

Hawkeye

Release 6.0.7

Test Type 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
Chapter 1 Hawkeye Test Types	1
Test type general description	3
Node to Node	3
Understanding Node to Node Metrics	5
What is Goodput?	10
Testing Throughput Using TCP or UDP	10
Node to Node Test Types	11
TCP Throughput Tests	11
UDP Throughput Tests	21
Network KPI tests	29
QOS Qualification Tests	36
Voice and Video Tests	41
Video Stream	43
Unified Communications	53
Real Time Transactional Applications Tests	61
DSCP (QOS) Settings Explained	77
Details on Class of Service - Different Standards	78
Common Errors - N2N	81
Default Number of Tests per Probe Type (N2N)	84
Real Services	90
Licensing	91
Continuous	92
Advanced	97
Path Discovery	128
Real Service Endpoint Support Matrix	133

Replicating Tests Across Multiple Endpoints	137
Test Types Reporting Wi-Fi Statistics	137
Supported Protocols and Standards	143
Supported Voice over IP Codecs	146
Index	147

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 3**
 - Node to Node 3
 - Understanding Node to Node Metrics 5
 - What is Goodput? 10
 - Testing Throughput Using TCP or UDP 10
- Node to Node Test Types 11**
 - TCP Throughput Tests 11
 - UDP Throughput Tests 21
 - Network KPI tests 29
 - QOS Qualification Tests 36
 - Voice and Video Tests 41
 - Video Stream 43
 - Unified Communications 53
 - Real Time Transactional Applications Tests 61
 - DSCP (QOS) Settings Explained 77
 - Details on Class of Service - Different Standards 78
 - Common Errors - N2N 81
 - Default Number of Tests per Probe Type (N2N) 84
- Real Services 90**
 - Licensing 91
 - Continuous 92
 - Advanced 97
- Path Discovery 128**
- Real Service Endpoint Support Matrix 133**
- Replicating Tests Across Multiple Endpoints 137**
- Test Types Reporting Wi-Fi Statistics 137**

Supported Protocols and Standards143

Supported Voice over IP Codecs146

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 5](#)

[What is Goodput? on page 10](#)

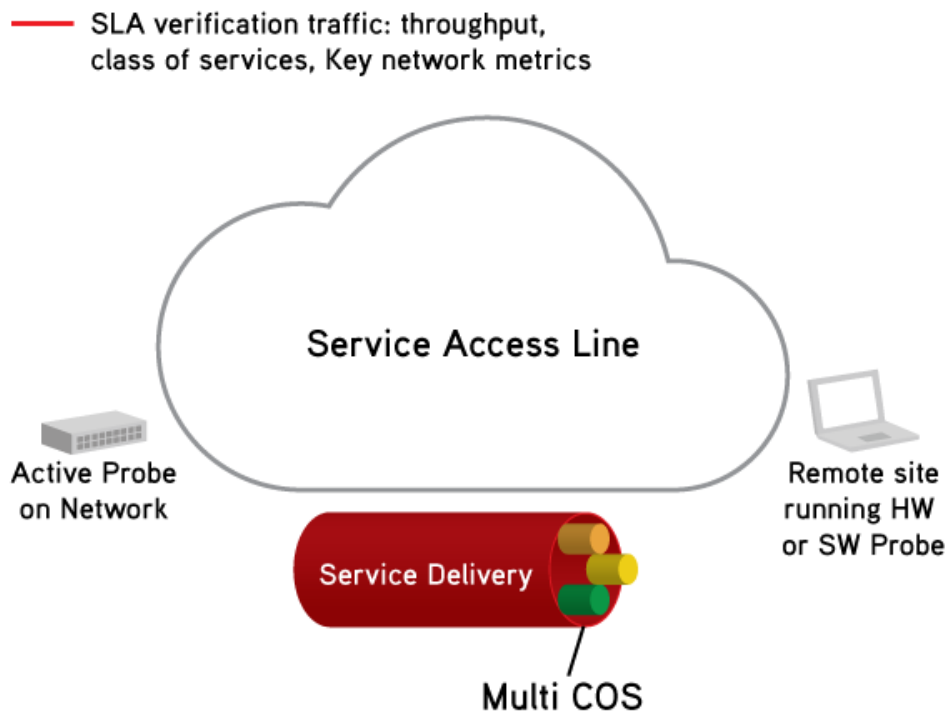
[Testing Throughput Using TCP or UDP on page 10](#)

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.

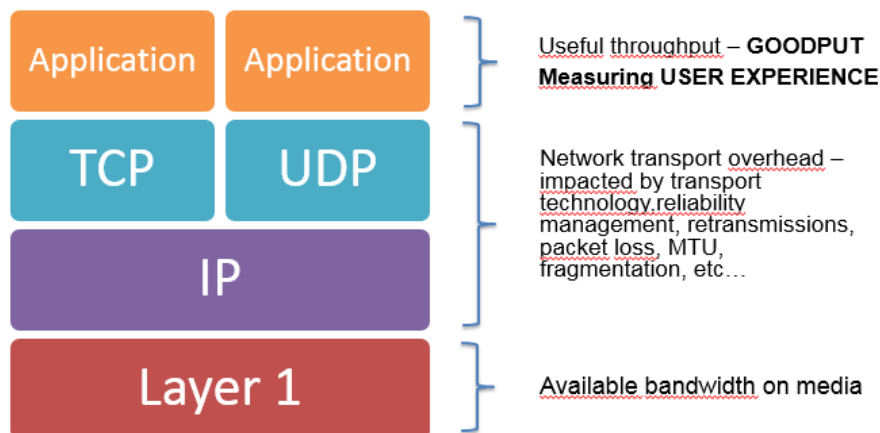
For example, if a file is transferred, the goodput that the user experiences corresponds to the file size in bits divided by the file transfer time. The goodput is always lower than the throughput (the gross bit rate that is transferred physically), which generally is lower than network access connection 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. <p>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.</p> <p>The recommended amount of TCP streams is between 5 and 10. The result is only displayed with aggregated results.</p> <p>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</p>

	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;">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> <p>NOTE 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.</p> <p>NOTE Maximize total throughput a large file size and small network delay are required.</p>
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

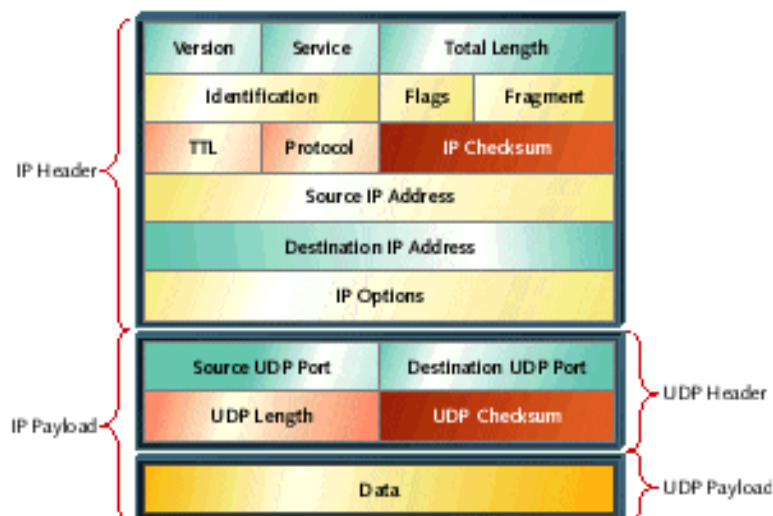
UDP Traffic Generation = Bit Blasting

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).

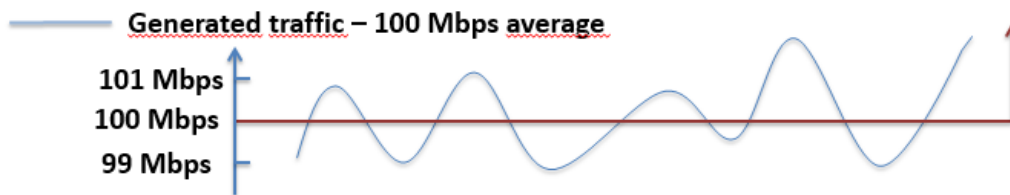
Even though the traffic generation is IP to IP (layer 4) inside UDP packets (layer 4) the result of the traffic generation can be considered as traffic blasting (aka RFC 2544 testing).

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> NOTE <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>

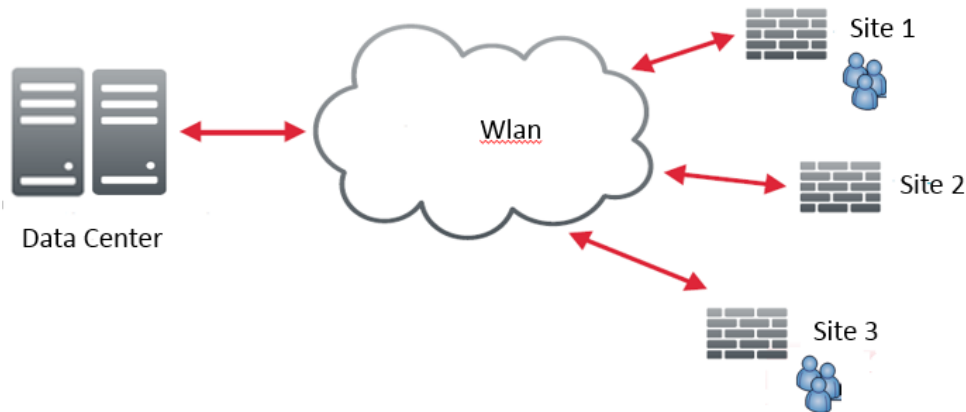
QOS Qualification Tests

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

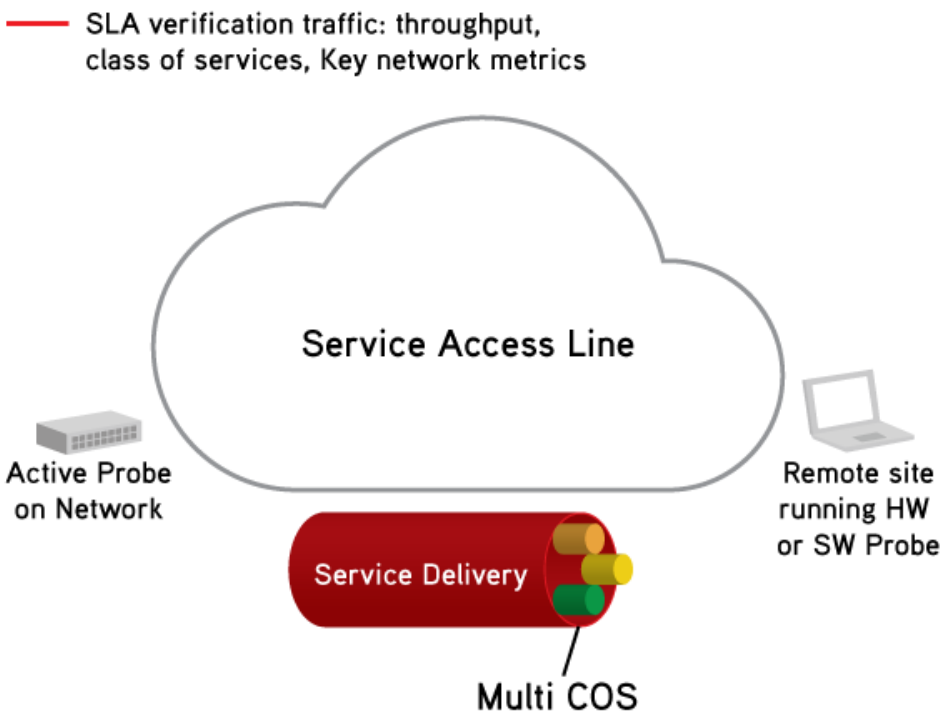


- Real time: Voice over IP, Unified communication voice
- Critical : Critical business applications
- Best Effort : Web, email etc...

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="display: flex; align-items: center;"> <div style="background-color: #cccccc; padding: 2px 5px; margin-right: 10px;">NOTE</div> <p>If generated bitrate is 0 on voice stream then this stream will be ignored</p> </div>
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> <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 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> <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 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.

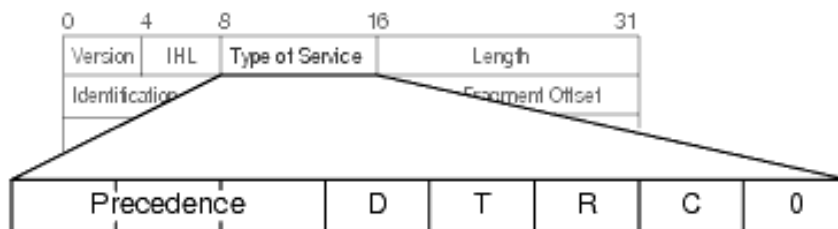
DS CP Class	DSCP (bin)	DSCP (hex)	DSCP (dec)	ToS (dec)	ToS (hex)	ToS (bin)	ToS Pr ec. (bin)	ToS Pr ec. (dec)	ToS Del ay Flag	ToS Throg hput Flag	ToS Reliab ility Flag	TOS String Format
none	000000	0x00	0	0	0x00	00000000	000	0	0	0	0	Routine
cs1	001000	0x08	8	32	0x20	00100000	001	1	0	0	0	Priority
af11	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	0×A 0	10100 000	101	5	0	0	0	Critical
ef	101 110	0× 2E	46	184	0×B 8	10111 000	101	5	1	1	0	Critical
cs6	110 000	0× 30	48	192	0×C 0	11000 000	110	6	0	0	0	Internetwork control
cs7	111 000	0× 38	56	224	0×E 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.

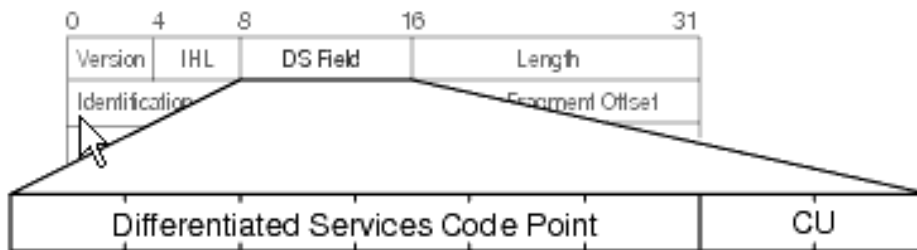
The last bit in the TOS byte is reserved and is always set to 0.

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
<div> <div>Status</div> <div>Reason Cause</div> </div>	
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

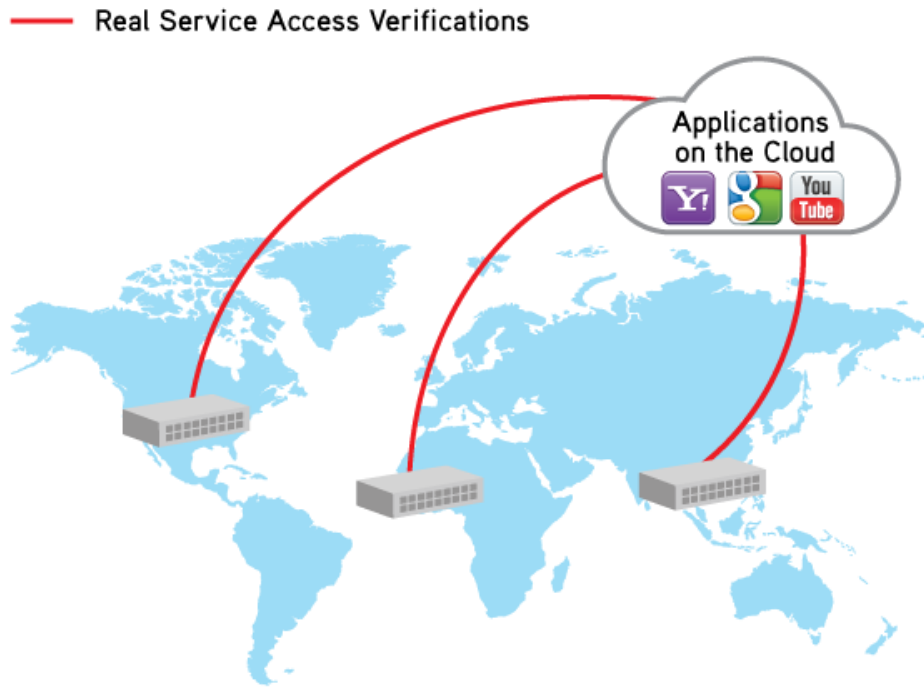
* The maximum number of simultaneous tests with the Trusted Subnet mode enabled is restricted to one.

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.

$3 \times 5 \times (60/90) = 10$ 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 <div> NOTE 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. </div>
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

Ping	
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	See Common Errors - Real Services.htm.

Web Page Download	
Description	The continuous HTTP request packets sent to a destination URL. Upto 10 destinations can be selected for each endpoint.
Purpose	To configure test once, so that the endpoint continuously reports test results.
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 • 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

Web Page Download	
	<ul style="list-style-type: none"> • 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

Wi-Fi	
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> NOTE 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. </div>
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 TCP SYN packets and listens for SYNACK responses.

Echo TCP	
Information	<div>NOTE</div> Up to 10 destinations can be selected for each endpoint.
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 <div>NOTE</div> 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.
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	This test sends UDP packets and listens for UDP packet responses. <div>NOTE</div> 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	<p>This test verifies key metrics to access AWS (Amazon Web Services) cloud.</p> <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>

	Cloud Test - AWS
	<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) • 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) • 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	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.

	Dropbox upload/download
	See Common Errors - Real Services in <i>Error Description Guide</i> .

	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 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	See Common Errors - Real Services in <i>Error Description Guide</i> .

	Email
Errors	

	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	This is user experience from probe to download file from specified FTP server If ftp not downloaded before end of timeout defined then the test will error out.
Potential Errors	See Common Errors - Real Services in <i>Error Description Guide</i> .

	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.

	FTP multistream download
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>
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

	Gaming Test - Fortnite
	<ul style="list-style-type: none"> • 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	<p>Generate TCP ping requests to known League of Legends servers.</p> <p>THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPi, XR-VM, and VisionE1S.</p>
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
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	Generate TCP ping requests to known World of Warcraft servers. THIS TEST IS SUPPORTED ON XR2000, XR2000VM, XRPI, XR-VM, and VisionE1S.
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 interpretation	See advanced information.
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

	HTTP Client Certificate Check test
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 Options	<ul style="list-style-type: none"> • Servers address or url - the list can contain up to 10 different servers • 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	This test will try to download http content on a url. It will simply analyze result

	HTTP response time
Information	<p>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>
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

	HTTP Server test
	<ul style="list-style-type: none"> • 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> $\text{Download time} = (\text{Download Size} * 8 / \text{KB Rate per sec})$ <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. <div style="background-color: #cccccc; padding: 5px; display: inline-block; margin-bottom: 10px;">NOTE</div> <p>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</p>

	HTTP Server test
	the certificate Select file pulldown selection menus.
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	Get user experience information downloading the web page content. this will include all images and JavaScript/css etc. Other information like DNS resolution will help correlate user experience to CDN (Content Data Network) architecture.
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	Per Web server and element: <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

	HTTP Server test-advanced
	<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 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. <div data-bbox="472 1451 662 1501">NOTE</div> <p>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	<p>The result should be reflective as the user experience getting from a browser to the web page.</p>

	HTTP Server test-advanced
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 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)

	ICMP test
	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 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

	IGMP test
	<ul style="list-style-type: none"> • 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
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.

Office365	
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 priority than data packets by network elements, therefore could show worst behavior than actual user traffic (prioritized) would experience in some cases.</p>
Potential Errors	<p>See Common Errors - Real Services in <i>Error Description Guide</i>.</p>

	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.

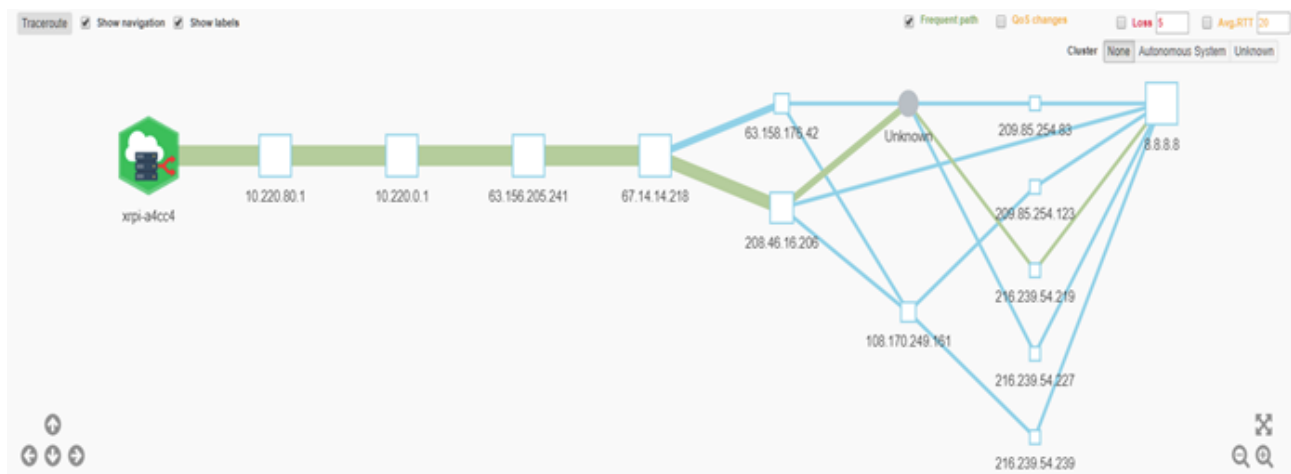
Destination port: this is used if protocol is TCP or UDP. The discovery messages will be sent with destination port set to this value and using a random source port. This can again be important when determining routing/COS management details on the path for specific protocol/port. Using the protocol 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:



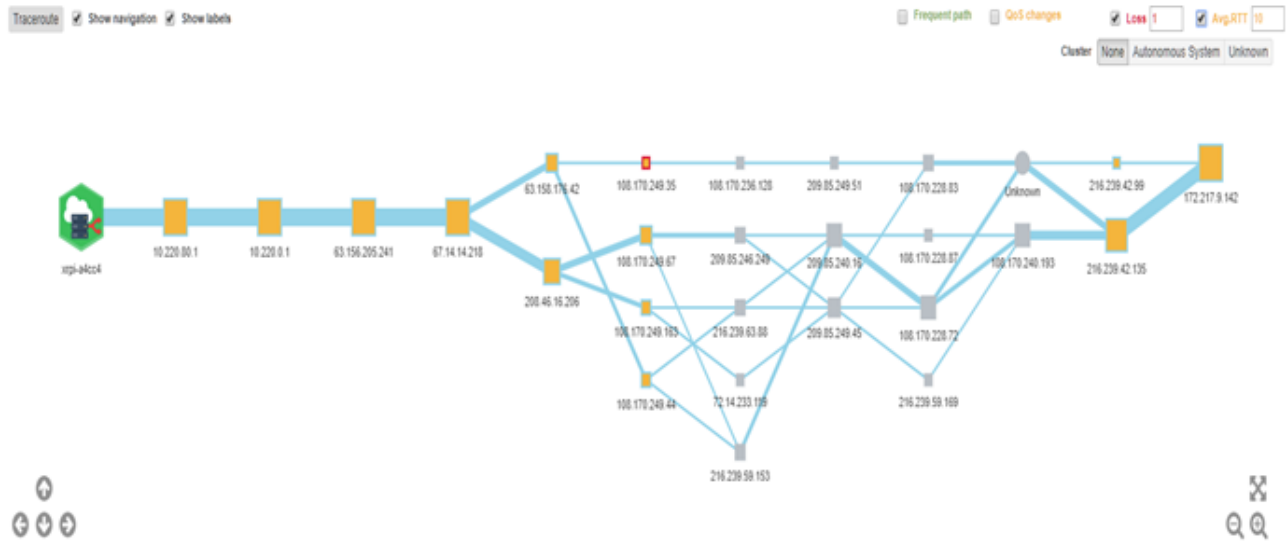
The different nodes detected in the path discovery are shown with squares.

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).

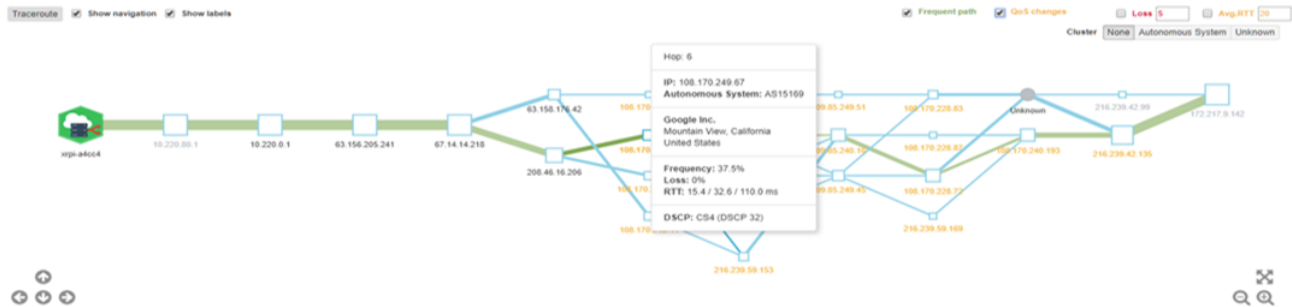
When the Hawkeye server has access to internet it can collect information to what AS code is registered.

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](#) 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	XRE1S	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	IxProb e IxTap IxByb pass
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	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	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

Index

	C
customer assistance	3
	P
product support	3
	T
technical support	3



© Keysight Technologies, 2025

This information is subject to change
without notice.

www.keysight.com

913-2383-01 Rev A