

# HST-3000

---

| IP Video Testing

User's Guide



# HST-3000

---

IP Video Testing

User's Guide



Communications Test and Measurement Solutions  
One Milestone Center Court  
Germantown, Maryland 20876-7100 USA  
Toll Free 1-855-ASK-JDSU  
Tel +1-240-404-2999  
Fax +1-240-404-2195  
[www.jdsu.com](http://www.jdsu.com)

**Notice** Every effort was made to ensure that the information in this document was accurate at the time of printing. However, information is subject to change without notice, and JDSU reserves the right to provide an addendum to this document with information not available at the time that this document was created.

**Copyright** © Copyright 2012 JDS Uniphase Corporation. All rights reserved. JDSU, Communications Test and Measurement Solutions, and the JDSU and logo are trademarks of JDS Uniphase Corporation (“JDS Uniphase”). All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted electronically or otherwise without written permission of the publisher.

**Copyright release** Reproduction and distribution of this guide is authorized for Government purposes only.

**Trademarks** JDS Uniphase, JDSU, HST-3000, and HST-3000C are trademarks or registered trademarks of JDS Uniphase Corporation in the United States and/or other countries.

Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Microsoft and Microsoft IPTV are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

NETGEAR is a registered trademark of NETGEAR, Inc. and/or its affiliates in the U.S. and certain other countries.

Rolling Stream is either a trademark or registered trademark of UTStarcom Inc. in the United States and/or other countries.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

**Ordering information** This guide is a product of JDSU's Technical Information Development Department, issued as part of the HST-3000. The catalog number for a printed guide is ML-058201. The catalog number for a USB stick containing the manual in electronic form is ML-060301.

**Terms and Conditions** The provision of hardware, services and/or software are subject to JDSU's standard terms and conditions available at [www.jdsu.com](http://www.jdsu.com).

**Federal Communications Commission (FCC) Notice** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with the limits of a Class B digital device JDSU requires that quality interface cables be used when connecting to this equipment. Any changes or modifications not expressly approved by JDSU could void the user's authority to operate the equipment.

**Industry Canada Requirements** This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

**WEEE and Battery Directive Compliance** JDSU has established processes in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive, 2002/96/EC, and the Battery Directive, 2006/66/EC.

This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from JDSU after 2005-08-13 can be returned for disposal at the end of its useful life. JDSU will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to JDSU for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to JDSU can be found in the Environmental section of JDSU's web site at [www.jdsu.com](http://www.jdsu.com). If you have questions concerning disposal of your equipment or batteries, contact JDSU's WEEE Program Management team at [WEEE.EMEA@jdsu.com](mailto:WEEE.EMEA@jdsu.com).

# Contents

---

<b>About This Guide</b>	ix
<b>Purpose and scope</b> . . . . .	x
<b>Assumptions</b> . . . . .	x
<b>Terminology</b> . . . . .	x
<b>Application-oriented user guide</b> . . . . .	xi
<b>HST-3000 base unit user's guide</b> . . . . .	xi
<b>Safety and compliance information</b> . . . . .	xi
<b>Technical assistance</b> . . . . .	xii
<b>Conventions</b> . . . . .	xiii

---

<b>Chapter 1</b>	<b>Getting Started</b>	<b>1</b>
	<b>Overview and options</b> . . . . .	2
	<b>Quick tour</b> . . . . .	3
	Status LEDs . . . . .	3
	Connections . . . . .	5
	Headset connector . . . . .	5
	USB connector . . . . .	5
	Ethernet connector . . . . .	5
	User interface navigation . . . . .	6

---

<b>Chapter 2</b>	<b>IP Video Testing</b>	<b>7</b>
	<b>About IP Video Testing</b> . . . . .	<b>8</b>
	<b>Specifying test settings</b> . . . . .	<b>8</b>
	Specifying Data settings . . . . .	9
	Specifying 802.1x security settings . . . . .	13
	Specifying STUN settings . . . . .	14
	Specifying PPP settings . . . . .	15
	Specifying WAN settings . . . . .	16
	<b>Video setup</b> . . . . .	<b>19</b>
	Specifying general video settings . . . . .	19
	Specifying Video QoS settings . . . . .	21
	Specifying MPEG QoS settings . . . . .	22
	Specifying Video Loss settings . . . . .	23
	<b>Authenticating on a secured network</b> . . . . .	<b>24</b>
	<b>Managing video channels</b> . . . . .	<b>26</b>
	Adding or editing video channels . . . . .	26
	Deleting a video channel . . . . .	27
	<b>Analyzing video streams</b> . . . . .	<b>28</b>
	Terminate mode . . . . .	29
	Monitor mode . . . . .	31
	<b>Measuring Class of Service</b> . . . . .	<b>33</b>
	<b>Saving test results</b> . . . . .	<b>36</b>

---

<b>Chapter 3</b>	<b>Interpreting Test Results</b>	<b>39</b>
	<b>About test results</b> . . . . .	<b>40</b>
	<b>Video Monitor</b> . . . . .	<b>41</b>
	<b>Stream QoS results</b> . . . . .	<b>43</b>
	<b>RTP results</b> . . . . .	<b>46</b>
	<b>Loss Summary results</b> . . . . .	<b>48</b>
	<b>Packet statistics</b> . . . . .	<b>50</b>
	<b>Stream (TS) statistics</b> . . . . .	<b>51</b>
	<b>Stream Rates</b> . . . . .	<b>53</b>
	<b>PID Map results</b> . . . . .	<b>54</b>
	<b>Video Totals results</b> . . . . .	<b>55</b>
	<b>Monitor Log</b> . . . . .	<b>57</b>



<b>Video Error Log results</b> . . . . .	57
<b>Class of Service results</b> . . . . .	58
Graphs . . . . .	58
Status . . . . .	59
Analysis . . . . .	59
Packet . . . . .	60
Config . . . . .	61
<hr/>	
<b>Appendix A Technology and methodology</b> . . . . .	63
<b>About IP video technology</b> . . . . .	64
Content Quality . . . . .	65
PCR Jitter . . . . .	66
Transport Error Indicator . . . . .	67
Network Quality . . . . .	67
Packet Loss . . . . .	67
Packet Jitter . . . . .	68
IGMP Latency . . . . .	68
Summary . . . . .	70
<b>Service Testing and Troubleshooting methodology</b> . . . . .	71
Packet loss . . . . .	71
PCR jitter . . . . .	72
Error indicator . . . . .	72
IGMP latency . . . . .	73
Summary . . . . .	73
Practical example . . . . .	73
<hr/>	
<b>Glossary</b> . . . . .	75
<hr/>	
<b>Index</b> . . . . .	79



# About This Guide

This chapter describes how to use this guide. Topics discussed in this chapter include the following:

- “Purpose and scope” on page x
- “Assumptions” on page x
- “Terminology” on page x
- “Application-oriented user guide” on page xi
- “HST-3000 base unit user’s guide” on page xi
- “Safety and compliance information” on page xi
- “Technical assistance” on page xii
- “Conventions” on page xiii

## Purpose and scope

The purpose of this guide is to help you successfully use the features and capabilities of the HST-3000.

This guide includes task-based instructions that describe how to configure, use, and troubleshoot the HST-3000's IP video testing option.

---

## Assumptions

This guide is intended for novice, intermediate, and experienced users who want to use the HST-3000 effectively and efficiently. We are assuming that you have basic computer experience and are familiar with basic telecommunication concepts, terminology, and safety.

---

## Terminology

The following terms have a specific meaning when they are used in this guide:

- **HST-3000** — Handheld Services Tester 3000. In this user's guide, "HST-3000" is used to refer to the HST-3000 family of products or to the combination of a base unit and attached SIM. "HST" is also sometimes used to refer to the base unit/SIM combination.
- **SIM** — Service Interface Module. Sometimes referred to generically as the module. The SIM provides test application functionality.

For definitions of other terms used in this guide, see "[Glossary](#)" on page 75.

## **Application-oriented user guide**

The ***HST-3000 IP Video Testing User's Guide*** is an application-oriented user's guide contains information relating to the basic use of the device and includes detailed procedures for testing and troubleshooting IP video service.

This user's guide should be used in conjunction with the *HST-3000 Base Unit User's Guide*.

---

## **HST-3000 base unit user's guide**

The *HST-3000 Base Unit User's Guide* contains overall information relating to device and general functions such as using the unit with a keyboard, peripheral support, battery charging, printing results, and managing files. This guide also contains technical specifications for the base unit and a description of JDSU's warranty, services, and repair information, including terms and conditions of the licensing agreement.

---

## **Safety and compliance information**

Safety and compliance information are contained in a separate guide and are provided in printed format with the product.

---

## Technical assistance

If you need assistance or have questions related to the use of this product, use the information in [Table 1](#) to contact JDSU's Technical Assistance Center (TAC) for customer support.

Before you contact JDSU for technical assistance, please have the serial numbers for the service interface module (SIM) and the base unit handy (see "Locating the serial number" in the *HST-3000 Base Unit User's Guide*).

**Table 1** Technical assistance centers

Region	Phone Number	
Americas	1-855-ASK-JDSU 1-866-228-3762 301-353-1550	<a href="mailto:tac@jdsu.com">tac@jdsu.com</a>
Europe, Africa, and Mid-East	+49 (0) 7121 86 1345 (JDSU Germany)	<a href="mailto:hotline.europe@jdsu.com">hotline.europe@jdsu.com</a>
Asia and the Pacific	+852 2892 0990 (Hong Kong)  +8610 6833 7477 (Beijing-China)	

During off-hours, you can request assistance by doing one of the following: leave a voice message at the TAC for your region; email the North American TAC ([tac@jdsu.com](mailto:tac@jdsu.com)); submit your question using our online Technical Assistance request form at [www.jdsu.com](http://www.jdsu.com).

## Conventions

This guide uses conventions and symbols, as described in the following tables.

**Table 2** Typographical conventions

Description	Example
User interface actions and buttons or switches you have to press appear in this <b>typeface</b> .	Press the <b>OK</b> key.
Code and output messages appear in this <i>typeface</i> .	All <code>results</code> okay
Text you must type exactly as shown appears in this <b>typeface</b> .	Type: <code>a:\set.exe</code> in the dialog box.
Variables appear in this <b>typeface</b> .	Type the new <b>hostname</b> .
Book references appear in this <i>typeface</i> .	Refer to <i>Newton's Telecom Dictionary</i>

**Table 3** Keyboard and menu conventions

Description	Example
A plus sign + indicates simultaneous keystrokes.	Press <b>Ctrl+s</b>
A comma indicates consecutive key strokes.	Press <b>Alt+f,s</b>
A slanted bracket indicates choosing a submenu from menu.	On the menu bar, click <b>Start &gt; Program Files</b> .

**Table 4** Symbol conventions



This symbol represents a general hazard.



This symbol represents a risk of electrical shock.



This symbol represents a risk of explosion



This symbol represents a Note indicating related information or tip.



This symbol, located on the equipment, battery, or packaging indicates that the equipment or battery must not be disposed of in a land-fill site or as municipal waste, and should be disposed of according to your national regulations.

**Table 5** Safety definitions

**DANGER**

Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

**WARNING**

Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

**CAUTION**

Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.



# Getting Started

# 1

This chapter provides a general description of the HST-3000's optional IP video testing features. Topics discussed in this chapter include the following:

- [“Overview and options” on page 2](#)
- [“Quick tour” on page 3](#)

## Overview and options

The HST-3000's optional IP video testing features (ordering number HST300S-IP-Video) allow verification of video service and testing of video quality.

The capabilities of the HST-3000 IP video feature includes the following:

- Physical medium test
- IP connectivity test
- Video service verification
  - IP multicast test - Broadcast video service  
Generate IGMP “join” and “leave” requests, verifying stream flows, changing channels, and multi-cast communications are working.
  - IP unicast test - VOD video service  
Generate RTSP client requests for access to VOD media server, verifying that program stream flows and uni-cast communications are working.
  - Microsoft IP TV service
  - UTStarcom Rolling Stream service
- Video quality test
  - Analyze video streams (ISO/IEC 13818 packet formats)
  - Provide statistics on up to 10 streams, with detailed analysis of up to three streams

You can expand your testing capability by purchasing additional IP Video testing options. The options available for purchase are as follows:

**Table 6** IP Video testing options

Option	Description	Order Number
Microsoft IP TV	Allows you to test Microsoft IP TV video streams.	HST3000-MSTV
Microsoft Video MOS	Provides mean opinion score (MOS) for IP video applications.	HST3000-VMOS

For additional information about HST-3000 options, SIMs, and services, contact your local JDSU representative or contact JDSU through the company web site, [www.jdsu.com](http://www.jdsu.com).

## Quick tour

The following section describes the status indicators and connections applicable to IP video.

**Status LEDs** These indicators report the status of the interface, and are not specific to the IP video application. The function of each LED is described in [Table 7](#).

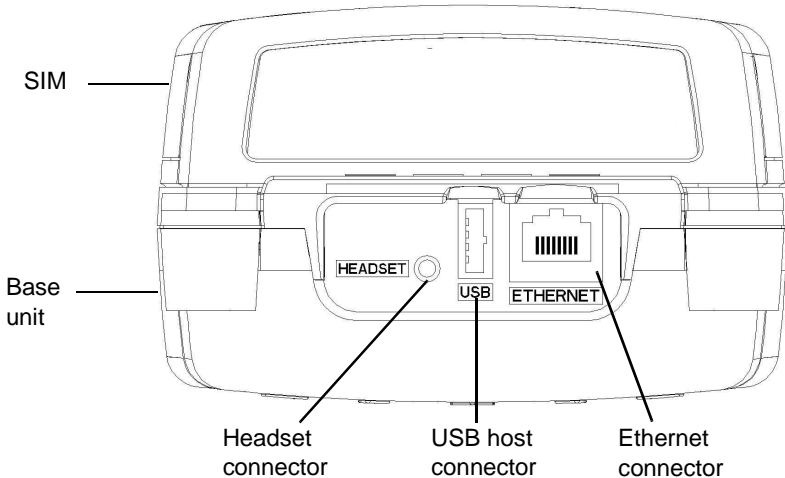
**Table 7** Status LEDs

LED	Function
Sync	<p>A two-color LED that reports the status of modem synchronization.</p> <ul style="list-style-type: none"> <li>– Flashing green indicates that the modems are training.</li> <li>– Solid green indicates that the modems have synchronized.</li> <li>– Solid red indicates a synchronization error has occurred.</li> </ul>

**Table 7** Status LEDs (Continued)

LED	Function
Data	<p>A two-color LED that reports the status of the data connection.</p> <ul style="list-style-type: none"><li>– Flashing green indicates that the data connection is not yet established.</li><li>– Solid green indicates that a data connection has been established with the network (so that the HST-3000 may send and receive data on the network).</li><li>– Solid red indicates that a data network connection has not been established.</li></ul>
Error	<p>A two-color LED that reports error conditions.</p> <ul style="list-style-type: none"><li>– Solid red indicates an error condition.</li></ul>
Alarm	<p>A two-color LED that indicates alarm conditions.</p> <ul style="list-style-type: none"><li>– Solid red indicates an alarm condition.</li></ul>
Lpbk	<ul style="list-style-type: none"><li>– Not used in IP video mode.</li></ul>
Batt	<p>Indicates the battery status. For more information, see the <i>HST-3000 Base Unit User's Guide</i>.</p>

**Connections** The HST-3000 top panel, is used to connect test leads, an audio headset, or to connect to an external output device. [Figure 1](#) shows the top panel.



**Figure 1** HST-3000 top panel

The connectors on the top panel are described in the following sections.

**Headset connector** The Headset connector is used to connect a 2.54mm microphone/speaker audio headset.

**USB connector** This USB host connector is used to connect the HST-3000 to a printer (device) for transferring test statistics.

**Ethernet connector** The Ethernet connector is used to connect a 10/100 BaseT Ethernet cable. If connecting to a PC, a cross-over cable should be used.

**User interface navigation** You can use the Home and Config keys to cycle through the applications. The menus cycle in order, top to bottom as shown on the main application screen.

For example, if you are in the Ethernet TE application, pressing Home will move to the VoIP application, and then IP Video.

The same methodology applies to the configuration menus. If you are viewing the Data settings, pressing Config will move to the VoIP General settings, and then the Video Settings.

# IP Video Testing

## 2

This chapter provides task-based instructions for using the optional HST-3000 IP video testing features. Topics discussed in this chapter include the following:

- “About IP Video Testing” on page 8
- “Specifying test settings” on page 8
- “Authenticating on a secured network” on page 24
- “Managing video channels” on page 26
- “Analyzing video streams” on page 28
- “Measuring Class of Service” on page 33
- “Saving test results” on page 36

## About IP Video Testing

For IP video testing, use either the Ethernet port or the DSL port to connect to the line. Thus, there are multiple ways to access the IP video feature: through ADSL mode, VDSL mode, or Ethernet mode.

**NOTE:**

This guide is specific to IP video testing. For more information on ADSL, VDSL, or Ethernet testing, including connecting to the line, see the *HST-3000 ADSL Testing User's Guide*, *HST-3000 ADSL2 Testing User's Guide* or the *HST-3000 VDSL Testing User's Guide*.

IP video testing involves the following steps:

- specifying test settings
- selecting Terminate or Monitor mode
- selecting service type (Terminate mode only)
- setting QoS thresholds
- performing the tests

---

## Specifying test settings

Before you begin testing, make sure the test settings on the HST-3000 match the settings of the line and network configuration you are testing.

The setup procedure varies slightly, depending on the access interface and the network configuration. Configurations can be stored for easy recall and use (for more information, see the *HST-3000 Base Unit User's Guide*).



The following settings must be specified:


- Data Settings (see “Specifying Data settings” on page 9)
- 802.1x Authentication Settings (see “Specifying 802.1x security settings” on page 13)
- STUN settings (see “Specifying STUN settings” on page 14)
- PPP Settings (see “Specifying PPP settings” on page 15)
- WAN Settings (see “Specifying WAN settings” on page 16)

For more information on other configuration items (Ping, Trace Route, and so on), see the *HST-3000 ADSL2 Testing User’s Guide* or the *HST-3000 VDSL Testing User’s Guide*.

## Specifying Data settings

The Data settings menu varies, depending on the interface. The following procedure describes how to set the Data settings.

### To specify Data settings

- 1 Select the interface (ADSL, VDSL, or Ethernet).
- 2 Do one of the following.
  - From the main ADSL or VDSL Measurements screen, select the **Data** application.
  - From main Ethernet Measurements screen, select **Ethernet TE**.
- 3 Press the **Configure**  navigation key.  
The parameter soft keys appear.
- 4 Press the **DATA** soft key.



### CAUTION: FAULTY RESULTS

Changing these settings during a test may cause errors in the test. Only change them before you begin a test.

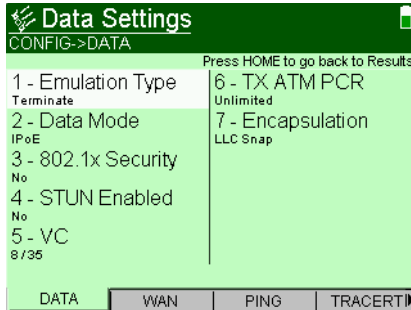
The Data Settings menu appears.

5 Specify the **Data mode**.

**NOTE:**

The Data mode must be set. If it is *Off*, Video testing is disabled.

6 Select **Emulation Type** and specify the type of emulation: Terminate or Through.



This selection is only available to change if on an ADSL or VDSL interface.

7 Select **802.1x Security** and then specify whether 802.1x authentication is supported on your network.

This setting is only applicable if you are using IPoE data mode.

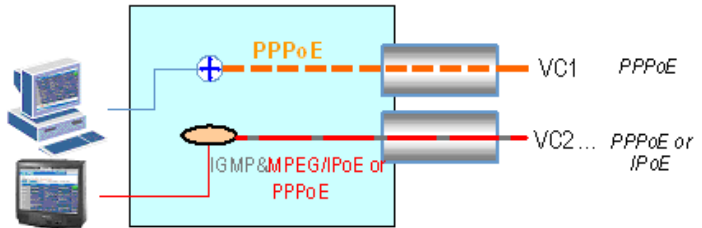
8 Select **STUN Enabled** and then specify whether STUN is enabled.

This setting is only applicable if you are using IPoE data mode.

If you are on a VDSL interface, you are finished specifying Data Settings.

9 If you are on an ADSL interface, enter the VPI and VCI, as outlined below. The process varies depending on your network configuration.

Typically, the video data flows are in a different VC from the internet data service, as shown below (VC1 is the internet data).



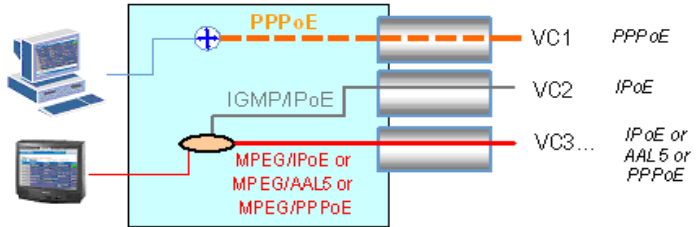
If this is your network configuration, perform the following:

- a Select **Data Mode**, and then select the type of line you are testing: IPoE or PPPoE.
- b Select **VC**, and then enter the virtual path indicator (VPI) and virtual channel indicator (VCI) for the virtual channel (VC) under test.
- c Select **TX ATM PCR**, and then enter the QoS setting called Transmit Peak Cell Rate. This limits the bandwidth of the signaling protocol flows (IGMP or RTSP).
  - **Unlimited** means that there is no specific limit placed on the signaling messages.
  - **User Specified** allows you to enter a value from 2 to 50000 cells per second, which limits the bandwidth, or data rate, of the signaling messages.

**NOTE:**

If the rate entered is not attainable, the HST will round down to the next attainable rate.

However, some networks use one virtual channel for the IGMP signaling and another for the actual video flows, as shown below.



If this is your network configuration, perform the following:

- a Select **Data Mode**, and then select **IPoE MVC Video** or **Bridged MVC Video**.
- b Select **VC**, and then enter the virtual path indicator (VPI) and virtual channel indicator (VCI) for the virtual channel (VC) of the IGMP signaling channel.
- c Select **TX ATM PCR**, and then specify the QoS setting called Transmit Peak Cell Rate. This limits the bandwidth of the signaling protocol flows (IGMP or RTSP).
  - **Unlimited** means that there is no specific limit placed on the signaling messages.
  - **User Specified** allows you to enter a value from 2 to 50000 cells per second, which limits the bandwidth, or data rate, of the signaling messages.

**NOTE:**

If the rate entered is not attainable, the HST will round down to the next attainable rate.

- d Select **Video RX VC 1**, and then enter the virtual path indicator (VPI) and virtual channel indicator (VCI) for the first video channel (the broadcast program data).
- e Select **Video RX VC 2**, and then enter the virtual path indicator (VPI) and virtual channel indicator (VCI) for the second video channel (the VOD program data).

- f Select **Video VOD VC**, and then enter the virtual path indicator (VPI) and virtual channel indicator (VCI) for the third video channel, which typically carries the RTSP video on demand (VOD) signaling.

**NOTE:**

The VPI and VCI selections for each virtual channel (VC) should be different. If your network does not require the additional virtual channels, ensure that the VPI and VCI selections do not match those in use.

- g Select **VOD TX ATM PCR**, and then specify the transmit peak cell rate for the third video channel.

The Data settings are specified.

**Specifying 802.1x security settings**

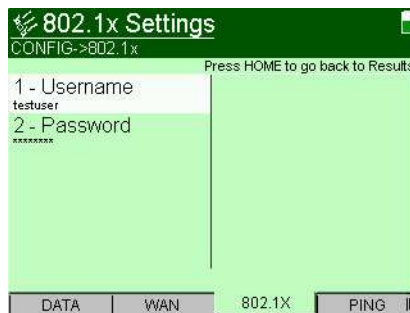
The 802.1x Settings menu appears only if you are using the IPoE data mode and “802.1x Security” is set to “Yes” on the Data Settings menu.

The 802.1x Settings are used to access a secured network. The following procedure describes how to specify the 802.1x settings.

**To specify 802.1x settings**

- 1 Press the **802.1X** soft key. You may need to scroll left or right to find it.

The 802.1x Settings screen appears.



- 2 Press **2** then enter the User Name.
- 3 Press **3** then enter the Password.

The 802.1x settings are specified.

## Specifying STUN settings

This screen is only available if you are using IPoE data mode and “STUN Enabled” is set to “Yes” on the Data Settings menu.

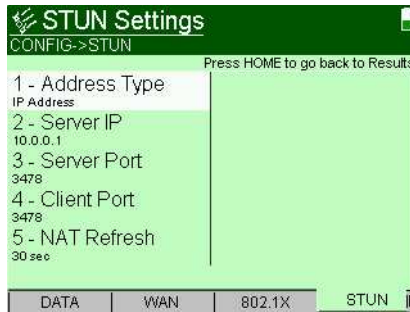
STUN (Simple Transversal of UDP [User Datagram Protocol] Through NATs [Network Address Translators]) allows VoIP calls across a NAT router. These settings should only be changed if necessary.

The following procedure describes how to specify the STUN settings.

### To specify the STUN settings

- 1 Press the **STUN** soft key.

The STUN Settings menu appears.



- 2 Select **Address Type**, and then specify whether an **IP Address** or **DNS Name** is used.
- 3 If you selected IP Address in [step 2](#), select **Server IP**, and then enter the IP address of the STUN server.

If you selected DNS Name in [step 2](#), select **Server Name**, and then enter DNS name of the STUN server.

- 4 Select **Server Port**, and then enter the port number for the STUN server.
- 5 Select **Client Port** and then enter the client port number.
- 6 Select **NAT Refresh** and then specify the NAT refresh rate. This is the number of seconds between messages to the STUN server to keep the NAT mapping alive.

The STUN settings are specified.

**NOTE:**

If STUN is enabled, the data layer will not come up until the STUN client on the HST has determined the type of NAT used between the HST and the STUN server.

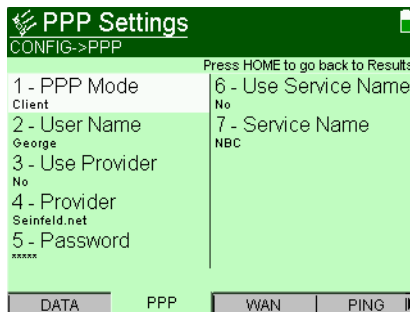
## Specifying PPP settings

The following procedure describes how to specify the point-to-point protocol (PPP) settings

### To specify PPP settings

- 1 Press the **PPP** soft key.

The PPP Settings menu appears.



- 2 Select **PPP Mode**, and then select either **Client** or **Server**.

Client is normally used. Use Server only when you have an ATU-C. This feature allows a remote ATU-R to establish a PPP session with the HST-3000.

**NOTE:**

If you selected “Server” as the PPP mode, connect only to other devices with the same service name.

- 3** Select **User Name**, and then enter a valid user name.  
This must be a valid user account with an ISP.
- 4** Select **Use Provider**, and then select either **Yes** or **No**.  
This option indicates whether to append the user name with the service provider domain name (for example, earthlink.net). Select Yes only if user names for the ISP must include the domain name as part of the user name. This setting automatically appends the @ sign for you.
- 5** Select **Provider**, and then enter the provider name.  
This is required if you selected Yes for “Use Provider.”
- 6** Select **Password**, and then enter the user password.  
This must be a valid password that matches the user name above. Passwords are often case-sensitive.
- 7** Select **Use Service Name**.  
This selection allows you to request a specific service, by name.
- 8** If you selected “Yes” for Use Service Name, enter the **Service Name**, up to 50 characters.

The PPP settings are specified.

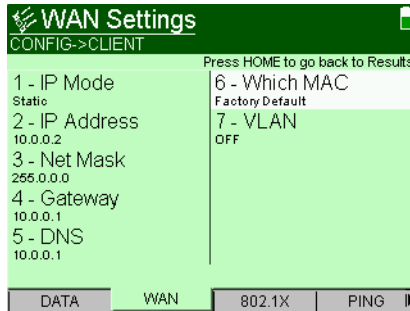
**Specifying WAN settings** The following procedure describes how to specify the wide area network (WAN) settings. The WAN interface is the DSL connection to tip and ring.



## To specify WAN settings

- 1 If you are on a xDSL line and using IPoE, PPPoE, or IPoA Data mode, press the **WAN** soft key. You may need to use the left or right arrows to find the soft key.

The WAN Settings menu appears.



The menu items vary depending on the Data mode.

### NOTE:

If you selected PPPoA or Bridged Ethernet as the Data mode, the WAN settings are not applicable, and thus the WAN tab is not displayed.

- 2 If you are using IPoE or IPoA data mode, select **IP Mode**, then select either **Static** or **DHCP** (dynamic host configuration protocol).

If you selected DHCP, do the following.

- a Select **Use Vendor ID** and specify whether the vendor ID is used.

If you selected Yes, enter the **Vendor ID**.

- b Go to [step 3](#).

If you selected Static, do the following.

- a Select **IP Address**, then enter the IP address.

- b Select **Net Mask**, then enter the net mask address.



## Video setup

After the physical layer is setup, you should configure the video setup.


There are three types of settings to specify:

- General video settings (see “[Specifying general video settings](#)”)
- Video QoS settings (see “[Specifying Video QoS settings on page 21](#)”)
- Video Loss settings (see “[Specifying Video QoS settings on page 21](#)”)

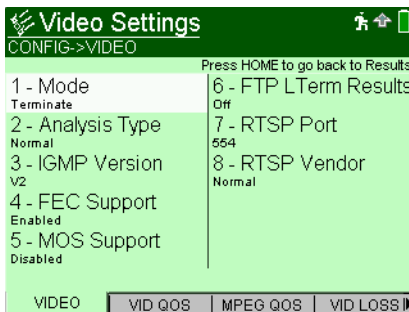
### Specifying general video settings

The following procedure describes how to specify the general video settings.

#### To specify general video settings

- 1 Press the **Configure**  navigation key.  
The parameter soft keys appear.
- 2 Press the **VIDEO** soft key. You may need to scroll left or right to find it.

The Video Settings screen appears.



- 3** Select **Mode**, and then select Terminate or Monitor.

This selection can only be changed if using an Ethernet connection. If using an ADSL or VDSL connection, the mode is set based on your application. If you are emulating a modem, the mode is set to Terminate; if you are in through mode, the mode is set to Monitor.
- 4** Select the **Analysis Type** (Terminate mode) or **Monitor Type** (Monitor mode) and then select Normal or UT (Microsoft is a third option but only in Monitor Mode).

Use **Microsoft** when analyzing Microsoft IPTV streams.  
Use **UT** when analyzing Rolling Stream video streams.
- 5** If you are in Monitor mode, specify the **Transport Type**: normal IPoE, VLAN IPoE, PPPoE, or VLAN PPPoE.
- 6** If you are in Terminate mode, select **IGMP Version**, and then specify the version of IGMP signaling being used on the circuit: version 2 or version 3.
- 7** Select **FEC Support**, and then enable or disable FEC Support.

This selection controls whether the HST will try to detect PRO-MPEG FEC error correction for the stream.
- 8** Select **MOS Support**, and then enable or disable MOS Support.

This controls whether the HST will calculate MOS values for the stream. If this is enabled, the simultaneous stream analysis capabilities of the HST are reduced from 3 to 2 on color LCD units and to 1 on monochrome LCD units.
- 9** If MOS Support is enabled, specify the MOS ISMA Audio specification and MOS ISMA Video specification.

If MOS analysis is done on an ISMA type stream, these items tell the HST what the video and audio codecs of the stream will be.
- 10** Select **FTP LTerm Results**, and then enable or disable transferring of results for long term tests.

This selection allows you to save results (as a .xml file) on a timed interval and FTP each file. This is useful for long term monitoring.

- 11 Select **RTSP Port**, and then enter the port number.

This is the port where RTSP signaling communication takes place in a particular network.

- 12 Select **RTSP Vendor** and then enter the RTSP Vendor.

This setting is only relevant in Terminate mode.

The Video settings are specified.

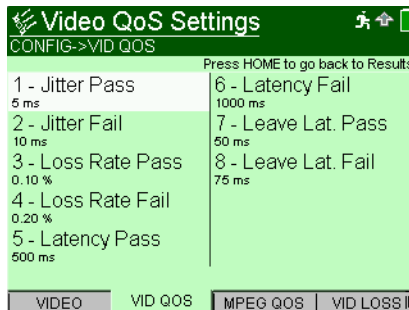
## Specifying Video QoS settings

The following procedure describes how to specify the Video QoS settings.

### To specify Video QoS settings

- 1 Press the **VID QOS** soft key. You may need to scroll left or right to find it.

The Video QoS Settings screen appears.



- 2 Press **1** then enter the Jitter Pass threshold, in msec.
- 3 Press **2** then enter the Jitter Fail threshold, in msec.
- 4 Press **3** then enter the Loss Rate Pass threshold, in percent.
- 5 Press **4** then enter the Loss Rate Fail threshold, in percent.

- 6 Press **5** then enter the Latency Pass threshold, in msec.
- 7 Press **6** then enter the Latency Fail threshold, in msec.
- 8 Press **7** then enter the Leave Latency Pass threshold, in msec.
- 9 Press **8** then enter the Leave Latency Fail threshold, in msec.

The video QoS settings are specified.

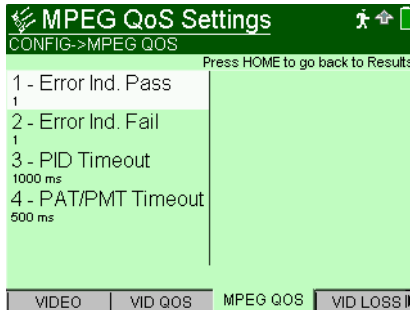
## Specifying MPEG QoS settings

The following procedure describes how to specify the MPEG settings.

### To specify MPEG QoS settings

- 1 Press the **MPEG QOS** soft key. You may need to scroll left or right to find it.

The MPEG QoS Settings screen appears.



- 2 Press **1** then enter the Error Indicator Pass threshold, between 1 and 1000.
- 3 Press **2** then enter the Error Indicator Fail threshold, between 1 and 1000.

This threshold controls the number of times the Error Indicator bit can be set in the MPEG2-TS header before the Error Ind. QoS is changed.

- 4 Press **3** then specify the PID Timeout.

This is the amount of time to wait for a PID that has been declared as having video or audio data for traffic, since the last traffic was received. If this threshold is violated, then the PID Timeout result will increment.

- 5 Press **4** then specify the PAT/PMT Timeout.

This is the amount of time to wait after the last received PAT or PMT packet before declaring a timeout condition (which would then increment the PAT Errors or PMT Errors statistics).

The MPEG QoS settings are specified.

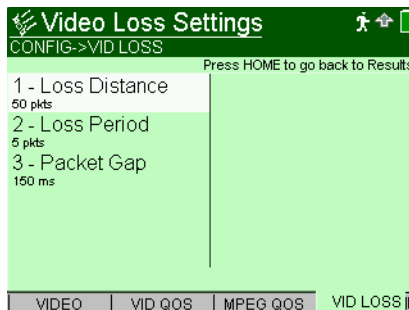
## Specifying Video Loss settings

RFC 2680 and RFC 3357 define enhanced analysis methods that are used to measure the quality of a media stream. There are two main statistics for this: Loss Period and Loss Distance. These two statistics are specified on the Video Loss screen.

### To specify Video Loss settings

- 1 Press the **VID LOSS** soft key. You may need to scroll left or right to find it.

The Video Loss Settings screen appears.



- 2 Press the **1** key to set the Loss Distance threshold, in number of packets. Enter a number between 1 and 10,000,000.

“Loss Distance” measures the difference in sequence numbers of two loss events, with a “loss event” being the loss of one or more packets in a row. So for the following stream (1 x 3 4 5 x x 8 9 10) the loss distance between the two events is 4. If the loss distance is less than the configured threshold, then the “Loss Distance Error” statistic will increment.

- 3** Press the **2** key to set the Loss Period threshold, in number of packets. Enter a number between 1 and 1000.

“Loss period” is the length of a single loss event, that is, the number of lost packets between two successfully received packets. So for the following example stream (1 x x x 5 6 7 x x 10 x 12), there are three loss periods, with lengths of 3, 2, and 1.

- 4** Press the **3** key to set the Packet Gap, in milliseconds. Enter a number between 10 and 10000.

The packet gap is the time interval between subsequent packets in a video stream. When the packet gap exceeds the threshold set here, the “Gap Errors” statistics will increment.

The video loss settings are specified.

---

## **Authenticating on a secured network**

IEEE 802.1x offers a framework for authenticating and controlling user traffic on a protected (secured) wireless network. Authentication involves a supplicant (a client device) attempting to connect with an authenticator (the 802.11 access point), using a certificate. The access point (authenticator) blocks all other traffic until it can verify the client's identity. After authenticated, the access point opens the client's port for other types of traffic, and the user can log into the network. For this authentication, the HST acts as a supplicant.



The process involves two main steps:

- downloading a certificate
- logging in to the secured network

#### **To authenticate on a secured network**

- 1** Press the **System** navigation key, and then press the **INSTRUMENT** soft key.
- 2** Select **Certificate Settings**.
- 3** Select **Cert FTP Addr**, and then enter the FTP address for retrieving a certificate.
- 4** Specify the **User Name** and **Password**.
- 5** Press the **Start** soft key.  
The HST downloads a certificate (using FTP).
- 6** Press the **Configure** navigation key, and then press the **DATA** soft key.
- 7** Verify that you are using IPoE **Data Mode**, and then enable **802.1x Security**.
- 8** Press the **802.1X** soft key, and then specify the user name and password.
- 9** Press the **Home** navigation key.

On the main screen, a lock icon indicates whether you are authenticated (indicated by a secured/closed lock) or unauthenticated (an open lock).

## Managing video channels

You can store the addresses for multiple broadcast channels using the video channels function. This function allows you to add, edit, and delete channels, similar to a speed-dial function.

### NOTE:

This function is only available if you have data layer synchronization on either the ADSL or Ethernet interface. This will be fixed in a future release.

### Adding or editing video channels

The following procedure describes how to add or edit video channels.

#### To add or edit video channels

- 1 Press the **Actions** soft key.
- 2 Select **Video Channels**.



- 3 Select **Manage Entries**.
- 4 Select **Add** or **Edit**.
- 5 If you selected **Edit**, choose a channel to edit.

The channel name dialog opens.



- 6 Enter the file name then press **OK**.

The protocol dialog opens.

- 7 Select the protocol type for this connection then press **OK**.

The address dialog opens.

- 8 Enter the address then press **OK**.

The new or edited address appears in the channel list.

## Deleting a video channel

The video channels function allows you to delete a stored channel. The following procedure describes how to delete video channels.

### To delete a channel

- 1 Press the **Actions** soft key.
- 2 Select **Video Channels**.
- 3 Select **Manage Entries**.
- 4 Select **Delete**.
- 5 Select the channel to delete then press **OK**.

The channel is deleted.

---

## Analyzing video streams

The HST-3000 analyzes the video data packet flow at the packet level. Since the initial video quality is established by the source material and encoding process at the head end, and the decoding quality is established by the STB, the effects of the transport and access networks on the video streams are the variables requiring analysis. Actual video content decoding is not performed.

**NOTE:**

The data connection must be established (indicated by a solid green Data LED) for video streams to be visible to the HST and the video statistics screens to show activity.

After the HST-3000 is setup, it can analyze video performance. Up to three streams can be simultaneously analyzed in Terminate mode. In monitor mode, up to 3 simultaneous streams can be analyzed at one time, with statistics available for up to 10 previous streams. In addition, the signaling can be analyzed. To view statistics on another stream, press the **Results** soft key then select the stream.

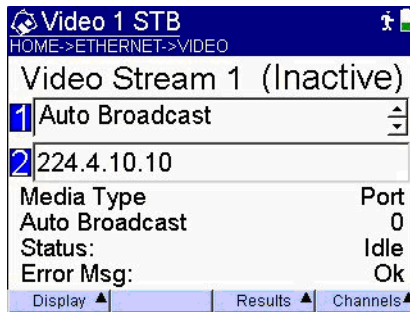
**NOTE:**

The use of the term “MPEG-2” for the service selection type is a general term for what has been called an MPEG-2 video Transport Stream packet as defined in the ISO/IEC 13818 standard. It does not mean or define the compression technology used in the payload of the transport packet. Thus, if the broadcast video flow is using the 13818 packet format, then any compression scheme may be used in the payload with no impact on the HST. For example, if MPEG-4 compression technology was used in the payload instead of MPEG-2, the HST would be able to perform as outlined here in without issue.

**Terminate mode** In the terminate mode, you can emulate a set-top-box and request broadcast programs.

**To perform IP video tests in Terminate mode**

- 1 Press the **Home** navigation key to return to the Summary screen.



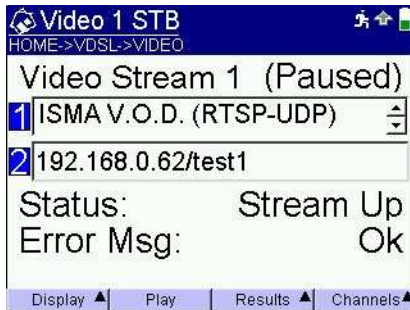
- 2 Enter the service type and address. This can be done two ways:
  - a Enter the channel's info manually.
    - Press **1** then use the arrow keys to select the video service: Auto Broadcast [automatically detects broadcast streams. The first detected stream's media type and port are displayed.], MPEG-2 Broadcast (UDP), MPEG-2 Broadcast (RTP), MPEG-2 V.O.D. (RTSP-UDP), Microsoft IPTV, ISMA Broadcast, ISMA V.O.D.(RTSP-UDP), ISMA V.O.D.(RTSP-TCP), Rolling Stream (R-RTP-UDP).

**NOTE:**

The Auto Broadcast behavior changes depending on the “Analysis Type” on the Video Settings menu. If it is set to “Normal”, the HST can detect MPEG2-TS RTP, MPEG2-TS UDP, and ISMA streams. To auto detect Rolling Stream test streams, it should be set to “UT”. If it is set to “Microsoft”, Microsoft IPTV streams can be detected. However, it is not restricted to only these streams. For example, if you have selected “Microsoft”, it will detect the “Normal” streams as well as the Microsoft IPTV streams.

- Press **2** then use the keypad to enter the IP address.  
After entering the IP address, enter the port number, if prompted. The port number is required for all services except Auto Broadcast. The default 8208 used by the HST-3000 is typically accepted by networks.
  - Press the **OK** key to accept the service and address.
  - b** Retrieve a stored channel’s information.
  - Press the **Actions** soft key then select a channel from the list. (See “[Managing video channels](#)” on page 26.)
- 3** Press the **OK** key to request the program material.  
This initiates the IGMP signaling protocol sequence. The status of the IGMP messaging is shown in the lower portion of the screen. Typically, the status will change from `Idle` to `Media Wait` to `Stream Up`.
- 4** *Optional.* To enable viewing of additional streams, perform the following.
- a** Press the **Results** soft key then select the stream.
  - b** Select the video service and enter the IP address, as in [step 2](#).
  - c** Repeat these steps for additional streams.
- 5** When a RTSP (VOD) stream is active, use the far right soft key to Pause or Play the stream.

- Press **Pause** to pause the video (This sends a pause message, as defined in RFC2326) to temporarily pause the VOD program stream.

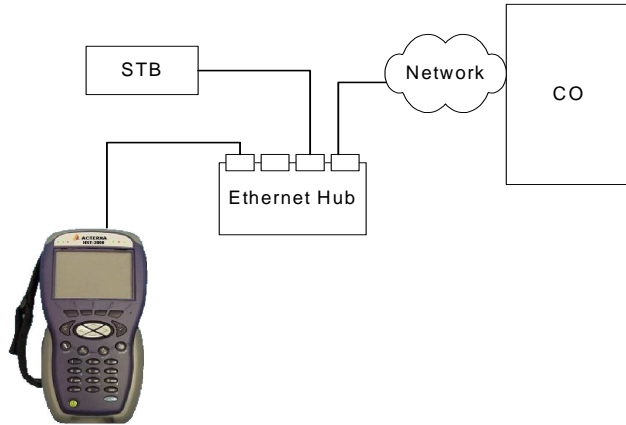


- Pressing **Play** sends the Play message, restarting the VOD program.
- 6** To view different types of statistics, do one of the following.
- Press the **Display** soft key, then select **Video**, then select a category.
  - Press the left or right arrow key to scroll through the screens.
- 7** To clear (or reset) the results, press the **Results** soft key, and then select **Clear Results for Stream**. (or Clear Log if you are viewing the Error Log).

See "[Interpreting Test Results](#)" on page 39 for information on analyzing the results.


**Monitor mode** In the monitor mode, up to 3 simultaneous streams can be analyzed at one time, with statistics available for up to 10 previous streams.

If monitoring on an Ethernet interface, you may need an Ethernet hub (such as a NETGEAR® EN 104) between the CO and the set-top-box, as shown in [Figure 2](#) below.



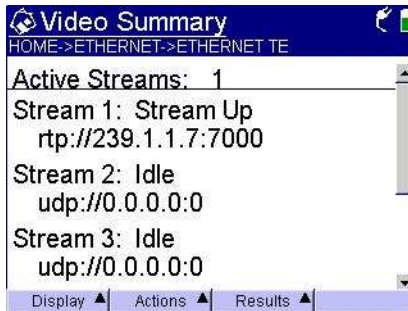
**Figure 2** IP video monitoring with a hub

**To perform IP video tests in Monitor mode**

- 1 If monitoring over a DSL interface, skip to [step 3](#).  
If monitoring over an Ethernet interface, do the following.
  - a Press the **Configure**  navigation key.  
The parameter soft keys appear.
  - b Press the **LAN** soft key.
  - c Enter an IP address.  
An IP address on the network is not required; however, you should enter a valid IP address (any address).
- 2 Verify that the **Data** LED is green.



- 3 Press the **Home** navigation key to return to the Summary screen.



This screen reports the summary data for up to 10 video streams.

- 4 To select a specific stream to analyze, press the **Results** soft key then select the stream.

You can repeat this step for streams 2 and 3, if desired.

- 5 To view different types of statistics, do one of the following.
  - Press the **Display** soft key, then select **Video**, then select a category.
  - Press the left or right arrow key to scroll through the screens.
- 6 To clear (or reset) the results, press the **Results** soft key, and then select **Clear Results for Stream** (or Clear Log if you are viewing the Monitor Log).

See [“Interpreting Test Results” on page 39](#) for information on analyzing the results.

---

## Measuring Class of Service

The development of IP packet based “Triple Play” services places new demands on the network to manage the priority of the services. Each application has its own specific quality of

service requirements, each with varying dynamic bandwidth demands. Many mechanisms exist to deliver the proper QoS for each application, but taken as a whole is called Class of Service (CoS).

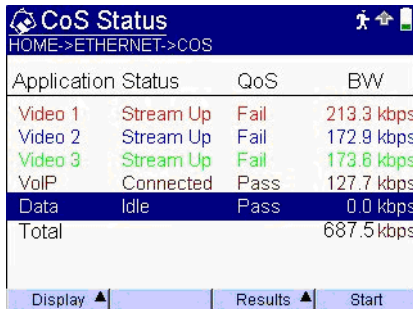
Although CoS mechanisms vary, validation of CoS *performance* is critical. Especially in the access network where bandwidth may be limited, interaction between competing application QoS demands may affect the individual services.

The HST-3000's Class of Service feature allows the testing of all three applications simultaneously and analysis that reveals their interactions. You can view multiple applications and see whether bringing up another application has a negative impact on existing applications. For example, if you add a third video stream and exceed the bandwidth needed for Video and VoIP services, will it degrade the existing streams or will it fail to come up? The goal is to validate that multiple streams can be running and that the network CoS mechanisms are working correctly.

### To measure the Class of Service

- 1 From a main measurements page, select **Class of Service**.

The COS Status screen appears.



The screenshot shows the 'CoS Status' screen with a navigation path 'HOME->ETHERNET->COS'. It contains a table with columns for Application, Status, QoS, and BW. The data rows are: Video 1 (Stream Up, Fail, 213.3 kbps), Video 2 (Stream Up, Fail, 172.9 kbps), Video 3 (Stream Up, Fail, 173.8 kbps), VoIP (Connected, Pass, 127.7 kbps), Data (Idle, Pass, 0.0 kbps), and a Total row (687.5 kbps). At the bottom, there are buttons for 'Display', 'Results', and 'Start'.

Application	Status	QoS	BW
Video 1	Stream Up	Fail	213.3 kbps
Video 2	Stream Up	Fail	172.9 kbps
Video 3	Stream Up	Fail	173.8 kbps
VoIP	Connected	Pass	127.7 kbps
Data	Idle	Pass	0.0 kbps
Total			687.5 kbps

This screen provides an overview of all active applications with Video first, VoIP second, and Data third.

- The **QoS** Pass/Fail comes from the applicable detailed QoS GUI for each item and is a Fail if any one result is in a fail state.
  - **BW** is the current average total bandwidth.
- 2** To view the detail for an application, use the up and down arrows to highlight the item, and then press the **OK** key. The detailed GUI screen for that item appears. For example, highlighting Video 1 will display the video QoS screen for Stream 1.

Press **Cancel** to return to this screen.

- 3** To start an application, press the **Start** soft key.

The soft key will change to Stop.

- 4** To view other result categories, press the **Display** soft key.

If there is any packet loss, the **Packet** screen provides visibility into the possible location.

The **Graph** screen shows the comparison of bandwidths for each application.

The **Analysis** screen provides multi-layer analysis to view correlation. For example, if there is video packet loss or excessive jitter, this would help identify which network segment may be responsible.

The **Config** screen provides summary configuration information for each application. For example, the stream type and address for video, the phone number and IP address for a VoIP call, or the IP address of a data transfer (FTP). This configuration information can be saved, recalled, or deleted.

See [“Class of Service results” on page 58](#) for information on analyzing the results.

## Saving test results

You can save your test results by pressing the **Results** soft key then selecting one of the options.

- **Save Results** saves the results to a text file.  
For more information on saving, retrieving, and managing result files, see the *HST-3000 Base Unit User's Guide*.
- **Timed Results Save** saves the results to a comma-separated-values (CSV) file at specified time intervals. For example, you can set the HST to save results to a file every 10 minutes. This is useful for long term monitoring. The file is saved to the HST's internal file system. (Use **Tools>FileManager** to view.)
- **Timed Results Save with FTP** saves the results to a .xml file at specified time intervals (as above) then transfers the file using FTP.

The following procedure describes how to save test results to a file at specified time intervals and transfer using FTP.

### To save results at specified intervals and transfer using FTP

- 1 Connect the power adapter to the HST.
- 2 Using a straight cable, connect the HST to the same LAN as the PC or laptop:
  - a Connect one end of the cable to the HST's Ethernet port located on the top panel of the unit.
  - b Connect the other end to the network.
- 3 If you haven't already done so, enable transferring of results for long term tests. See [step 10](#) of "[Specifying general video settings](#)" on [page 19](#).
- 4 To specify the FTP settings, do the following:
  - a Press the **System** navigation key.
  - b Press the **INSTRUMENT** soft key.

- c Press the **4** key.  
The FTP Settings menu appears.
  - d Press the **1** key, and then enter the address for the **FTP server**.
  - e Press the **2** key, and then enter the **user name** for the FTP server. The default name is “anonymous.”
  - f Press the **3** key, and then enter the **password** for the FTP server. The default password is “anonymous@jdsu.com.”
- 5 Press **Home** to return to the main Video screen.
  - 6 From any results screen, press the **Results** soft key, and then select **Start Timed Results Saving with FTP**.  
This item will only appear if you have enabled **FTP LTerm Results** on the Video Settings configuration menu (see [step 3](#)). Otherwise, it says “Start Timed Results Saving” (no *with FTP*).
  - 7 Enter a file name for the results files, and then press the **OK** key.
  - 8 Enter the **Save Interval**, in minutes.
  - 9 Pressing **OK** will start the clock for the first interval.  
A results file will be transferred at the interval specified in [step 8](#).  
The file name will be the name you specified, but will include a timestamp at the end of the file name.
  - 10 At the end of your test, press the **Results** soft key again, and then select **Stop Timed Results Saving with FTP**.

For more information on saving, retrieving, and printing results, see the *HST-3000 Base Unit User's Guide*.



# Interpreting Test Results

## 3

This chapter describes the test results that are gathered when running a test. These results allow you to analyze the transport stream. The available test results vary depending on the mode. Topics discussed in this chapter include the following:

- “About test results” on page 40
- “Video Monitor” on page 41
- “Stream QoS results” on page 43
- “RTP results” on page 46
- “Loss Summary results” on page 48
- “Packet statistics” on page 50
- “Stream (TS) statistics” on page 51
- “Stream Rates” on page 53
- “PID Map results” on page 54
- “Video Totals results” on page 55
- “Monitor Log” on page 57
- “Video Error Log results” on page 57
- “Class of Service results” on page 58

---

## About test results

After the HST-3000 is setup and a data connection is established, video streams become available for analysis. The test results used for analysis are split among several categories. To view the different categories of statistics, press the **Display** soft key, then select **Video**. The categories that are available vary depending on the mode. [Table 8](#) lists the categories available per interface.

**Table 8** Result categories per mode

Category	Terminate mode	Monitor mode
STB Emulation	√	
Video Monitor		√
Stream QoS	√	√
RTP Results	√	√
Loss Summary	√	√
Packet Statistics	√	√
Stream Statistics	√	√
Stream Rates	√	√
PID Map	√	√
Video Totals	√	√
Monitor Log		√
Error Log	√	√



## Video Monitor

When in monitor mode, up to 3 simultaneous streams can be analyzed at one time, with statistics available for up to 10 previous streams. The Video Summary page provides the slots which currently carry active streams, the type of stream, the IP address and port number of each stream, and the status of each stream. An example of the Video Monitor result screen is shown in [Figure 3](#).



**Figure 3** Video Monitor results

[Table 9](#) describes the Video Summary results.

**Table 9** Video Monitor results

Result	Description
Active Stream IDs	Reports which slots contain results for media streams that are currently active.

**Table 9** Video Monitor results (Continued)

Result	Description
Each result provides the following four statistics:	
State	Status of the stream <ul style="list-style-type: none"><li>– <b>Stream Up</b> - Active</li><li>– <b>Idle</b> - No active stream</li><li>– <b>Failed</b> - A stream is no longer detected.</li></ul> All streams brought up using RTSP protocol will eventually reach the Failed state. This is because the HST does not detect RTSP termination messages or RTSP messages used for special features such as pause.
Type	The type of media detected: <ul style="list-style-type: none"><li>– <b>udp</b> (for MPEG-2 TS Video over UDP)</li><li>– <b>rtp</b> (MPEG-2 TS Video over RTP)</li></ul>
IP address	The IP address of the stream.
Port	The RTSP port of the stream.

**NOTE:**

The State, Type, IP address, and Port results refer to the media stream, *not* the signaling protocol (IGMP or RTSP) that brought up the stream.

## Stream QoS results

This category provides a summary of the video quality of the selected program flow. An example of the Stream QoS result screen is shown in [Figure 4](#).

	Current	Max	Score	Hist.
PCR Jitter	0ms	0ms	Pass	Pass
RTP Lost	0.00%	0.00%	Pass	Pass
Err. Ind.	NA	NA	NA	NA
Overall:	<b>Pass</b>			
Latency	0ms	NA	Pass	Pass
Leave Lat.	0ms	NA	Pass	Pass

**Figure 4** Stream QoS results

This screen varies depending on the stream type. [Table 10](#) describes the Stream QoS results.

**Table 10** Stream QoS results

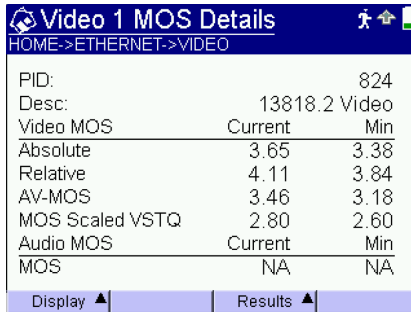
Result	Description
PCR Jitter	MPEG2 Program Clock Reference deviation, in milliseconds.
RTP Jitter	The current jitter, in milliseconds, when analyzing UDP, ISMA, or Rolling Stream video streams.
RTP Lost	Percentage of packets that were lost.
Err. Ind.	Number of MPEG2 bits with the error indicator bit set.
Cont. Err	MPEG2 Continuity Errors or lost packets, in percent.
Overall	A rating (good, fair, poor) of the combination of jitter, latency, and cont.err. (FAIL if any one item is a fail status).

**Table 10** Stream QoS results

Result	Description
Latency	Time to complete a program change, in milliseconds.
Leave Latency	Delay from when a stream is terminated (via an IGMP leave request) and when we receive the last media packet.

Press the **Results** soft key to access more result options:

- View results for a different video stream
- If “MOS Support” is enabled, view the MOS (Mean Opinion Score) results: either details (Figure 5) or degradation factors (Figure 6).



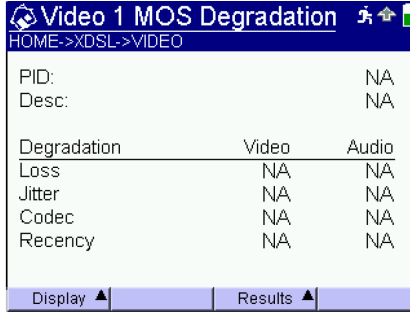
**Figure 5** MOS details results

**Table 11** MOS Details results

Result	Description
PID, Desc.	Provides the PIDs (Packet Identifiers) for each piece (video, audio, and data) of the video program stream, as well as the description of the service.

**Table 11** MOS Details results

Result	Description
Absolute MOS	Mean Opinion Score (MOS) estimation based upon all factors including network impairments, bitrate, codec, and encoder parameters such as interleaving.
Relative MOS	Mean Opinion Score (MOS) estimation based upon the same factors as Absolute MOS with the exception of bitrate and encoder parameters.
AV MOS	An overall MOS score that includes both the video and associated audio stream into consideration. This is only valid if there is an associated audio stream available.
MOS Scaled VSTQ	VSTQ is an R-value like measurement that only takes network impairments into account in its calculations. Its normal range is 0-50, but the statistic is scaled to the MOS (0-5) range for comparison with the other scores.
Audio MOS	MOS estimation based on all factors for the audio stream.



The screenshot shows a window titled "Video 1 MOS Degradation" with a breadcrumb path "HOME->XDSL->VIDEO". It displays a table of results for video and audio components. The table has columns for "Degradation", "Video", and "Audio". The rows include "Loss", "Jitter", "Codec", and "Recency", all with "NA" values. There are also fields for "PID:" and "Desc:" with "NA" values. At the bottom, there are "Display ▲" and "Results ▲" buttons.

Degradation	Video	Audio
Loss	NA	NA
Jitter	NA	NA
Codec	NA	NA
Recency	NA	NA

**Figure 6** MOS degradation factor results

[Table 12](#) describes the MOS Degradation factor results.

**Table 12** MOS Degradation factor results

Result	Description
PID, Desc.	Provides the PIDs (Packet Identifiers) for each piece (video, audio, and data) of the video program stream, as well as the description of the service.
Loss	Amount of degradation due to loss.
Codec	Amount of degradation due to the codec and codec parameters (bitrate, GOP Size, etc.)
Recency	Amount of degradation caused by recent impairments.

## RTP results

The RTP results display RTP loss statistics typically used to measure the transport quality of the stream.

An example of the RTP result screen is shown in [Figure 7](#).

RTP Loss	Config	Curr	Max	Total
Distance Err.	50	NA	NA	NA
Period Err.	5	NA	NA	NA
Min Distance	NA	Max Period		NA
RTP Lost				NA
RTP OOS				NA
RTP Errors				NA

Display ▲      Results ▲

**Figure 7** RTP results

[Table 13](#) describes the RTP results.

**Table 13** Stream QoS results

Result	Description
RTP Loss Config Distance Err.	Not actually a result, just a redisplay of the configured “Loss Distance Threshold” setting.
RTP Loss Cur Distance Err.	“Loss Distance Errors” measured in the current measurement interval, which is 5 minutes.
RTP Loss Max Distance Err.	The maximum of all of the “RTP Loss Current Loss Distance” values, over the lifetime of the stream.
RTP Loss Total Loss Distance Err.	The total of all of the “RTP Loss Current Loss Distance” values, over the lifetime of the stream.
RTP Loss Config Period Err.	Not actually a result, just a redisplay of the configured “Loss Period Threshold” setting.
RTP Loss Cur Period Err.	“Loss Period Errors” measured in the current measurement interval, which is 5 minutes.
RTP Loss Max Period Err.	The maximum of all of the “RTP Loss Current Period Err.” values, over the lifetime of the stream.
RTP Loss Total Period Err.	“Loss Period Errors” measured over the lifetime of the stream.

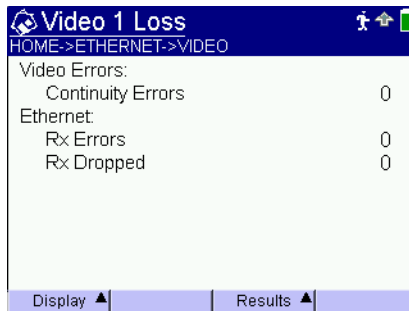
**Table 13** Stream QoS results

Result	Description
Min Distance	The minimum distance between two loss events, measured over the lifetime of the stream.
Max Period	The maximum loss period (i.e. greatest number of consecutive loss packets) measured over the lifetime of the stream.
RTP Lost	Number of RTP packets that were lost.
RTP OOS	RTP OOS Number of RTP packets that were out of sequence.
RTP Errors	RTP Errors Number of RTP packets with errors in the RTP header.

Press the **Results** soft key to view FEC or RUDP results. If using Microsoft as the Analysis Type, RUDP appears, for other Analysis Types, FEC appears. These results provide a percentage of corrected and uncorrected FEC/RUDP errors as well as the FEC/RUDP rate.

## Loss Summary results

This category provides information on lost packets. An example of the Loss Summary screen is shown in [Figure 8](#).



**Figure 8** Loss Summary results



**NOTE:**

This example reflects the Loss Summary when testing on an Ethernet interface. The display will change if testing over the ADSL interface.

Table 14 describes the Loss summary results.

**Table 14** Loss summary results

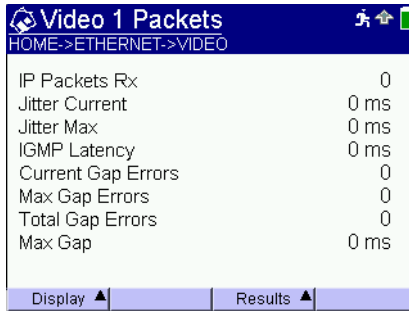
Result	Description
ATM Layer RX CRC Errors	Number of ATM AAL5 frames received which had CRC errors. (Appears only if testing on ADSL interface)
ATM Layer RX AAL5 Length Errors	Number of ATM AAL5 frames received which were too short or too long due to errors. (Appears only if testing on ADSL interface)
ADSL SEF	Number of ADSL severely errored frames. (Appears only if testing on ADSL interface)
ADSL CRC	Number of ADSL CRC errors. (Appears only if testing on ADSL interface)
ETHERNET RX Errors	Number of Ethernet errors received. (Appears only if testing on Ethernet interface)
ETHERNET RX Dropped	Number of dropped Ethernet frames received. (Appears only if testing on Ethernet interface)
VDSL RX Packet Errors	Number of VDSL packet errors received. (Appears only if testing on VDSL interface)
VDSL RX Packet Drops	Number of dropped VDSL frames received. (Appears only if testing on VDSL interface)

**NOTE:**

ATM length errors do not generate CRC errors. ATM AAL5 frames with the wrong length are counted as Length Errors; CRC errors occur when the AAL5 frame is the correct length but is corrupted based on a cyclic redundancy check.

## Packet statistics

This category provides statistics for the packets at the IP layer. An example of the Packet statistics screen is shown in [Figure 9](#).



**Figure 9** Packet statistics results

[Table 14](#) describes the Packet statistics.

**Table 15** Packet statistics

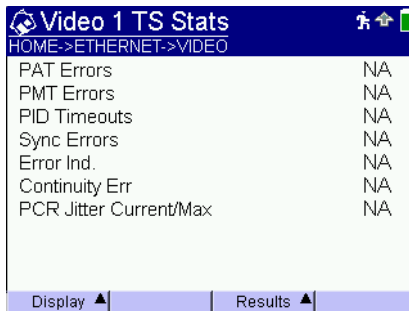
Result	Description
IP Packets Rx	Total number of IP packets received.
Jitter Current	The current jitter value.
Jitter Max	The maximum jitter value.
IGMP Latency	The measure of time to complete a program change. For example, in broadcast video, it is the time between the IGMP join message is sent to the time the first video packet is received.

**Table 15** Packet statistics (Continued)

Result	Description
Current Gap Errors	The current number of gap errors.
Max Gap Errors	The maximum number of gap errors received since the start of the test.
Total Gap Errors	The total number of gap errors received since the start of the test.
Max Gap	The maximum gap received.

## Stream (TS) statistics

This category provides statistics for each test stream (TS) of video. Statistics are kept on up to three streams. An example of the TS statistics screen is shown in [Figure 10](#).



Video 1 TS Stats	
HOME->ETHERNET->VIDEO	
PAT Errors	NA
PMT Errors	NA
PID Timeouts	NA
Sync Errors	NA
Error Ind.	NA
Continuity Err	NA
PCR Jitter Current/Max	NA

Display ▲      Results ▲

**Figure 10** TS statistics results

Table 16 describes the TS statistics.

**Table 16** Stream statistics

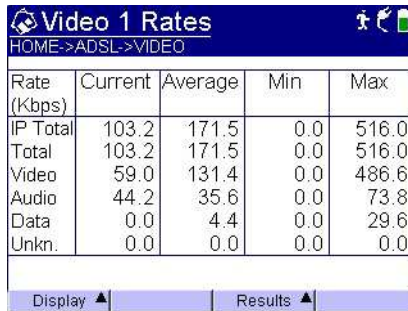
<b>Result</b>	<b>Description</b>
PAT Errors	Number of errors in the Program Association Table. Error conditions include any of the following: <ul style="list-style-type: none"><li>– scrambling is ON</li><li>– repetition rate is less than the configured threshold value</li><li>– PAT not found</li></ul>
PMT Errors	Number of errors in the Program Map Table. Error conditions include any of the following: <ul style="list-style-type: none"><li>– scrambling is ON</li><li>– repetition rate is less than the configured threshold value</li><li>– PMT not found</li></ul>
PID Timeouts	Number of occurrences when the PID for Video or Audio is not present for more than the configured threshold value.
Sync Errors	Number of MPEG2 synchronization errors.
Error Ind.	Number of MPEG2-TS packets with the error indicator bit set.
Continuity Err	Number of MPEG continuity errors detected.
PCR Jitter Current/Max	Current and maximum values for jitter of the MPEG2 program clock reference.

**NOTE:**

The Error Indicator is set by the video stream encoder when it detects corrupted source content. Typically any count will result in an anomaly on the TV.

## Stream Rates

This category provides individual bit rates for each portion of the video stream. An example of the Stream rates screen is shown in [Figure 11](#).



Rate (Kbps)	Current	Average	Min	Max
IP Total	103.2	171.5	0.0	516.0
Total	103.2	171.5	0.0	516.0
Video	59.0	131.4	0.0	486.6
Audio	44.2	35.6	0.0	73.8
Data	0.0	4.4	0.0	29.6
Unkn.	0.0	0.0	0.0	0.0

Display ▲      Results ▲

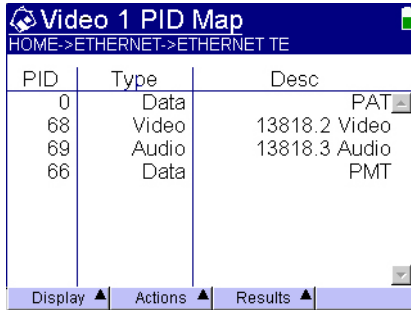
**Figure 11** Stream rates results

The “IP Total” statistics measure the bandwidth used by the video stream, including the UDP and IP headers.

## PID Map results

This category provides the PIDs (Packet Identifiers) for each piece (video, audio, and data) of the video program stream. Statistics are kept on up to three streams.

An example of the PID map results screen is shown in [Figure 12](#).



The screenshot shows a window titled "Video 1 PID Map" with a breadcrumb path "HOME->ETHERNET->ETHERNET TE". It contains a table with the following data:

PID	Type	Desc
0	Data	PAT
68	Video	13818.2 Video
69	Audio	13818.3 Audio
66	Data	PMT

At the bottom of the window, there are three buttons: "Display ▲", "Actions ▲", and "Results ▲".

**Figure 12** PID Map results

**NOTE:**

The PAT and PMT items are table data inserted into the stream to enable the decoder to perform correctly. These two items should always be present.

## Video Totals results

This category reports the total number of active video streams and provides the combined total data rate associated with the ATM Video Virtual Channel selected when configuring the ADSL interface or the Ethernet port used in the Ethernet mode. The screen provides a quick summary of the total data rates for all of the video program flows present on the interface under test.

An example of the Video Totals results screen is shown in [Figure 13](#). This screen changes depending on the Analysis Type (in this example, Microsoft Analysis Type is used).

Video Totals			
HOME->ETHERNET->VIDEO			
Active Streams	2		
Video Rates (kbps)	Curr	Max	
Combined	7175.2	13126.1	
MSTV ICC	0.0	13126.1	
MSTV Latency (ms)	Curr	Avg	Max
RUDP Latency	9	13	48
Join Latency	0	5	9
ICC Media Latency	8	9	10
Status Latency	9	5	9
MSTV Request Timeouts	0		
Display ▲	Results ▲		

**Figure 13** Video Totals results

The total video bandwidth (“Combined Video Rate”) peaks can be important in analyzing total bandwidth available. The total bandwidth is found on the DSL Summary screen. The difference in the two numbers is the bandwidth available for either Internet data or Internet data and VoIP data.

[Table 17](#) describes the Video Totals.

**Table 17** Video Totals

Result	Description
Combined Video Rates	Total video bandwidth

**Table 17** Video Totals (Continued)

<b>Result</b>	<b>Description</b>
MSTV ICC Video Rate	Bandwidth used only for ICC media packets (appears only when using Microsoft Analysis Type)
RUDP Latency	Displays the number of received RUDP unicast retry media packets (appears only when using Microsoft Analysis Type).
Join Latency	Time to complete a program change, in milliseconds. The time between the join message being sent to the time the first video packet is received.
ICC Media Latency	Time, in milliseconds, of a MSTV ICC request to the first unicast media packet of the video stream.
Status Latency	Time, in milliseconds, of a MSTV command message to its appropriate response, including ICC request and status.
MSTV Request Timeouts	The number of occurrences where a timeout was reached while waiting for a transmitted frame to return.



## Monitor Log

The Video Monitor Log displays a list of the IGMP and RTSP signaling activity. An example of the Video Monitor Log screen is shown in [Figure 14](#).



Figure 14 Video Monitor Log

## Video Error Log results

The Video Error Log category reports any state change for each of the QoS parameters (for example, delay change from fail to pass). An example of the Video Error Log result screen is shown in [Figure 15](#).



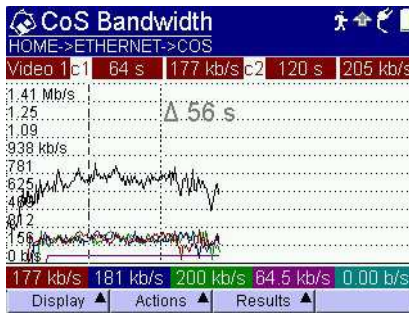
Figure 15 Video Error Log results

## Class of Service results

When measuring class of service, the following results are available:

- Graph
- Status
- Analysis
- Packet
- Config

**Graphs** This category provides individual graphs for each bandwidth and a comparison of bandwidths. [Figure 16](#) is an example of the comparison of all bandwidths.



**Figure 16** CoS graph of bandwidths

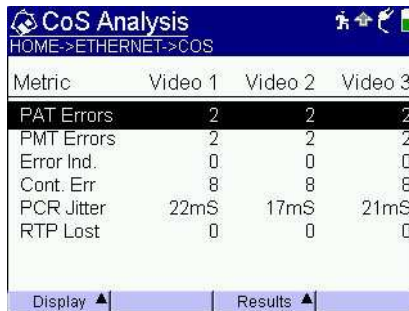
The labels are color coordinated with the stream colors. They identify the graph data type (Total, Video1, etc.) and elapsed time from the start of a stream, in seconds. The graph can show about 320 seconds of data (on a first-in-first-out basis), and then it saves the graph. The graph is saved in the CoS/Graphs directory, which you can view using the File manager (in the System>Tools menu).

There are two cursors (selected using the **Actions** soft key) which can be used to determine time intervals, shown in [Table 16](#) with the delta symbol. The **Actions** soft key also allows zoom in and zoom out.

Use the up and down keys to move among the graphs.

**Status** This category provides summary status information for each application, such as whether a stream is up or Qos analysis passed or failed.

**Analysis** The Analysis screen provides multi-layer analysis to view correlation. For example, if there is video packet loss or excessive jitter, this would help identify which network segment may be responsible. See [Figure 17](#).



The screenshot shows the 'CoS Analysis' screen with a table of metrics for three video streams. The table has columns for 'Metric', 'Video 1', 'Video 2', and 'Video 3'. The metrics listed are PAT Errors, PMT Errors, Error Ind., Cont. Err, PCR Jitter, and RTP Lost. The values for each metric are: PAT Errors (2, 2, 2), PMT Errors (2, 2, 2), Error Ind. (0, 0, 0), Cont. Err (8, 8, 8), PCR Jitter (22mS, 17mS, 21mS), and RTP Lost (0, 0, 0). The screen also shows navigation options like 'Display' and 'Results' at the bottom.

Metric	Video 1	Video 2	Video 3
PAT Errors	2	2	2
PMT Errors	2	2	2
Error Ind.	0	0	0
Cont. Err	8	8	8
PCR Jitter	22mS	17mS	21mS
RTP Lost	0	0	0

**Figure 17** CoS Analysis screen

When two or three similar (SD to SD or HD to HD) video broadcast streams are up with QoS data present, compare PCR jitter. If a stream shows a PCR jitter value of 10% or more above the other stream or streams, there is a content issue.

Any Error Indicator count indicates a content issue.

Any PMT or PAT error condition due to scrambling “on” is a content issue.

Repetition rates for PSI table data presence and continuity error data are analyzed. A content error occurs if continuity error rates are below 0.1%, and repetition rates are greater than threshold settings.

Continuity error rates above 0.1% indicate a network issue.

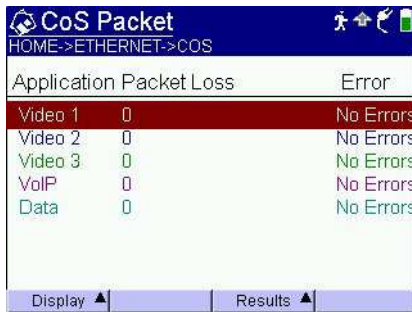
IP packet jitter above the threshold settings indicate a network issue.

IP packet loss above threshold settings indicate a network issue.

Packet loss and physical layer stats on the test interface are analyzed. If physical layer errors are present when MPEG-TS packet losses are present, the Packet loss line will report a physical error.

Physical layer stats are all those available on a given interface such as un-correctable block errors for ADSL.

**Packet** If there is any packet loss, this screen provides visibility into the possible location, as shown in [Figure 18](#).



Application Packet Loss		Error
Video 1	0	No Errors
Video 2	0	No Errors
Video 3	0	No Errors
VoIP	0	No Errors
Data	0	No Errors

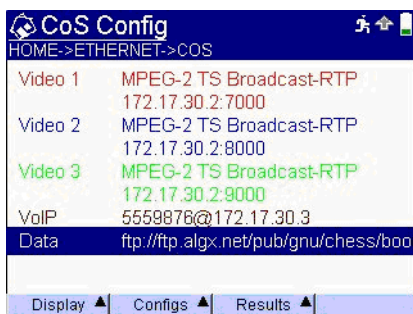
**Figure 18** CoS Packet statistics

The Error column reports the first error condition from the application's "Error" screen, for example, CRC errors on a VDSL interface.

While there are QoS items of various types, the focus of this screen is on the interaction of the packet flows, indicated by the packet loss detail comparison.

Fail is an indication of any detected packet loss at the applicable layer. Pass is no packet loss at the applicable layer.

**Config** This category provides summary configuration information for each application. For example, the stream type and address for video, the phone number and IP address for a VoIP call, or the IP address of a data transfer (FTP). See [Figure 19](#).



**Figure 19** Cos Config screen

This configuration information can be saved, recalled, or deleted. With an application highlighted, press the OK key to move to the setup configuration screen for that application. You can make changes and then press Cancel to move back to this screen.

The key summary data shown displays the configuration that would change most often once the basic applications are individually configured.



# Technology and methodology

## A

This appendix describes the basics of IP video technology, measuring the quality of service, and methodologies of testing. Topics discussed in this appendix include the following:

- [“About IP video technology” on page 64](#)
- [“Service Testing and Troubleshooting methodology” on page 71](#)

## About IP video technology

Next generation, standards-based networks, using distributed network architecture and packet transport mechanisms are making possible the cost effective delivery of so called “triple play” services: data, voice, and video. These new networks, however, must also deliver specific CoS (Class of Service) support for these three service classes, each with application specific QoS (Quality of Service) needs. IP video (packet based video delivery) places unique demands on these networks.

Today's data service-based networks do meet specific performance levels generally based upon loss packet parameters. Typical data applications compensate for lost packet events through a retransmission of lost data. Thus, at the application level, error free performance can be achieved. However, packetized voice services (VoIP) are placing more stringent requirements on the networks. New CoS mechanisms are beginning to achieve acceptable levels of performance.

For example, packet loss rates of up to 4% of the flow and packet jitter approaching 40 msec can be tolerated and still deliver toll quality voice. But, broadcast video services can not tolerate more than 0.1% packet loss nor more than 5-10 msec packet jitter. In actual practice, voice codecs can hide lost data more effectively than lost video can be masked. When data and voice flows are mixed with video flows which have much greater bandwidth requirements, network planning and engineering become even more challenging. In addition, new signaling protocol flows, IGMP for broadcast video and RTSP for VOD services, greatly expand the complexity. Also, the delivery of the required CoS becomes very complex and demanding based on the dynamic nature of these flows. This is due to viewing habits, channel changing loads, and dynamic VOD media requests.

While networks are rising to the challenge, measurement of the accumulated effects of the network on critical application specific QoS parameters must be made at the premise during



service installation to validate proper service delivery. Gathering and recording this QoS data is also key to rapid trouble resolution if fault conditions arise at a later date. The quality of the source material or video content and the quality of the video decoder in the STB (Set Top Box) determine the “possible” quality. The network is the variable in between and can only detract from the design quality. Thus, the focus of the recommended test concept is to measure network specific variables. These variables are content quality and network quality.

**Content Quality** Obviously the quality of the content is the starting point. Decisions made in the video head end where content is acquired determine what quality is possible. What content sources are used, what compression algorithms will be implemented, what encoders will be employed, and what source quality monitoring present, establish the initial quality. The data output of the encoders start the video packet flow. There are two critical source quality parameters which can be seen in the video flows at the premise and/or in the last mile access network: PCR (Program Clock Reference) jitter and the video transport packet Error Indicator bit status.

Figure 20 describes the transport stream header detail, including the PCR and error indicator bit.

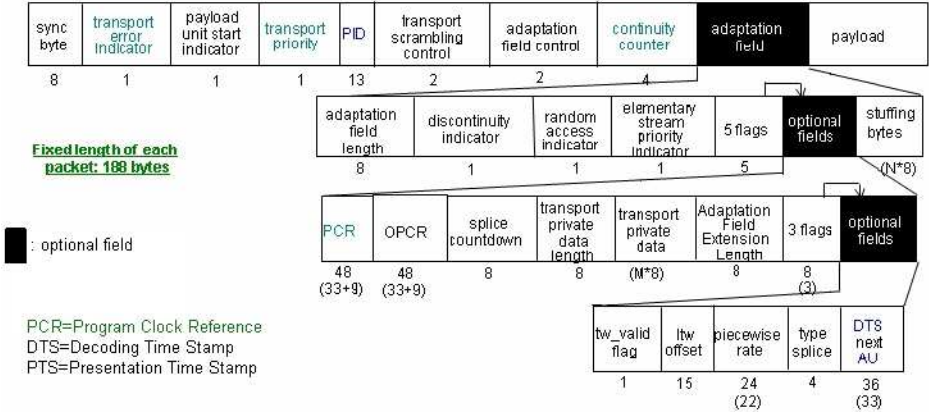


Figure 20 Transport Stream Packet Header Detail

**PCR Jitter** In each program material data flow, the video encoder embeds a synchronization signal which is used by the video decoders to synchronize to the encoded data stream. Thus, there are two timing parameters embedded within each audio and video program. These timing parameters (called Decode Time Stamps and Presentation Time Stamps) are used to decode the video content and present the decoded video to the display unit (television, etc.). If excessive PCR jitter is present, the decoder cannot synchronize itself correctly to the data stream with the end result being visual impairments such as, pixelization, frame freezes, loss of color, etc. will be seen. What amount of PCR jitter is excessive is not a constant but rather determined by various parameters including the input buffer sizes of the decoder and STB design. In today's typical packet video networks, however, PCR jitter should be less than 10 msec and preferably less than 5 msec depending on decoder/STB designs.

PCR jitter can be caused by several things, but most likely are: 1) overall network packet jitter, 2) transcoding problems in the encoder, or 3) local ad insertion issues (that is, issues related to insertion of advertisements). If packet jitter is not excessive when PCR jitter is present, then the cause is specific to the particular program flow. In this case an encoder may not be performing up to specifications. If this is so, PCR jitter will be constantly excessive. If, however, it is not constant, then a momentary problem from inserting local programming may be suspected.

**Transport Error Indicator** The transport error indicator is a bit set by the encoders in any video packet transmitted where the encoders detects corrupted source content. The presence of packets with this indication is strictly an issue with the content quality and not due to the performance of the distribution network. Monitoring video encoder's output streams in the head end can detect this condition providing an early opportunity for problem resolution. Error Indicator counts seen at the premise reveal a source quality problem.

**Network Quality** Network performance is the other determinant of video quality of a variable nature. This can be distilled down to a few specific parameters: 1) packet loss, 2) packet jitter, and 3) IGMP latency. Each of these items can be analyzed at the premise or in the last mile access network.

**Packet Loss** Packet loss is measured by analyzing the video packet flows and determining the presence of a continuity error event. Standards define the process, but since each video packet carries a sequence number, continuity errors can definitely be determined. For example, since a MPEG-2 transport packet is 188 bytes in length, an IP frame will carry within it 7 such MPEG-2 Transport packets. Thus, losing 1 IP frame will result in losing 7 MPEG-2 Transport packets. Conversely, if the MPEG-2 Continuity Counter jumped by 7 between 2 consecutive MPEG-2 packets, one can observe with a fair amount of

certainty that there was a loss of an IP frame. Missing packets, out of sequence packets, and duplicate packets are all counted as errors. Each of these events can cause decoding errors. Depending upon the temporal or spatial components contained in the frames within a MPEG-2 Transport packet; a single packet error event, may or may not be seen on the TV. However, the actual network performance is measured by the packet loss parameters regardless of whether or not the decoder can or cannot hide the problem.

**Packet Jitter** If the overall packet flow experiences excess jitter, due to congestion problems and resulting CoS mechanism performance issues, this jitter can directly causes PCR jitter. If it is excessive enough it could cause decode buffers to run out resulting in gaps in decoder output. Gaps may appear as freeze frame or pixelization events seen on the TV.

**IGMP Latency** IGMP (Internet Group Management Protocol) is the signaling protocol used to access broadcast video services which use a one-to-many (multicast) network design managing network bandwidth efficiently. The use of this signaling protocol enables each STB to obtain only the programming that the viewer is interested in watching conserving bandwidth in the access network. In this implementation a message (a join message) is sent from the STB to the network asking the network to send the requested program (channel) to the STB by joining a multi-cast group carrying the desired broadcast channel. The time from sending the join message until the first video packet is received by the STB is referred to as the IGMP latency. Thus, IGMP latency is a measure of both service provisioning, i.e., broadcast video is available, and network response performance.

These messages travel upstream into the network to the first device that can add (join) the requestor to an existing broadcast channel flow. This parameter measures the network performance, but not the end user experience for the channel changing time. The IGMP latency plus the time it takes to fill

the decode buffer and to decode and display the content is the total user experience time. However, the buffer fill time and decode time are functions of the network architecture and are not variables. Thus, the measurement of the variable network performance piece, i.e. IGMP latency, is the critical parameter for measuring actual network performance.

Figure 21 outlines an example IGMP message flow when a broadcast program, channel 2, is requested, and then a channel change to another program, channel 3, is requested.

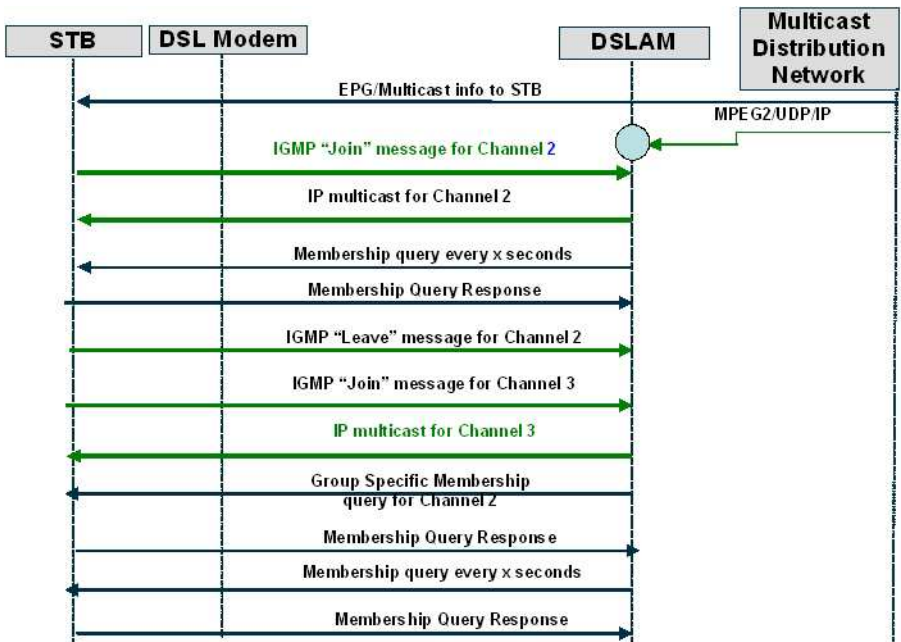


Figure 21 IGMP Message Flows

The DSLAM in this example has access to the requested programs. It is performing a Snooping function, looking at the requested program material and if it is directly available at the DSLAM, the join is performed. If the requested program was not available at the DSLAM, the IGMP messages would continue up-stream to a location, a Video Hub Office possibly,

where the material was available. The “join” would be performed there and the program routed to the DSLAM and on to the STB.

**Summary** Network Quality parameters (Packet loss, Packet jitter, IGMP latency) and Content Quality parameters (PCR jitter and Error indicator) measure the critical variables in the delivery of broadcast video services.

In the case of narrowcast services (i.e. services tailored for a specific viewer), such as VOD, IGMP latency does not apply since RTSP (Real Time Streaming Protocol) protocol is used. But, more importantly the request for access to a stored program does not carry the same latency expectations. If the actual request involves the completion of a payment transaction, then latency becomes even less critical and the network can easily meet expectations for initial access to the desired program.

Therefore, a simple definition of video QoS parameters for evaluating network performance includes the following:

- for Broadcast video service performance
  - PCR jitter - level
  - IGMP latency - level
  - Continuity error - rate
  - Error indicator - count
- for VOD service
  - PCR jitter - level
  - Continuity error - rate
  - Error indicator - count

However, looking at a single program flow may not reveal the whole picture so to speak as it relates to actual service. Since some impairments are source specific and some are network performance specific, it is important to make these measure-

ments on more than one stream at a time. Thorough testing requires simultaneous analysis of at least two streams and preferably three if access network bandwidth allows.

---

## Service Testing and Troubleshooting methodology

As mentioned above, individual program flows should be analyzed to ensure that both content quality and network performance parameters are within desired network specifications. The suggested thresholds are listed below:

Packet loss = less than or equal to 0.1%

Packet jitter = less than or equal to 5 msec\*

PCR jitter = less than or equal to 5 msec\*

Error indicator = zero count

IGMP latency = less than or equal to 200 msec

\*Specific STB/decoder designs may be able to tolerate higher levels of jitter based on larger buffer designs. Less than or equal to 10 msec may be acceptable.

Five to ten msec is a conservative PCR jitter level. As network designs and STBs increase buffer sizes, the acceptable level will rise. The acceptable level for a particular network is a company-specific issue.

When these measurements are made simultaneously on more than one channel, then content problems can be easily separated from distribution network problems, a critical determination for problem resolution.

**Packet loss** Packet loss (continuity error) problems are typically seen on all channels/programs coming to the premise because they are not source or content related. If packet loss is present, analysis of the physical layer at the xDSL interface or Ethernet interface will aid in sectionalization. If no physical layer errors

are present, then packet loss is most likely being caused by the distribution network not from the access network. Congestion is most likely at issue.

Looking further into the temporal component can help pinpoint the issue. The answers to the following questions can help find the problem area(s). Are packets being lost during known peak traffic times during the day? Are they coming in bursts with intervals with no loss? Are they random single or small packet loss events?

Bursts of loss might be more symptomatic of buffer overflows related to heavy traffic. Random single or small events might be more related to noise hits on the access network impacting packet flows. DSL loop performance in the access network may be pushing the bandwidth limits when signal to noise margins are low and the addition of a second or third channel flow reaches 100% capacity of the loop. The copper may be poorly balanced allowing high impulse noise to impact the data flows. In-home wiring may be introducing noise which also can damage data flows.

**PCR jitter** PCR jitter problems may be due to content quality problems as outlined previously or overall network packet jitter. By evaluating more than one channel/program at a time, this can be determined. If excessive PCR jitter is present at more than one channel, network jitter is most likely at fault. If excessive PCR jitter is present on only one channel, then a source problem as described above is normally the cause.

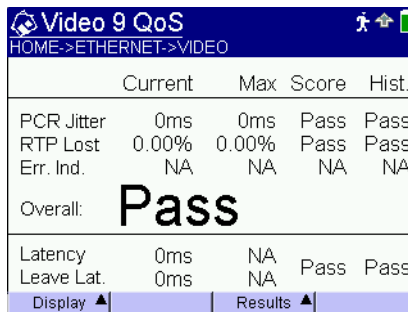
**Error indicator** Error Indicator analysis will further reveal content problems. Since the indicator can only be set by the encoder, it specifically reveals content only problems. Typically this would affect only one program or channel. However, if a multiple program feed in the head end is experiencing problems, more than one program/channel could be affected. Analyzing a channel from another source, or different feed would be instructive.



**IGMP latency** IGMP latency measures the network's performance. Typically, IGMP latency would be similar for multiple channels. However, if network topology and management place access to certain program material farther back in the network, then differences could be experienced. If such a hierarchical approach is used, then differences might be detected based upon which programs are accessible deeper in the network. Testing multiple channels/programs to exercise this network design would be useful.

**Summary** In summary, analysis of whether or not poor video QoS performance is seen on more than one channel or not when troubles are reported will start the resolution process effectively. Simultaneous analysis of the key QoS parameters mentioned on multiple video flows will further refine the analysis and lead to efficient and effective trouble resolution.

**Practical example** Two parameters are shown in [Figure 22](#): PCR Jitter and Latency (IGMP Latency = channel changing time not including Decoder buffer file and decode times). These parameters summarize the video quality of the selected program flow.

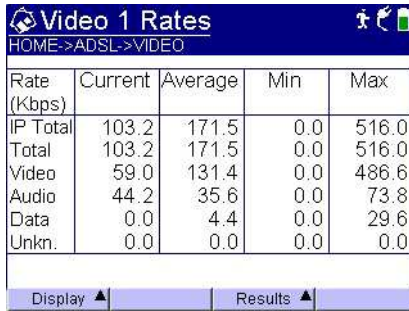


Video 9 QoS				
HOME->ETHERNET->VIDEO				
	Current	Max	Score	Hist.
PCR Jitter	0ms	0ms	Pass	Pass
RTP Lost	0.00%	0.00%	Pass	Pass
Err. Ind.	NA	NA	NA	NA
Overall:	<b>Pass</b>			
Latency	0ms	NA	Pass	Pass
Leave Lat.	0ms	NA	Pass	Pass
Display ▲	Results ▲			

**Figure 22** Stream QoS results

Additional data can be obtained by analyzing the stream in more detail.

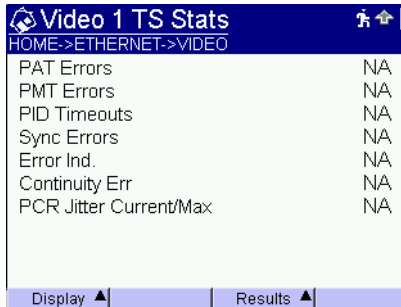
Since each stream includes a video, audio, and data (program table data, etc.) portion, packet stats can be obtained for each, as shown in [Figure 23](#).



Rate (Kbps)	Current	Average	Min	Max
IP Total	103.2	171.5	0.0	516.0
Total	103.2	171.5	0.0	516.0
Video	59.0	131.4	0.0	486.6
Audio	44.2	35.6	0.0	73.8
Data	0.0	4.4	0.0	29.6
Unkn.	0.0	0.0	0.0	0.0

**Figure 23** Stream rates

More importantly, the Error Indicator count will reveal a content problem. [Figure 24](#) shows the stream statistics.



PAT Errors	NA
PMT Errors	NA
PID Timeouts	NA
Sync Errors	NA
Error Ind.	NA
Continuity Err	NA
PCR Jitter Current/Max	NA

**Figure 24** Stream statistics results

The video may show poor quality with only the Error Indicator count showing a problem. Any count is bad.

# Glossary

---

## A

**Alias** — An alternate method of addressing the endpoint. Alias addresses include private telephone numbers, public E.164 numbers, numeric strings representing names, e-mail like addresses, etc. Alias addresses are unique within a zone.

**ATM** — Asynchronous Transfer Mode.

---

## B

**BTV** — Broadcast TV

---

## C

**CPE** — Customer Premises Equipment

---

## D

**Delay** — How long, usually in milliseconds, it takes data to move from source to destination. Total delay can be broken down into encoding, packetization, network transmission, and buffering sub-categories.

**DHCP** — Dynamic Host Control Protocol.

**DNS** — Domain Name Server.

**DSLAM** — Digital Subscriber Line Access Multiplexer

---

## E

**Ethernet** — One of the most common local area network (LAN) technologies. It operates over a variety of physical media and various speeds. Most

commonly used are 10/100 Base-T, 10 Mbps, and 100 Mbps over twisted pair cable.

---

## G

**GK** — Gatekeeper. A network device that provides two-way, real-time connections between endpoints.

**GSQ** — Group Specific Query. An IGMP message asking the host if it wants to join a particular multicast channel.

**GW** — Gateway. A network device that provides address translation and network access for endpoints, gateways, and MCUs. Optionally, it may also provide bandwidth control and network topology information.

---

## I

**ICMP** — Internet Control Message Protocol. The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

**IGMP** — Internet Group Management Protocol

**Internet Protocol (IP)** — The network layer protocol for the Internet protocol suite.

**IP Address** — The 32-bit (IP version 4) address assigned to hosts that want to participate in a TCP/IP Internet.

**IP video** — Technology used to transmit video streams over a data network using the internet protocol.

**ISMA** — Internet Streaming Media Alliance

---

## J

**Jitter** — The variance in packet arrival times at an endpoint.

---

## L

**LAN** — Local Area Network. A limited distance (typically under a few kilometers or a couple of miles) high-speed network (typically 4 to 100 Mbps) that supports many computers.

**LED** — Light Emitting Diode. The lights indicating status or activity on electronic equipment.

**Loss** — The dip in signal level between two points on a network.

---

## M

**MAC** — Media Access Control

**MOS** — Mean Opinion Score

---

**N**

**Netmask** — Network mask. Used to determine if an IP address is on your subnetwork.

---

**P**

**Ping** — Packet Internet Groper. An IP datagram message that is sent using the ICMP in order to obtain information from the far end (Destination) regarding the status of the networks ability to deliver a message. Think of ping as sonar on a network. IP packets (ICMP “echo” requests) are sent to the destination (target), which automatically responds. Ping tells you if the destination is alive and awake, how fast the ping went to the destination and back, and if ping packets were dropped and lost along the way.

---

**R**

**RTP** — Real Time Protocol.

**RTSP** — Real Time Streaming Protocol.

**Route** — The path that network traffic takes from its source to its destination. The route a data-

gram may follow can include many gateways and many physical networks.

---

**S**

**STB** — Set top box

**STUN** — Simple Transversal of UDP (User Datagram Protocol) Through NATs (Network Address Translators). As defined by *The Internet Society*: A protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the public Internet Protocol (IP) addresses allocated to them by the NAT. STUN works with many existing NATs, and does not require any special behavior from them. As a result, it allows a wide variety of applications to work through existing NAT infrastructure.

---

**T**

**Throughput** — The actual amount of useful and non-redundant information which is transmitted or processed.

**Trace route** — The capability to evaluate the hops taken from one end of a link to the other on a TCP/IP network.

---

**U**

**UDP** — User Datagram Protocol. A connectionless protocol with very limited error recovery capabilities.

---

**V**

**VC** — Virtual Channel

**VCI** — Virtual Channel Identifier

**VLAN** — Virtual LAN

**VOD** — Video On Demand

**VPI** — Virtual Path Identifier

# Index

---

## Numerics

802.1x security settings [13](#)

---

## A

Adding video channels [26](#)  
Analyzing the transport stream [28](#)  
Assumptions [x](#)  
Auto Broadcast [30](#)

---

## C

Capabilities [2](#)  
Compliance information [xi](#)  
Connections [5](#)  
Conventions [xiii](#)

---

## D

Delay, defined [75](#)  
Deleting a video channel [27](#)  
Detecting streams automatically [30](#)

---

## Documentation

base unit user's guide [xi](#)  
IP Video testing user's guide [xi](#)

---

## E

Editing video channels [26](#)  
Emulating an STB [8–27](#)  
Error log [57](#)  
Ethernet  
connector [5](#)  
defined [75](#)

---

## F

Features [2, 8](#)

---

## H

Headset connector [5](#)

---

## I

IP address, defined [76](#)

---

**L**

Loss summary [44](#), [48](#)

---

**M**

Managing test configurations

Managing video channels [26–27](#)

---

**P**

Packet statistics [50](#)

PID map [54](#)

---

**Q**

QoS thresholds, setting [19](#), [21](#), [23](#)

Quick tour [3](#)

---

**R**

Results

Error log [57](#)

Loss Summary [44](#), [48](#)

Packet statistics [50](#)

PID map [54](#)

saving [36–37](#)

Stream QoS [43](#), [57](#)

Stream rates [53](#)

Stream statistics [51](#), [74](#)

Video totals [55](#)

---

**S**

Safety information [xi](#)

Saving results at specified intervals  
[36–37](#)

Saving test results [36–37](#)

Security, 802.1x settings [13](#)

Setup

test settings [8–18](#)

video [19–24](#)

Status LEDs [3](#)

Stream QoS [43](#), [57](#)

Stream rates [53](#)

Support, technical assistance [xii](#)

---

**T**

Technical assistance [xii](#)

Terminology [x](#)

Test parameters, setting [8](#)

Testing

emulating an STB [8–27](#)

Timed results save with FTP [36–37](#)

TS Stats [51](#), [74](#)

---

**U**

USB connector [5](#)

User documentation

base unit user's guide [xi](#)

IP Video testing user's guide [xi](#)

---

**V**

Video channels, managing [26](#)

adding [26](#)

deleting [27](#)

editing [26](#)

Video results

Error log [57](#)

Loss Summary [44](#), [48](#)

Packet statistics [50](#)

PID map [54](#)

Stream QoS [43](#), [57](#)

Stream rates [53](#)

Stream statistics [51](#), [74](#)

Video totals [55](#)

Video settings [19](#), [21](#), [23](#)

Virtual channel indicator [11](#), [12](#), [13](#)

Virtual path indicator [11](#), [12](#), [13](#)





**Communications Test and Measurement Regional Sales**

**North America**

Toll Free: 1 855 ASK JDSU  
Tel: +1 240 404 2999  
Fax: +1 240 404 2195

**Latin America**

Tel: +55 11 5503 3800  
Fax: +55 11 5505 1598

**Asia Pacific**

Tel: +852 2892 0990  
Fax: +852 2892 0770

**EMEA**

Tel: +49 7121 86 2222  
Fax: +49 7121 86 1222

[www.jdsu.com](http://www.jdsu.com)

21109345-005  
Revision 000, 08/2012  
English

