Change the Package Repo
	optional arguments:	
	-h, --help	show this help message and exit
	--version	show program's version number and exit
	-q, --quiet	Perform quietly; only report errors
	--url URL	Repo base URL
	--release RELEASE	Release version (Major.Minor)

	Diagnostic output options:	
	-v, --verbose	Verbose output
	--debug DEBUG	Set debug output level
	--ftrace	Include function trace in debug output
collectDiagnostics		collect system diagnostics for inclusion in support escalations.
	-h, --help	show this help message and exit
	--version	show program's version number and exit
	-d DIAGNOSTICS, --diagnostics DIAGNOSTICS	collect system diagnostics, default: true
	-l LOGS, --logs LOGS	collect system logs, default: true
	-i INTERVAL, --interval INTERVAL	Interval for logs collector, ex: hour, day, week, Jun 1 2020 13:36
	-e ENCRYPT, --encrypt ENCRYPT	Encrypt archive, default: false
	-m MEMBERID, --memberid MEMBERID	Used just for UI calls, when greater than 0 it creates notification
	-td TIMEDIFF, --timeDiff TIMEDIFF	Used just for UI calls, time difference client-server
	-tza TIMEZONEABBREV, --timezoneAbbrev TIMEZONEABBREV	Used just for UI calls, client timezone abbreviation
	-a, --abort	Abort any collectDiagnostics process
	-ir, --isrunning	Check and respond if another collectDiagnostics process is running
hawkeyeConfigurationValidator		Validate the SQL Database configuration
	optional arguments:	
	-h, --help	show this help message and exit

	--version	show program's version number and exit
	-q, --quiet	Perform quietly; only have an exit code(0 no failures)
	-v, --verbose	Verbose output
	--debug DEBUG	Set debug output level
	-u USER, --user USER	User name to use for accessing Hawkeye Database
	-p PASSWD, --passwd PASSWD	Password to use for accessing Hawkeye Database
	-g GOLDEN, --golden GOLDEN	Golden file, just the version
	-d GOLDDIR, --golddir GOLDDIR	Directory where the Golden files are located
hawkeyeServices		Restart Hawkeye Services
	optional arguments:	
	-h, --help	show this help message and exit
	-i INCLUDE, --include INCLUDE	Include Services
	-e EXCLUDE, --exclude EXCLUDE	Exclude Services
hawkeyeStatus		Check the status of the Hawkeye Services
	optional arguments:	
	-h, --help	show this help message and exit
	--version	show program's version number and exit
	-a, --alarms	Include system monitor alarms in output
	-A, --archive_alarms	Include alarms archived in database in output
	-s, --stats	Include system monitor stats in output

	-c, --color	Force color output even if not a TTY
	-q, --quiet	Perform quietly; only report errors
	Diagnostic output options:	
	-v, --verbose	Verbose output
	--debug DEBUG	Set debug output level
	--ftrace	Include function trace in debug output
	--timestamps TIMESTAMPS	Include timestamps in logs ('relative' for relative timestamps)
packageCleanup		Removes old packages that are no longer needed. ex. Old Kernel packages
	optional arguments:	
	-h, --help	show this help message and exit
	--version	show program's version number and exit
	-y, --assumeyes	Assume "yes" to the delete query
	-f, --force	Force unsafe operation
	-n, --noact	Take no action that actually changes anything, just show what would be done
	-q, --quiet	Perform quietly; only report errors
	Diagnostic output options:	
	-v, --verbose	Verbose output
	--debug DEBUG	Set debug output level
	--ftrace	Include function trace in debug

		output
	--timestamps TIMESTAMPS	Include timestamps in logs ('relative' for relative timestamps)
renameHost		Takes HOSTNAME argument to change Server Hostname
updateServer		Trigger update of the Server from the CLI (online/offline)
	-h , --help	Prints help menu
	-c , --backupConfiguration	Create a backup for configuration (MariaDB)
	-r , --backupResults	Create a backup for results (ElasticSearch)
	-v , --releaseVersion	Set a fix release version, ex: 5.0
	-a , --abort	Stop static files server, restart Hawkeye services
	-C , --checkVersionOnly	Check the current version and the possible update version
	-n , --noninteractive	Interactive mode off
	-u , --ui	Request is performed from UI
	--offline	Perform and update from a local Hawkeye Server ISO

This page intentionally left blank.

CHAPTER 13

Troubleshooting

This chapter contains troubleshooting step for various functions of the Hawkeye Server. It also covers how to install additional tools to extend troubleshooting capabilities.

LDAP**Logs**

LDAP actions and errors are logged as part of Hawkeyes Authentication Logging. This log file can be found in /opt/hawkeye/logs/Hawkeye/Authentication.log

The following are example logs showing what is logged in various scenarios:

Bad password or if the user was not found.

```
[2021-02-05 14:58:27.596624 UTC] (index) Bind failed: Invalid credentials
[2021-02-05 14:58:27.596733 UTC] (index) Could not connect using remote authentication
server - Invalid credentials LDAP redirecting to login
```

User exists in ldap but is not a member of the group configured in preferences.

```
[2021-02-06 03:32:07.955771 UTC] (index) LDAP Group based authentication - start
[2021-02-06 03:32:08.014499 UTC] (index) Trying to bind with -
[2021-02-06 03:32:08.017528 UTC] (index) Found 1 LDAP group entries for filter
(cn=QualityControl)
[2021-02-06 03:32:08.018546 UTC] (index) Found 1 LDAP user entries for filter (|
(cn=devtester))
[2021-02-06 03:32:08.018616 UTC] (index) LDAP devtester matches the cn in LDAP element
returned - devtester
[2021-02-06 03:32:08.018753 UTC] (index) User not in authorized group. LDAP redirecting
to login
```

Generate packet captures

To generate a pcap to ensure traffic is leaving the expected interface with the correct ports assigned, do the following:

1. Ssh to the Hawkeye console as ksuser.
2. Execute the following command to capture a pcap trace of an openLDAP login.

```
# tcpdump 636 or 389 -I eth0 -w /tmp/openLDAP_trace.pcap
```

3. While the trace is running, attempt logging into Hawkeye.
4. Terminate capture with <ctrl>-C
5. Transfer the pcap trace to another computer and view the pcap trace file in Wireshark.

This page intentionally left blank.

Index

A

about this guide 13

C

component list unavailable for Hawkeye Express 13

configuring auto learn threshold 313

configuring global auto learn threshold 314

configuring IxProbe 86

configuring outlier 314

connecting IxProbe to Hawkeye 83

connecting through IxProbe CLI 83

customer assistance 3

D

detailed view 85

E

endpoints for Hawkeye 20

F

fudge factor 315

G

grid view 84

H

Hawkeye endpoints 20

Hawkeye introduction 14

Hawkeye overview 14

I

introduction to Hawkeye 14

IxProbe dashboard 83

IxProbe element manager introduction 83

IxProbe element manager overview 83

L

list view 84

N

new enhancements 11

new features 11

new updates 11

O

Outlier

introduction 313

overview 313

overview of Hawkeye 14

P

performing bulk action 89

add trap destination 89

add trusted subnet 89

delete 89

set hawkeye server 89

sync 89

product support 3

Q

quantization 315

S

Services, Apache web server service, mysql
service 334

T

technical support 3

types of views 83

U

upgrade server 378
 online upgrade 378
upgrade server;offline upgrade 378
upgrading hawkeye server 378

V

viewing audit trail 88
viewing port statistics 85
viewing system information 89

W

what's new 11

X

XR2000 overview, configuration 40
XRPi content, XRPi system information 22
XRPi setup, configure XRPi 25



© Keysight Technologies, 2025

This information is subject to change
without notice.

www.keysight.com

913-2383-01 Rev A