NETSCOUT

OneTouch™ AT 10G
Network Assistant

User Manual

Released 01/2018 for Software Release v6.5.1

LEGAL NOTIFICATION

Use of this product is subject to the End User License Agreement available at **http://www.netscout.com/legal/terms-and-conditions/** or which accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NETSCOUT SYSTEMS, INC., and the purchaser of this product ("Agreement").

Government Use and Notice of Restricted Rights: In U.S. government ("Government") contracts or subcontracts, Customer will provide that the Products and Documentation, including any technical data (collectively "Materials"), sold or delivered pursuant to this Agreement for Government use are commercial as defined in Federal Acquisition Regulation ("FAR") 2.101and any supplement and further are provided with RESTRICTED RIGHTS. All Materials were fully developed at private expense. Use, duplication, release, modification, transfer, or disclosure ("Use") of the Materials is restricted by the terms of this Agreement and further restricted in accordance with FAR 52.227-14 for civilian Government agency purposes and 252.227-7015 of the Defense Federal Acquisition Regulations Supplement ("DFARS") for military Government agency purposes, or the similar acquisition regulations of other applicable Government organizations, as applicable and amended. The Use of Materials is restricted by the terms of this Agreement, and, in accordance with DFARS Section 227.7202 and FAR Section 12.212, is further restricted in accordance with the terms of NETSCOUT's commercial End User License Agreement. All other Use is prohibited, except as described herein.

This Product may contain third-party technology. NETSCOUT may license such third-party technology and documentation ("Third-Party Materials") for use with the Product only. In the event the Product contains Third-Party Materials, or in the event you have the option to use the Product in conjunction with Third-Party Materials (as identified by NETSCOUT in the applicable Documentation), then such third-party materials are provided or accessible subject to the applicable third-party terms and conditions contained in the "Read Me" or "About" file located on the Application CD for this Product. To the extent the Product includes Third-Party Materials licensed to NETSCOUT by third parties, those third parties are third-party beneficiaries of, and may enforce, the applicable provisions of such third-party terms and conditions.

Open-Source Software Acknowledgment: This product may incorporate open-source components that are governed by the GNU General Public License ("GPL") or licenses that are compatible with the GPL license ("GPL Compatible License"). In accordance with the terms of the GNU GPL, NETSCOUT will make available a complete, machine-readable copy of the source code components of this product covered by the GPL or applicable GPL Compatible License, if any, upon receipt of a written request. Please identify the product and send a request to:

NetScout Systems, Inc.
GNU GPL Source Code Request
310 Littleton Road
Westford, MA 01886
Attn: Legal Department

NETSCOUT SYSTEMS, INC. reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.

Contents

Chapter 1: Get Acquainted

Chapter 2: Setup Wizard

Chapter 3: Basic Operation

Chapter 4: Network Infrastructure Tests

Chapter 5: User Tests

Chapter 6: Profiles

Chapter 7: Wired Analysis

Chapter 8: Tools

Chapter 10: Managing Files

Chapter 11: Maintenance

Chapter 12: Link-Live Cloud Service

Chapter 13: Specifications

List of Figures

Chapter 1: Get Acquainted

Overview of Features

The OneTouch™ AT 10G Network Assistant is a rugged, easy to use, handheld network analyzer. The OneTouch analyzer can be used to:

- Test network connectivity and performance
- Diagnose problems that impact network access and performance
- Troubleshoot problems when performing network move/change/add tasks
- Test up to 10G in the network data center
- Use NETSCOUT cloud endpoints to test network performance

The OneTouch AT 10G analyzer answers questions such as:

- Can I connect to the network?
- Are the ports on my 10G switch working?
- Are basic services such as DHCP and DNS operational?
- Can I access the Internet from the network?
- Are my email and FTP servers working?
- What is the performance of my web servers/services, email, and other application-layer functionality?
- What is the performance of my network infrastructure?

The analyzer features:

- User-configurable tests
- User-configurable Profiles
- Complete L1/L2 measurements across copper/RJ45 Ethernet media
- Network services measurements
- USB Type A port
- Wired Performance tests using a Peer or Reflector
- Built-in 10/100M management port and optional Wi-Fi management port (using a Wi-Fi USB adapter)
- Ethernet packet capture

The analyzer features a Setup Wizard that guides you through configuring the analyzer for testing. See “Setup Wizard” on page 45.

Safety Information

Table 1 shows the international electrical symbols used on the analyzer or in this manual.

Table 1. Symbols

	Warning or Caution: Risk of damage or destruction to equipment or software. See explanations in the manuals.
	Warning: Risk of fire, electric shock, or personal injury.
	Warning: Class 1 laser when an SFP module is installed. Risk of eye damage from hazardous radiation.
	Do not put products containing circuit boards into the garbage. Dispose of circuit boards in accordance with local regulations.

Warning

To prevent possible fire, electric shock, or personal injury:

- **Remove the batteries if the Product is not used for an extended period of time, or if stored in temperatures above 50 °C. If the batteries are not removed, battery leakage can damage the Product.**
- **The battery door must be closed and locked before you operate the Product.**
- **Repair the Product before use if the battery leaks.**
- **Replace the batteries when the low battery indicator shows to prevent incorrect measurements.**
- **Turn off the Product and disconnect all cables before you replace the battery.**
- **Be sure that the battery polarity is correct to prevent battery leakage.**
- **Do not disassemble or crush battery cells and battery packs.**

- **Do not put battery cells and battery packs near heat or fire.**
- **Do not put in sunlight.**
- **Do not continuously charge battery packs when not in use.**
- **Do not expose battery pack to mechanical shock.**
- **Do not open the battery pack. There are no user serviceable parts inside.**
- **Refer to the Product manual for proper instructions on charging the battery pack.**
- **Do not operate the Product with covers removed or the case open. Hazardous voltage exposure is possible.**
- **Remove the input signals before you clean the Product.**
- **Have an approved technician repair the Product.**
- **Do not put metal objects into connectors.**
- **Do not short the battery terminals together.**
- **For Products with rechargeable batteries, use only AC adapters approved by NETSCOUT for use with the Product to supply power to the Product and charge the battery.**

⚠ Warning: Class 1 and Class 2 Laser Products

To Prevent eye damage and personal injury:

- **Do not look directly into optical connectors. Some optical equipment emits invisible radiation that can cause permanent damage to your eyes.**
- **Do not look into the laser. Do not point laser directly at persons or animals or indirectly off reflective surfaces.**
- **When you inspect fiber endfaces, use only magnification devices that have the correct filters.**

- **Use the Product only as specified or hazardous laser radiation exposure can occur.**

⚠ Caution

- **To prevent damage to the Product, accessories, or cables under test and to prevent data loss, read all safety information given in all documentation supplied with the Product.**
- **Do not connect the Product to a telephone line or ISDN line.**
- **Use the correct cables and connectors when connecting the Product to a network.**
- **Do not block or restrict the Product's air intake or exhaust ports.**

Contact NETSCOUT

For more contact information, go to our website.

http://enterprise.netscout.com

customercare@netscout.com

Toll free: +1-844-833-3713
International: 978-320-2150

Additional Resources

For OneTouch analyzer product information and accessories, see **http://enterprise.netscout.com**.

For help in Link-Live Cloud Service, go to **https://app.link-live.com/support**.

AC Adapter and Battery

You can use the AC adapter or the included lithium ion battery to supply power to the analyzer. The AC adapter recharges the battery.

Charge the Battery

Before you use the battery for the first time, charge the battery for about 2 hours with the analyzer turned off.

A fully-charged battery operates for approximately 4 hours of typical use. The battery typically takes approximately 4 hours to recharge from 10% to 90% when the analyzer is turned off.

Notes

You do not need to fully discharge the battery before you recharge it.

The battery will not charge if its temperature is outside the range of 32°F to 104°F (0°C to 40°C).

Switch the Power On

To turn on the analyzer, press the green power key ⏻. The key will illuminate and in a few seconds the HOME screen will appear.

Set the Language

1. On the **HOME** screen, tap the **TOOLS** icon (located in the lower-left corner of the screen).
2. Scroll down to the Maintenance Tools section and tap **Language**.
3. Select a language from the list.
4. Press the HOME key to return to the HOME screen.

Check the Battery Status

The battery status icon is located in the upper-left corner of the screen. The battery status icon is normally green. It turns red when the battery's charge drops below 20%. If the battery is not installed in the analyzer, the icon is red.

When the AC adapter is connected to the analyzer, the AC Power Indicator LED (see Figure 4) is red while the battery is charging; green when fully charged. If the battery's temperature is too high

or too low to permit charging, the AC Power Indicator turns yellow.

To see more information about the battery status, tap the Tools icon  , then scroll down and tap the **Battery Status** button.

Extend Battery Operating Time

The display backlight consumes power. Decreasing the display brightness will increase battery operating time.

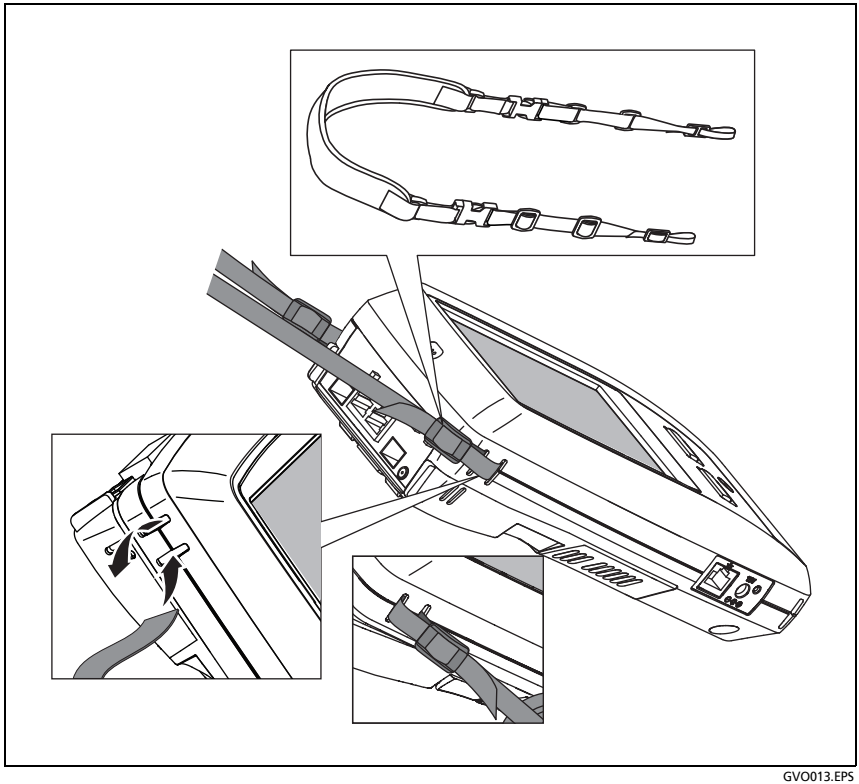
You can make the backlight shut off after a period of inactivity. You can also make the analyzer power down after a period of inactivity. See "Timeout Periods (Power-Down and Backlight)" on **page 39**.

Extend the Life of the Battery

- Recharge the battery frequently. Do not let the battery discharge completely.
- Do not keep the battery at temperatures below -20°C (-4°F) or above +50°C (+122°F) for periods longer than one week.
- Before you put a battery into storage, charge it to approximately 50% of full charge.

Install and Use the Strap

You can install the strap on any two of the four attachment points on the analyzer.



GVO013.EPS

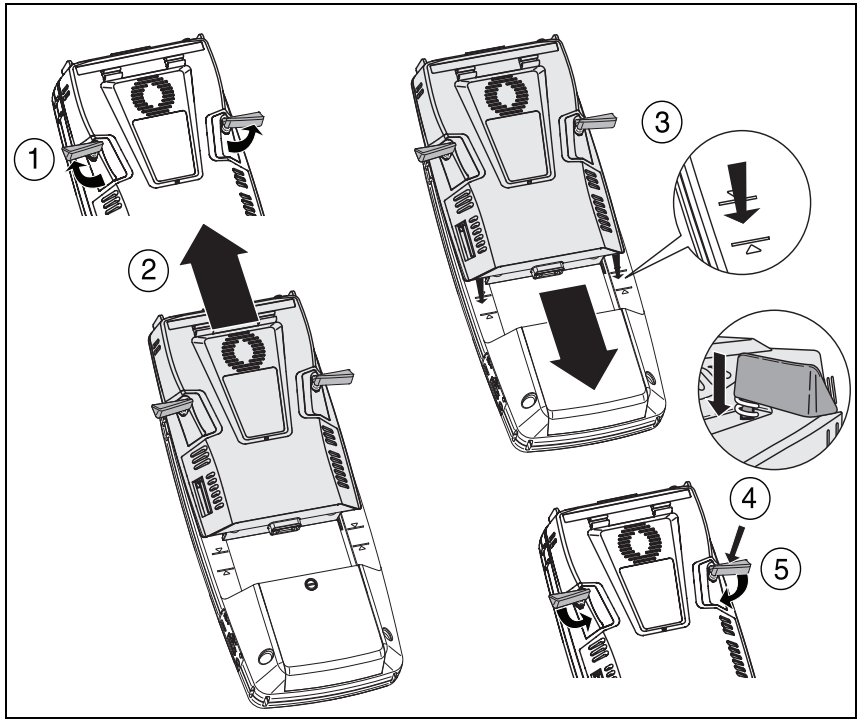
Figure 1. Install and Use the Hang Strap

OneTouch Platform

The OneTouch platform is a handheld computer and display platform that accepts modules like the OneTouch AT 10G module. The modules attach to the system as shown.

Remove and Install a Module

Switch off the analyzer's power before removing the module.



GVO004.EPS

Figure 2. Remove and Install a Module

Connectors, Keys, and LEDs

This section describes the external characteristics of the OneTouch AT 10G hardware platform.

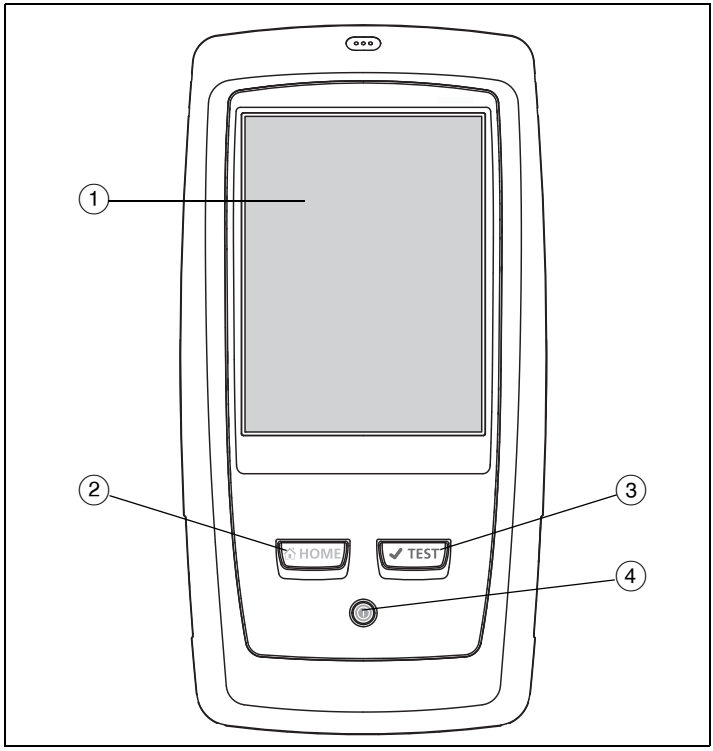


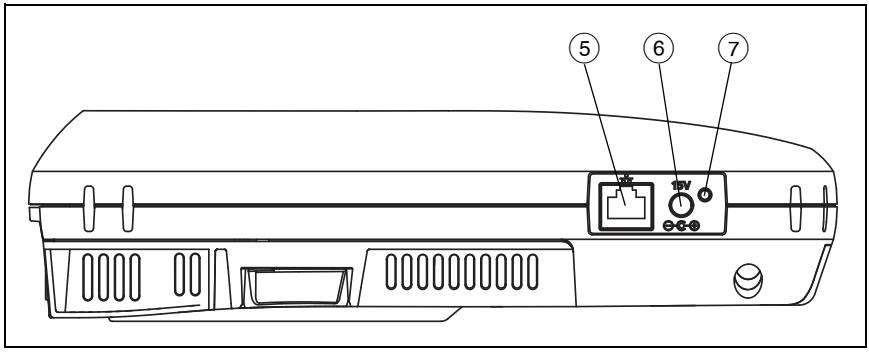
Figure 3. Features of the Main Unit

① **LCD display with touch-screen** - To change the brightness, tap **Tools→Display**. See also: "Touchscreen" on **page 33**.

② HOME - Press this key to go to the Home screen. See "The HOME Screen" on **page 29**.

③ **AutoTest key** TEST - The analyzer is silent on the network until you run AutoTest. AutoTest initiates link, infrastructure test, and user test activity. This key performs the same function as the AutoTest button TEST that appears on the display.

④ **Power Key** - The Power Key illuminates when you switch the power on. Press it again to switch the power off. See also: "AC Adapter and Battery" on **page 17**.



GVO006.EPS

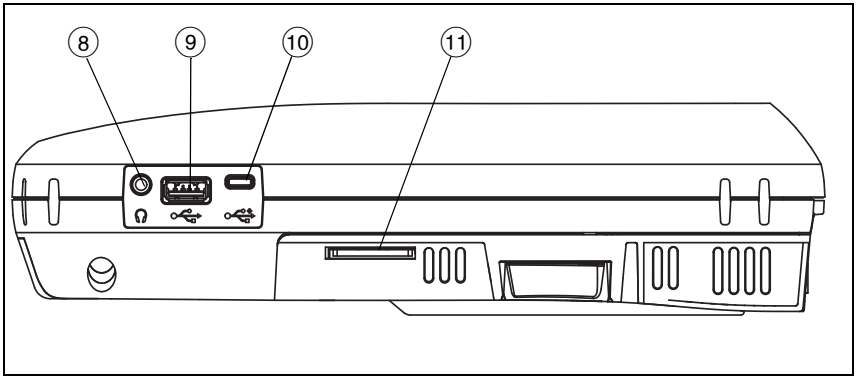
Figure 4. Left Side View

⑤ **Management Port** - Connect to the analyzer via this 10/100M RJ-45 Ethernet Port for:

- Remote control of the analyzer
- Copying files to or from the analyzer
- Browsing the web from the analyzer
- SSH or telnet to switches, etc. from the analyzer

⑥ **Power Connector** - Connect the supplied AC adapter to a power source and to the OneTouch analyzer. See “AC Adapter and Battery” on **page 17**.

⑦ **AC Power Indicator** - This LED is red while the battery is charging; green when fully charged.



GVO007.EPS

Figure 5. Right Side View

⑧ **Headphone Jack** - You can connect headphones to hear audio indicators when they occur.

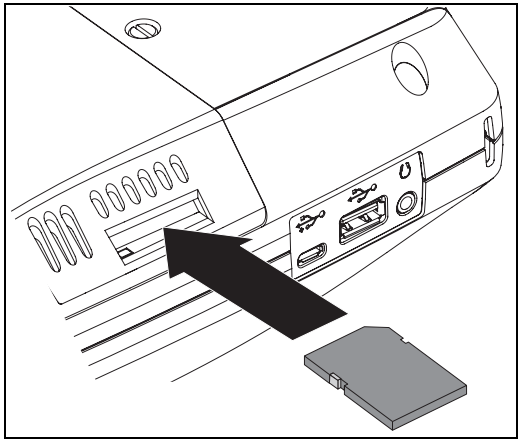
⑨ **USB-A Connector** - Used to manage files on a USB storage device such as a flash drive. See Chapter 10: "Managing Files," beginning on **page 229**. Also used to connect to a USB Wi-Fi adapter which provides a Wi-Fi management port. See “Management Port” on **page 211**.

Many USB flash drives have an LED on the front. Note that the USB flash drive is inserted into the OneTouch analyzer with the back of the flash drive facing the front of the analyzer.

You do not need to software-eject a USB storage device before removing it. Wait for the analyzer to stop writing to the device, then physically remove it. USB keyboard operation is supported on the port; mouse operation is not.

⑩ **Micro-USB Connector** - This connector is reserved for future use.

⑪ **SD Card Slot** - This is for inserting an SD card. You can manage files on an SD card. See Chapter 10: "Managing Files," beginning on **page 229**.



GVO015.EPS

Figure 6. Insert the SD Card

You do not need to software-eject the SD card before removing it. Wait for the analyzer to stop writing to the card. Then gently push the card in until a soft click is heard. Release the card and remove it.

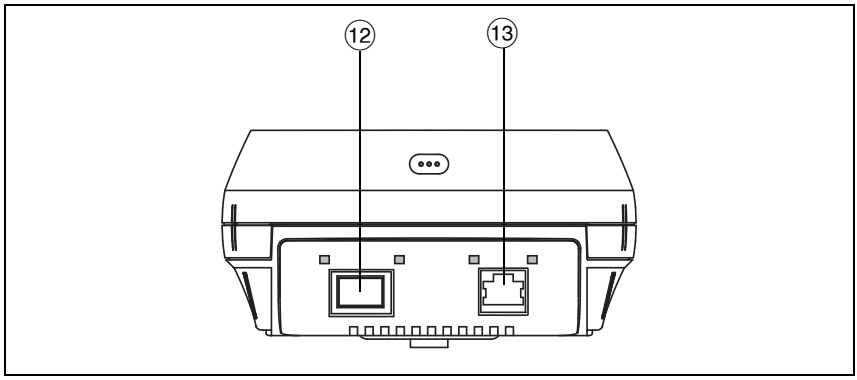


Figure 7. Top End View - Connectors

⑫ **Fiber Port** (SFP / SFP+ receptacle)

⑬ **Wired Ethernet Port** (RJ-45 connector)

The OneTouch AT 10G analyzer has two ports used for network testing:

- 10/100/1000M RJ-45 Ethernet connector (for copper connection)
- 1000M and 10G standard SFP+ socket (for fiber connection)

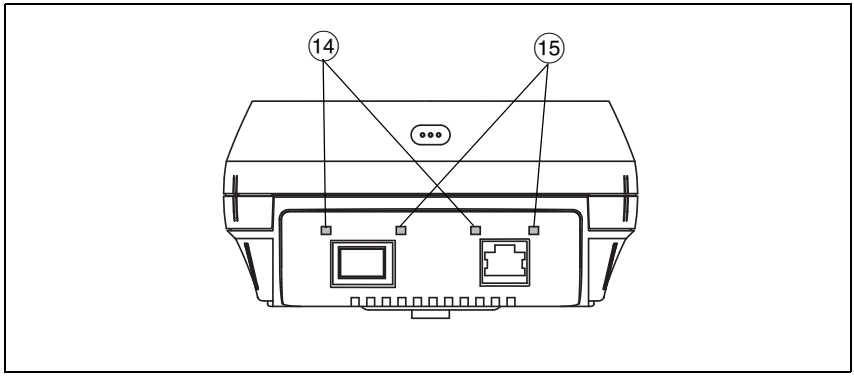
To connect to a network using a copper cable, make a connection to the RJ-45 port.

To connect to a network using optical fiber, insert the appropriate SFP+ adapter into the analyzer's SFP+ port. Then make a fiber connection from the network to the SFP+ adapter. The OneTouch analyzer supports 100BASE-FX and 1000BASE-X SFP+ adapters.

The analyzer links when you tap the AutoTest button ✔TEST or press the AutoTest ✔TEST key.

If the analyzer is connected to the network using both the Ethernet and fiber ports, the analyzer will use the fiber port.

The management port and each network test ports have two LEDs: “Link” and “Activity.”



GVO008.EPS

Figure 8. Top End View - LEDs

⑭ **ACT -** Activity LEDs

⑮ **Link -** Link LEDs

Table 2. Link LED

LED State	Meaning
Off	The port is not linked.
Green	Link is established on the port.

Table 3. Activity LED

LED State	Meaning
Off	No activity.
Flashing Green	Receive or transmit activity.

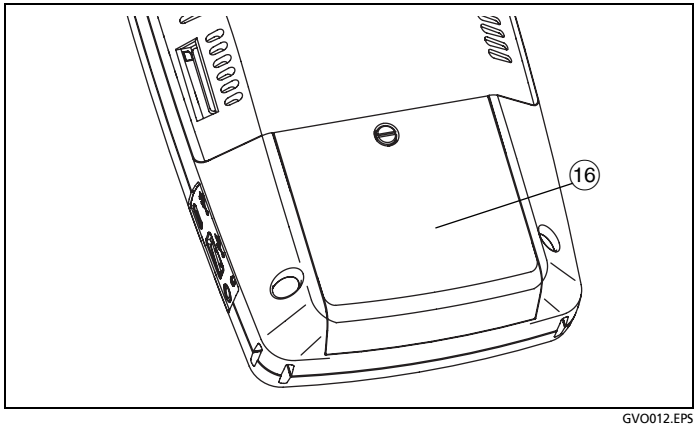


Figure 9. Battery Compartment

⑯ Battery Compartment - The battery pack can be replaced. See "Remove and Install the Battery" on **page 242**.

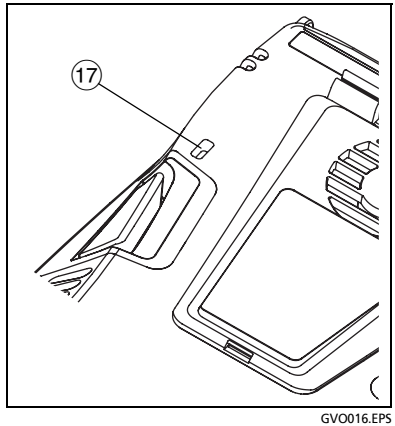


Figure 10. Kensington Security Slot

⑰ Kensington Security Slot - You can attach a Kensington security cable to physically secure the analyzer. The Kensington security slot is on the back of the analyzer.

The HOME Screen

Press the HOME key to display the Home screen.

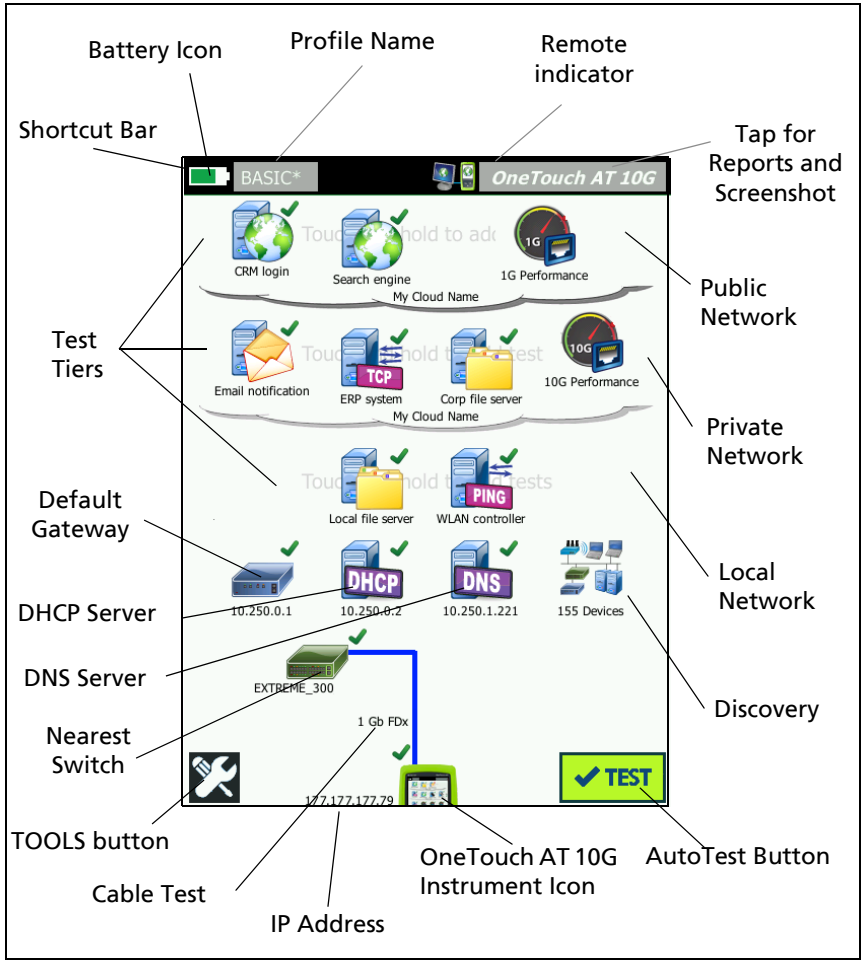


Figure 11. The OneTouch AT 10G Home Screen

Shortcut Bar

① **Shortcut Bar:** The shortcut bar's background is black until AutoTest completes. When AutoTest completes the shortcut bar's background turns green if all tests pass, or red if any test fails.

Test warnings (indicated by a warning icon ⚠ next to a test's icon on the HOME screen) do not affect the pass/fail status of AutoTest.

② **Battery Status Indicator:** Shows the battery's approximate charge. The indicator is green when the battery's charge is 20% or more. The indicator turns red when the battery's charge falls below 20%. When the indicator turns red, connect the AC adapter to avoid running out of power.

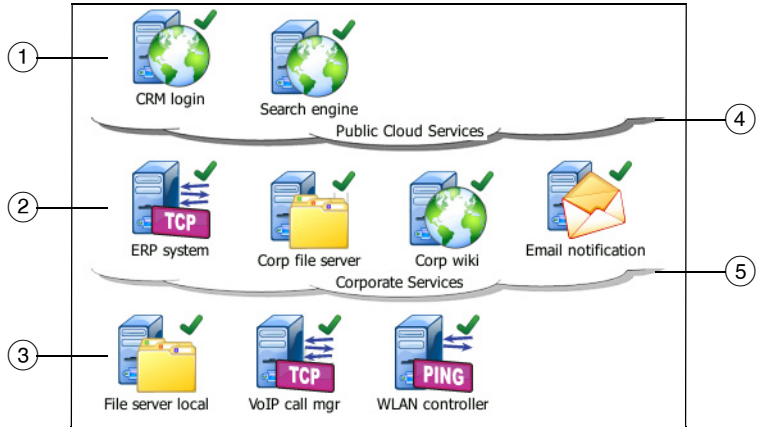
To see more information about the battery status, tap the Tools icon, then scroll down and tap the Battery Status button. See also: "AC Adapter and Battery" on **page 17**.

③ **Profile Button:** A Profile contains OneTouch analyzer setup and test information. An asterisk (*) appears after the profile name if changes have been made but have not been saved to the named profile.

④ **Remote Connection Indicator**: This icon appears when a remote connection to the OneTouch analyzer is established.

⑤ **OneTouch AT 10G Button:** Tap the OneTouch AT 10G button to open a menu that lets you capture a screen (take a screen shot), create a report, or save an AutoTest capture file. For more information, see "Screens" on **page 210**, "Reports" on **page 205**, and "To Save an AutoTest Capture" on **page 227**.

Test Tiers



You can use the three test tiers to organize your tests any way you like.

① **Public Network Tier:** This tier is generally used for tests of servers that are in the public network (for example, the internet).

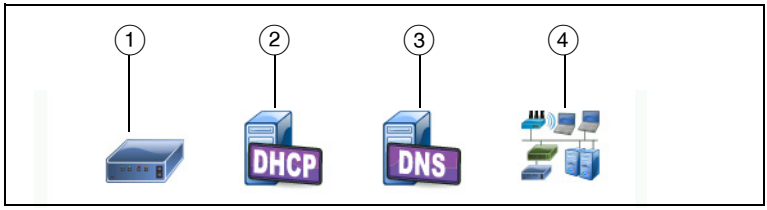
② **Private Network Tier:** This tier is generally used for tests of servers that are in the private network (for example, a corporate intranet).

③ **Local Network Tier:** This tier is generally used for tests of servers that are in the local network (for example, the premise).

④ **Public/Internet Network:** Touch the cloud to rename it. See page 58.

⑤ **Private/Intranet Network:** Touch the cloud to rename it. See page 58.

Network Services Tier



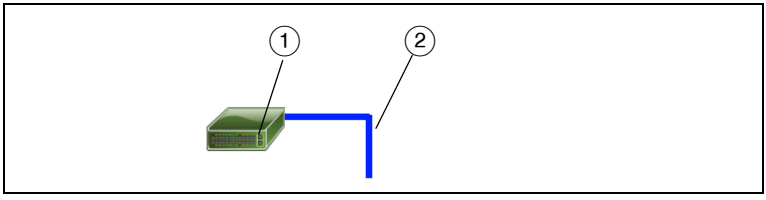
① **Default Gateway:** This shows the default gateway for the wired connection. Tap the icon for details of this router. If a problem is detected, a red X appears on the icon. See page 74.

② **DHCP Server:** Tap the icon to show details of the DHCP test. If the service is unavailable, a red X appears on the icon. See page 77.

③ **DNS Server:** Tap the icon to show details of the DNS test. If the service is unavailable, a red X appears on the icon. See page 79.

④ **Discovered Networks and Devices:** The total number of discovered devices is displayed beneath this icon. Tap the icon to display the WIRED ANALYSIS screen. For more information see “Wired Analysis” on page 157.

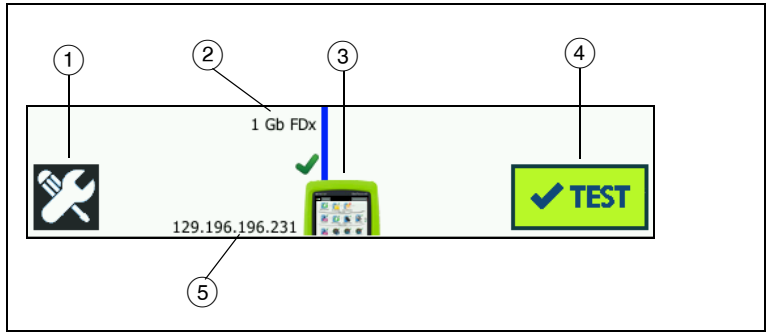
Network Access Tier



① **Nearest Switch:** Tap the icon to show details of the nearest switch. If a problem is detected, a red X appears on the icon. See page 70.

② **Cable:** Tap the link icon to view cable information. See “Cable Test” on **page 66** and “Nearest Switch Test” on **page 70** for more information.

Instrument Tier



① **TOOLS button:** Tap this button to enter the TOOLS menu. See Chapter 8: "Tools," beginning on **page 183**.

② **Cable:** Tap the text to view cable and link test results. See "Cable Test" on **page 66** and "Nearest Switch Test" on **page 70** for more information.

③ **OneTouch Icon:** Tap the icon to view a detailed list of wired transmit and receive statistics, along with address information. Note that the analyzer's wired IP addresses are shown to the left and right of the icon.

④ **AutoTest Button:** Tap the button to run all configured tests. The analyzer does not link and does not perform any infrastructure tests or user tests until you tap the AutoTest button (or press the AutoTest key ✔TEST).

⑤ **Wired IP Address:** This is the IP address of the Ethernet NUT (Network Under Test) port.

Touchscreen

⚠ Caution

For correct operation and to prevent damage to the touchscreen, touch the screen only with your fingers. Do not touch the screen with sharp objects.

You can use these gestures on the touchscreen:

- Tap: To select an item on the screen, tap the item lightly.
- Flick: To scroll a screen, touch the screen then move your fingertip in the direction you want the screen to move.
- Touch and Hold: To add a new test to a test tier, touch white space between the tests on the HOME screen and hold your finger in place. A menu will appear.

To move, copy, or delete a test, touch the test and hold your finger in place. Choices will appear.

To clean the touchscreen, turn off the analyzer, then use a soft, lint-free cloth that is damp with alcohol or a mild detergent solution.

Entering Text

When you tap a panel to enter text, a keyboard is displayed on the bottom half of the screen (see Figure 12).

- To enter characters, tap the characters on the keyboard.
- To enter one upper-case letter, tap **SHIFT**, then tap the letter. The keyboard goes back to lower-case mode after you enter one character. Note: Accented letters are not available as upper-case letters.
- To enter multiple upper-case letters, tap **SHIFT** twice. The shift key turns white when the keyboard is in upper-case mode. To enter lower-case characters, tap **SHIFT** again.
- To delete characters, tap **BACK**.

- To enter accented characters, tap the **çñßà** key (at the lower-left corner of the keyboard), then tap the letters on the keyboard. To enter non-accented characters, tap **çñßà** again.

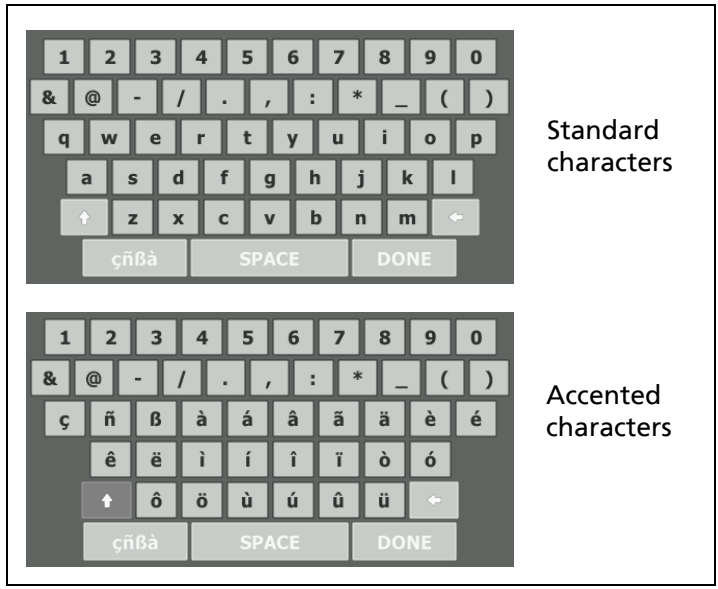


Figure 12. Keyboards for Text Entry

Entering Passwords and Other Hidden Text

When entering passwords, SNMP v1/v2 community strings, or SNMP v3 credentials, the characters are shown as dots.

To show characters in plain text as you type them:

1. Clear all of the characters in the text box. The lock and unlock icons will appear.
2. Select the unlock icon.

3 Enter the characters

When you have entered the characters and tapped the **DONE** button, the characters can no longer be viewed as plain text. The characters appear as a series of dots.

URL Keyboard

When entering a URL, the keyboard includes buttons for adding “www.” to the beginning, or “.com,” “.net,” or “.org” to the end. See Figure 13.

Figure 13. Keyboard for URL Entry

IPv4 Address Entry Keyboard

When entering an IPv4 address, the keyboard includes buttons for entering common number combinations, and disallows entry of alphabetic characters. See Figure 14.

Figure 14. Keyboard for IPv4 Address Entry

IPv6 Address Entry Keyboard

When entering an IPv6 address, the keyboard is customized with buttons for common number combinations, the colon separator, and hexadecimal digits. An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons. Leading

zeros can be omitted. Groups of consecutive zeros can be replaced by a double colon (::).

Figure 15. Keyboard for IPv6 Address Entry

Set Preferences

Typically, you will set the following preferences once, and you will not need to set them again.

Language

See “Set the Language” on **page 18.**

Date/Time

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the Maintenance Tools section and tap **Date/Time.**

3 Tap the setting you want to change:

- To set the date, tap **Date**. Tap <left arrow> or <right arrow> to select a month and year for the calendar, then select the correct date on the calendar. Tap **DONE** to save your settings.
- To set the time, tap **Time**. Tap <up arrow> or <down arrow> to increase or decrease the setting for hours, minutes, and seconds. Tap **DONE** to save your settings.
- To set the date format, tap **Date Format**, then select a format for the day (**DD**), month (**MM**), and year (**YYYY**). Note that the date format used in file naming of reports, screen shots, packet captures, etc. is based on the language setting. See "Language" on **page 38.**
- To set the time format, tap **12 hr** or **24 hr** to use a 12-hour clock or a 24-hour clock.

Note

If you remove the battery and do not connect the AC adapter, the clock keeps the current date and time for a minimum of 24 hours.

Number Format

The analyzer can show decimal fractions with a decimal point (0.00) or a comma (0,00).

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the Maintenance Tools section and tap **0.0** or **0,0** on the **Number** button.

Units for Length Measurements

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the Maintenance Tools section and tap **ft** for feet or **m** for meters on the **Length** button.

Timeout Periods (Power-Down and Backlight)

To increase battery operating time, the analyzer can turn off the backlight and/or automatically power down when you do not press any keys for a specified period.

These settings only apply when the analyzer is operating on battery power.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section, and tap **Timeout Period**.

3 Tap **Backlight** or **Power Down**.

4 Select a time. To always keep the backlight or analyzer on, tap **Disabled**.

Chapter 2: Setup Wizard

Warning

Before you use the analyzer, read the safety information that starts on page 15.

This chapter helps you quickly begin using the OneTouch analyzer.

Setup Wizard

The Setup Wizard, which appears when you initially power on the OneTouch AT analyzer, guides you through these tasks:

- **Setting up the Link-Live Cloud Service**, which extends the analyzer's network testing capability
- **Configuring the analyzer's settings and tests**, which prepares the analyzer to run an informative AutoTest

Working with the Setup Wizard

If you want to skip the **Setting Up the Cloud Service** or **Configuring the Analyzer's Settings and Tests** task, select the "Don't show me this again" check box at the beginning of the section.

At the beginning of each section, a **Yes/No** toggle control 

is displayed.

- Keep the default selection (**Yes**), and tap the **NEXT** button 

to complete the section.
- Select **No** and tap the **NEXT** button to skip the section.

You can exit the Setup Wizard at any time by selecting the **EXIT** button 

.

To Start the Setup Wizard at a Later Time

You can run the Setup Wizard again, at any time, to create additional Profiles.

1 Tap the **TOOLS** icon  on the HOME screen.

2 Tap the **Setup Wizard** button.

Connect to the Management Port

Connect a cable from your network to the RJ-45 Ethernet connector at the lower left side of the analyzer, next to the power connector. After making the connection, tap the NEXT  button.

Handling connection problems

If you get an error message stating that the OneTouch Internet connection was not established, follow these steps to troubleshoot the problem.

Proxy Server

If a network connection was established at the management port but the analyzer could not reach the OneTouch AT cloud site on the Internet, the next screen displayed will give you the opportunity to specify a proxy server.

Ensure that the management port received an IP address

1 Exit the Setup Wizard.

2 Tap the **TOOLS** icon  on the HOME screen.

3 Scroll down to the Maintenance Tools section, and tap the **Management Port** button.

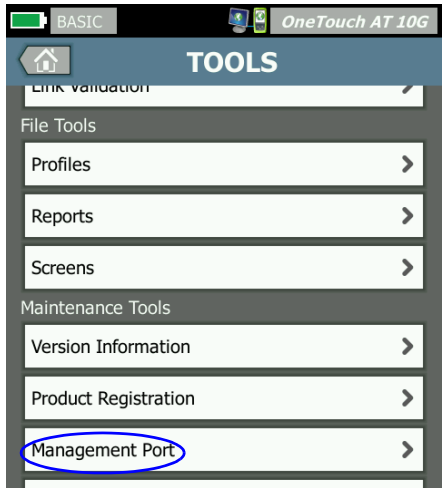


Figure 16. Management Port Button in TOOLS Menu

4 Ensure that the management port has an IP address, as shown below.

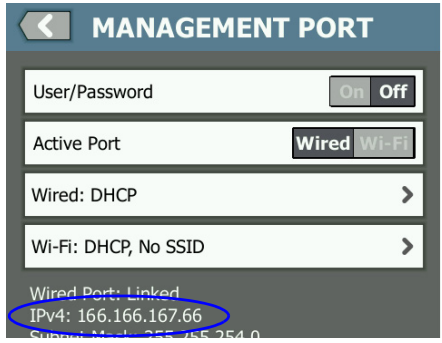


Figure 17. Management Port IP Address

If a static IP address is required

If your network requires you to assign a static IP address for the OneTouch analyzer's management port:

1 From the HOME screen, tap the TOOLS icon  .

2 Scroll down to the Maintenance Tools section, and tap the **Management Port** button.

3 Tap the **Wired** button.

4 Tap **STATIC** on the **Address** button and set the address.

Setting up the Cloud Service

Next, the Cloud Service Setup screen is displayed, and the analyzer guides you through setting up the Cloud Service.

Follow the on-screen prompts.

For more information, see the following sections:

- "Working with the Setup Wizard" on **page 41**
- "A **Cloud Remote icon** will be shown on the unit at the top of the screen." on **page 251**
- "Handling connection problems" on **page 42**

Configuring the Analyzer's Settings and Tests

Next, the Setup Wizard guides you through configuring network settings and tests, and storing them in a Profile.

A Profile contains various test, network, and security settings that are used when you run AutoTest.

Essentially, a profile is similar to a script that runs when you tap the AutoTest button. Profiles are the foundation of consistent, standardized testing.

You can create multiple Profiles for performing specific sets of tests. For example, you may want to create Profiles to test connectivity and performance for specific buildings on a site, specific departments within a business, or specific clients.

The first two sections of the Setup Wizard guide you through configuring the OneTouch AT analyzer to operate on your network. The sections are:

- Wired network settings
- SNMP configuration (Analysis)

The next sections let you set up network infrastructure/services tests.

- DHCP server response time limit
- DNS server response time limit

The last sections of the Setup Wizard let you set up network connectivity, infrastructure/network services, network performance, and application and protocol performance tests. These are referred to as User Tests, and they are shown as icons on the Test Tiers (see page 31) on the HOME screen.

- Ping (ICMP)
- Connect (TCP)
- Web (HTTP)
- File (FTP)
- Wired Performance
- Multicast (IGMP)
- Video (RTSP)
- Email (SMTP)

The entire configuration is stored in a Profile that you can easily recall and use. See Chapter 6: "Profiles," beginning on **page 151**.

You can exit the Setup Wizard at any time before saving a Profile by selecting the EXIT button 

. Partially completed Profiles are not saved. You can re-start the Setup Wizard later, as described on page 41.

Network Connectivity - Wired

The first configuration section of the Setup Wizard is Wired Network Connectivity. Here you can configure your network settings for a wired connection, e.g. speed/duplex, PoE, and network address.

For more information about wired network configuration, see "Analysis" on **page 188**.

To manually configure your wired network settings without using the Setup Wizard:

1 Tap **TOOLS** at the bottom left corner of the HOME screen.

2 Select **Wired** from the list.

Infrastructure Analysis/Network Services

This portion of the Setup Wizard allows you to configure your network's SNMP community strings to allow in-depth network analysis. For additional information about Network Analysis configuration, see "Analysis" on page 188.

Note

Configuring SNMP community strings enables additional network analysis and troubleshooting tools. The additional information is included in device configuration, system group information, and switch/router multiport statistics.

To manually configure your network's SNMP settings without using the Setup Wizard:

1 Tap **TOOLS** at the bottom left corner of the HOME screen.

2 Select **Analysis** from the list.

Network Performance

This Setup Wizard section lets you:

- Set the response time limit for your DHCP server test

- Specify a name to look up and response time limit of your DNS server test.

For information about the DHCP server test, see page 77, and for DNS test details, see page 79.

To manually configure your network's DHCP or DNS test settings outside of the Setup Wizard:

1 On the HOME screen, tap the **DHCP** icon  or the **DNS** icon  .

2 Select the **SETUP** tab.

Application and Protocol Performance

This section of the Setup Wizard lets you add User Tests to the Profile. The list of User Tests is shown on page 45. User Tests can verify performance of common applications and protocols running on your network.

A brief description of each User Test is shown on-screen along with its typical use. You can create multiple User Tests of each type.

For *detailed*, step-by-step instructions for adding a User Test without using the Setup Wizard, see "Adding User Tests" on page 49.

For *general* instructions on adding user tests without using the Setup Wizard, see Chapter 5: "User Tests," beginning on **page 83**.

Setup Wizard Completion

After completing the last configuration section, The Setup Wizard asks you to save your new Profile. The new Profile is loaded and ready to use on your OneTouch analyzer.

Now you are ready to run AutoTest and view the results. Continue to the next chapter.

Chapter 3: Basic Operation

Before you use the analyzer, read the safety information that starts on page 15.

This chapter provides instructions for:

- Adding a User Test to the HOME screen (detailed instructions)
- Connecting to a network
- Running AutoTest and viewing the results
- Using and customizing the HOME screen

Adding User Tests

User tests are tests that you create to test specific functionality of your network.

The following example explains how to add a Connect (TCP) user test to the HOME screen. Other user tests can be added by performing similar steps.

You can also add user tests from a Wired Analysis screen as described in “Wired Analysis Tools” on **page 167**.

Add a TCP Test to the Home Screen

You can add user tests to any of the three tiers on the HOME screen. The tiers provide a framework for you to organize the tests according to the network’s structure.

The Connect (TCP) test performs a TCP port open to the selected target to test for application port reachability using a TCP SYN/ ACK handshake.

1 To add a Connect (TCP) user test, touch and hold any white space on a test tier of the Home screen. For this exercise, touch and hold white space on the top tier.

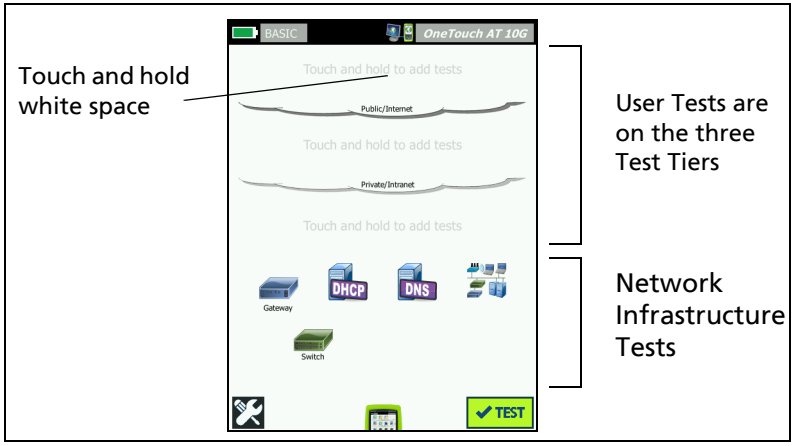


Figure 18. The Home Screen

The ADD TEST screen is displayed.

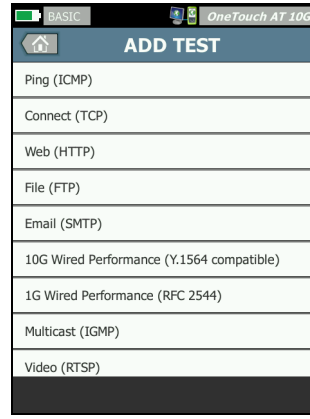


Figure 19. ADD TEST Screen

2 Tap **Connect (TCP)**. The test's screen opens with the SETUP tab selected.

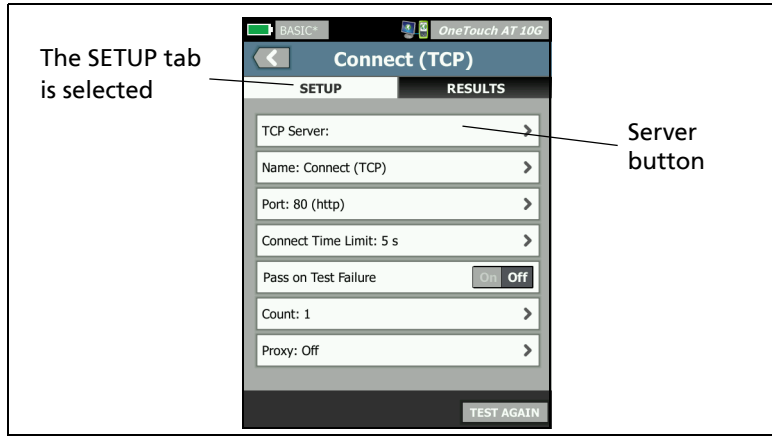


Figure 20. Connect (TCP) Test Setup Screen

3 Tap the **TCP Server** button. A context sensitive keyboard is displayed.

Figure 21. URL Keyboard

4 At the top of the screen, tap the **URL** button.

- The keyboard changes based on the type of information to be entered (e.g. IPv4 address, IPv6 address, URL).
- Shortcut buttons (e.g. “www.” and “.com”) on the keyboard help you to enter information quickly and easily.

5 Tap the **www.** button.

6 Type **enterprise.netscout** using the keyboard keys.

7 Tap the **.com** button.

8 Tap the **DONE** button.

9 The **Name** button allows you to assign a custom name to a test. The test’s name appears under the test’s icon on the HOME screen and in OneTouch Reports. For your convenience, the OneTouch analyzer automatically names the test based on the URL or IP address. Tap the **Name** button if you want to change the name.

10 The **Port** button lets you specify the TCP port number on which the connection will be established. For this test do not change the port from the default, which is port 80 (HTTP).

11 The **Time Limit** button lets you choose the amount of time allowed for the test to complete. If the test doesn't complete in the allowed time, it will fail. Set the time limit to 10 seconds.

12 **Count** specifies the number of three-way handshakes that will be completed. Set **Count** to 1.

13 The **Proxy** control lets you specify a proxy server through which the TCP requests can be routed. If your network uses a proxy server, tap the **Proxy** button, tap **On**, and set the server's address and port. Otherwise, continue to the next step.

14 Press the HOME key to return to the HOME screen.

When you add a user test, an asterisk appears after the Profile name to indicate that it has been changed, but not yet saved. See also: Chapter 6: "Profiles," beginning on **page 151**.

Connect to a Network

You can connect the OneTouch AT 10G analyzer to a network via the RJ-45 or SFP+ fiber ports.

If Ethernet connections are available at both the fiber and copper network ports, the analyzer uses the fiber port.

Establish a Wired (Copper) Connection

Connect an appropriate cable from the OneTouch AT 10G analyzer's RJ-45 port to the network that you want to test.

If you need to change the default wired connection configuration:

1 Tap the **Tools** icon  .

2 Tap the **Wired** button.

3 Set appropriate parameters for your network. See your network administrator for details. See also: “Wired” on page 184.

Establish a Fiber Connection

Install or Remove the SFP+ Fiber Adapter

To install an SFP+ Fiber adapter, remove the protective cap from the adapter and slide the adapter into the fiber port. To remove, gently pull the adapter’s bail. If the adapter has retention tabs, press and hold the tabs on the sides of the adapter and pull it from the fiber port.

The analyzer supports 1000M and 10G SFP+ fiber adapters.

Run AutoTest

AutoTest provides a comprehensive test of network infrastructure, along with user-defined tests.

The OneTouch analyzer does not initiate any link, user test, or infrastructure test activity until you run AutoTest.

Tap the AutoTest button 

(located at the lower-right corner of the HOME screen) or press the AutoTest key 

(located on the front panel). The analyzer will:

- Link on active ports
- Obtain IP addresses
- Run Network Infrastructure Tests (listed on page 66)
- Run User Tests (including the Connect (TCP) user test that you just created)
- When multiple user tests are present, they are run consecutively, starting with the lower-left test on the bottom test tier and finishing with the upper-right test on the top test tier.

You can capture traffic to and from the analyzer during AutoTest. See "AutoTest Capture" on **page 227**.

Icons Indicate Test Status

When AutoTest begins, the AutoTest button 

changes to a stop button  . Tap the stop button if you want to stop AutoTest before it completes. You can also stop AutoTest by pressing the AutoTest key 

.

As AutoTest runs, each user test icon changes to indicate its status.

The test has not started. The icon is faded.

The test is in progress.

The test passed.

The test failed.

The Connect (TCP) test is complete when its icon is marked with the green check mark ✔ to indicate it passed, or the red X ✖ to indicate it failed.

The shortcut bar's background is black until AutoTest completes. When AutoTest completes the shortcut bar's background turns green if all tests pass, or red if *any* test fails.

View the Test Results

On the HOME screen, each test's icon indicates whether the test passed ✔ or failed ✖.

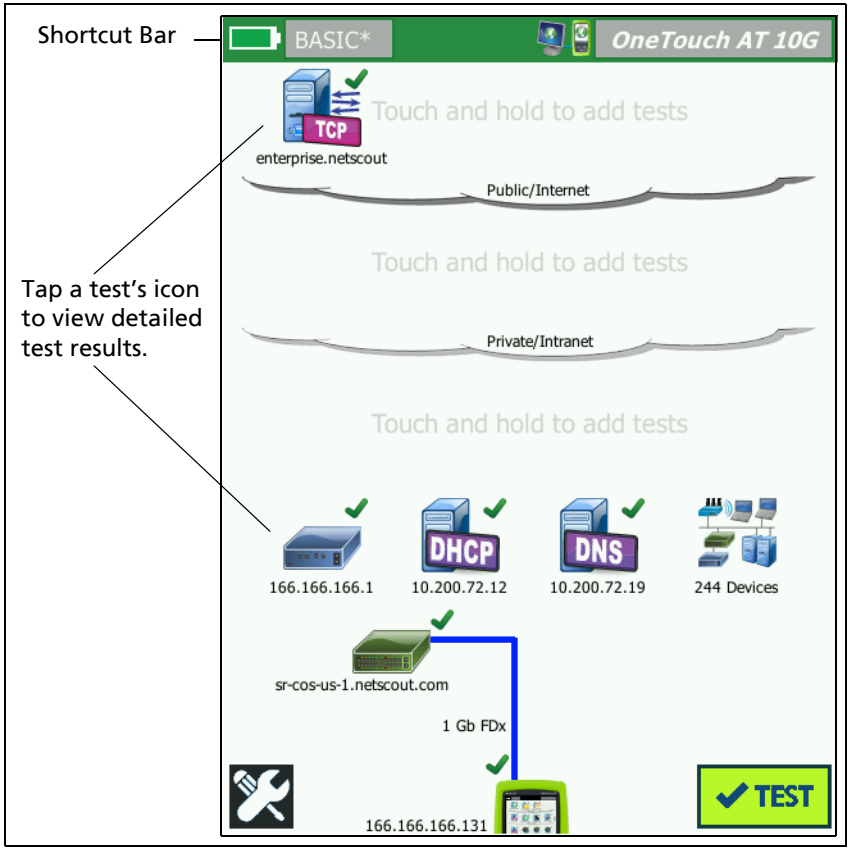


Figure 22. HOME Screen After Running AutoTest

View Detailed Test Results

Tap the Connect (TCP) test's icon. The enterprise.netscout Connect (TCP) test screen is displayed with the RESULTS tab selected.

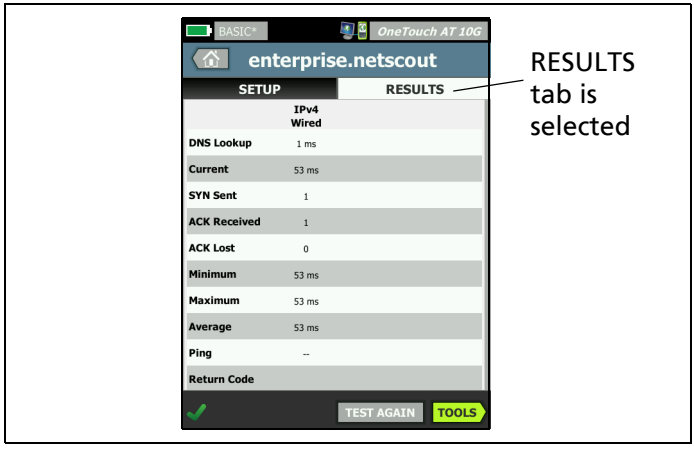


Figure 23. Connect (TCP) Test Results Tab

Measurement results for this example - Connect (TCP) - as well as all other user tests are described in Chapter 5: "User Tests," beginning on **page 83**.

Add More User Tests

You can add more user tests of any type to the HOME screen. Touch and hold white space on any of the three user test tiers to display the ADD TEST screen. You can touch and hold white space between existing test icons. Test tiers are shown on page 50.

You can also add user tests from a Wired Analysis screen as described in "Wired Analysis Tools" on **page 167**.

Organize User Tests on the Test Tiers

User tests are performed starting with the left side of the bottom tier, progressing from left to right on each tier, ending with the right-most test on the top tier.

You can use the test tiers to logically group your tests in a way that is meaningful to you. You can customize the test tier names to match your logical test grouping.

Rename the Clouds

On the HOME screen, the user test tiers are separated by clouds. By default, the cloud names are Public/Internet and Private/ Intranet. Tap a cloud to open the cloud's SETUP and RESULTS screen. The SETUP tab lets you rename the cloud. The RESULTS tab provides a summary of the number of tests on the tier above and the number of tests that failed when AutoTest was run.

See Off-Screen Tests

On the HOME screen, a chevron › at the end of a tier indicates that one or more tests are off-screen.

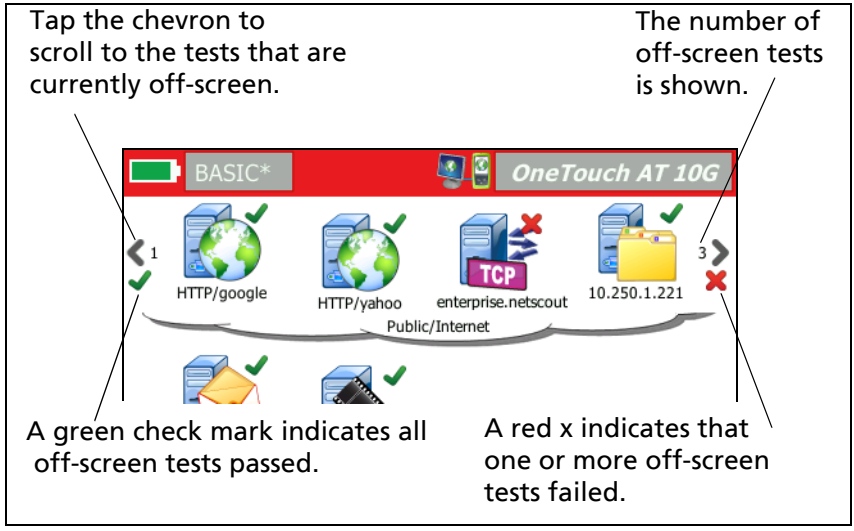


Figure 24. Seeing Off-Screen Tests

Run a Single User Test Again

You can run or re-run a single test.

1 On the HOME screen, tap the test's icon.

2 Tap the **TEST AGAIN** button TEST AGAIN .

Edit a User Test

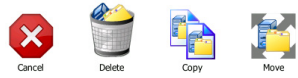
To edit a test, tap its icon. Tap the test's SETUP tab to edit the test parameters.

After editing a test, if it has been run and results are displayed, an asterisk (*) is displayed on the RESULTS tab to indicate that the results are not current. Re-run the test to view current results.

An asterisk is also displayed after the profile name at the top-left corner of the HOME screen, to indicate that the test profile has been changed. See Chapter 6: "Profiles," beginning on **page 151**.

Move, Copy, or Delete a User Test

Touch and hold the test's icon on the HOME screen. Four icons appear at the bottom of the screen.



- Tap the stop button to cancel the operation.
- Tap the trash can to delete the test.
- Tap the copy icon to copy the test. The copied test appears to the right of the original test.
- Tap the move icon, then tap a highlighted destination to move the test.
- If you do not tap one of the Cancel, Delete, Copy, or Move icons, you can tap a destination on one of the three user test tiers to move the test.

More About AutoTest

AutoTest is the automatic test feature of the OneTouch AT 10G analyzer.

AutoTest provides a comprehensive test of network infrastructure, followed by customizable user tests that you define.

- Network Infrastructure Tests are described on page 63.
- User Tests are described on page 83.

When AutoTest runs, the HOME screen is displayed so you can monitor the overall results. You can tap a test's icon to view its RESULTS screen.

When AutoTest completes, the analyzer retains its wired connections (link and IP address), and wired analysis begins.

When you run AutoTest again, the following actions occur.

- The wired links are dropped.
- Infrastructure test results, user test results, and wired discovery results are cleared.
- The wired link is re-established.
- Wired IP addresses are requested.
- All network infrastructure tests and user tests are re-run.
- The shortcut bar (at the top of the screen) turns green to indicate all tests passed, or red to indicate that one or more tests failed.

Next Steps

View Other Test Results

To view the results of other tests, return to the HOME screen and tap the test's icon.

Run Path Analysis, Browse to, or Telnet/SSH to a Test's Target Server

To run path analysis to a user test's target server, launch a browser against the target server, or Telnet/SSH to the server, tap the TOOLS button TOOLS on the test's RESULTS screen.

The following tests offer these tools:

Gateway Test

Nearest Switch Test

DNS Test

Ping (ICMP) Test

Connect (TCP) Test

Web (HTTP) Test

File (FTP) Test

Video (RTSP) Test

Email (SMTP) Test

See Also:

"Path Analysis" on **page 169**

"Browse to a Test Target from the HOME Screen" on **page 197**

"Telnet/SSH" on **page 197**

Configure the OneTouch AT 10G Analyzer to Use SNMP

Add SNMP Community Strings/Credentials to allow display of SNMP-enabled switch and gateway statistics, and enable cross-linking between wired device details via the Discovery Button. See "SNMP" on **page 158**.

Store Your Test Setup in a Profile

You can save OneTouch AT 10G analyzer test configurations in Profiles. See "Profiles" on **page 151.**

See IPv6 Results

To see IPv6 test results, enable IPv6 operation and run AutoTest again. See "Address" on **page 185**.

Generate a Report

See "Reports" on **page 205.**

Set Up Remote Control of the Analyzer

See "Remote User Interface and File Access" on **page 234.**

Chapter 4: Network Infrastructure Tests

When you run AutoTest the network infrastructure tests are performed to check the overall health of the network. Network infrastructure test icons are located on the lower half of the HOME screen.

When the network infrastructure tests complete, your user tests will run. See “User Tests” on **page 83.**

Each network infrastructure test is listed below. Select a test in the list to view its instructions.

OneTouch AT 10G Instrument 

Description

Tap the OneTouch AT 10G instrument icon (located at the bottom of the HOME screen) to show details of the wired network connections, including addresses, transmit and receive statistics, errors, and SFP information.

Configuration

Connect the OneTouch AT 10G analyzer to a wired network and tap the AutoTest button 

.

How it Works

The analyzer collects and displays connection parameters such as IP addresses, and monitors and reports on transmitted and received frames. Received frames with errors are categorized based on the type of error, and error counts are shown. If an SFP is installed, its manufacturer, model, type, serial number, and revision code are shown.

Results

On the HOME screen, the wired IP address is shown to the left of the OneTouch AT 10G instrument icon.

Tap the OneTouch AT 10G instrument icon to view test results and statistics gathered from the wired connections.

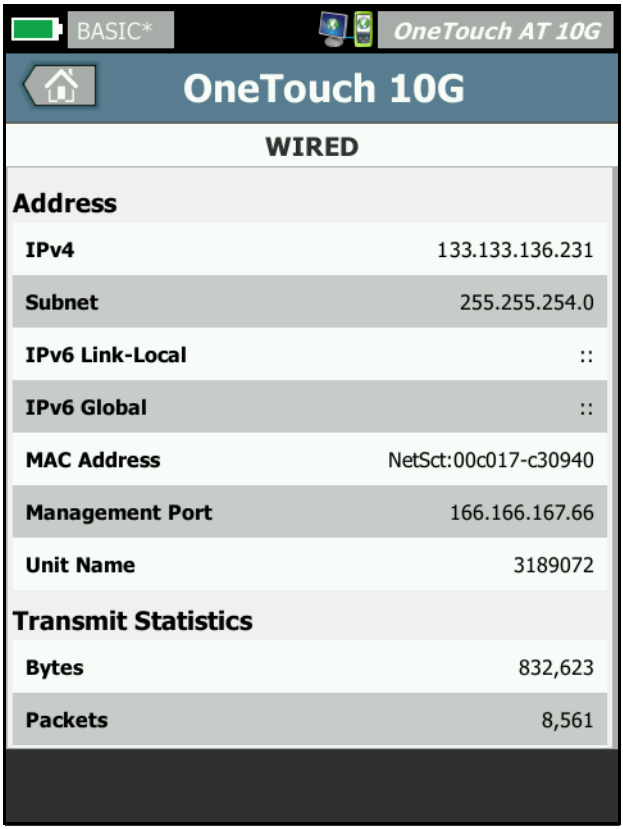


Figure 25. Wired OneTouch AT 10G Results

Address - The details of the analyzer's wired test port are shown. The analyzer's management port IP address is shown (if it is linked) at the bottom of this section.

Transmit Statistics - The number of bytes and total packets are shown.

Receive Statistics - The following information is displayed:

- **Bytes** - The total number of bytes received

- **Packets** - The total number of packets received
- **FCS Errors** - This counter increments for each frame received that contains a frame check sequence error.

Cable Test 

Description

This test verifies the integrity of a copper Ethernet cable connected to the OneTouch AT 10G analyzer. Additionally, optical power measurement is available when a fiber cable is used with a DDM-capable SFP.

When you tap the AutoTest button 

, the analyzer attempts to establish link. If the analyzer cannot establish link, it performs cable test instead.

Copper Cable Test

Configuration and Capabilities

Connect an Ethernet cable to the RJ-45 connector. The other end of the cable can be terminated (that is, connected to a network device) or unterminated (not connected).

When the test is run, for each copper pair, the analyzer reports the following:

- Opens (if they are more than 2 meters from the far end), and the distance to the open.
- Shorts, and the distance to the short.
- Splits (short to another pair), and the distance to the split.
- Termination

- Length (cable length is reported *only when* the pair is not terminated)
  Note: The length measurement is accurate to plus-or-minus 10 meters.

Results

Run AutoTest, then tap the cable icon on the home screen to view test results.

The following figures show the results of various analyzer and cable configurations.

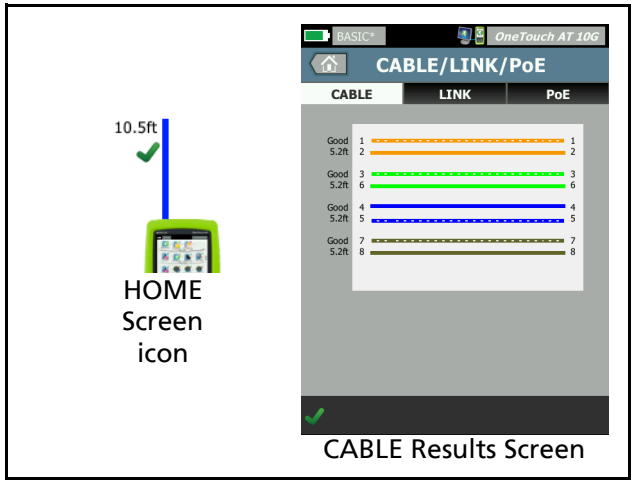


Figure 26. Unterminated Cable

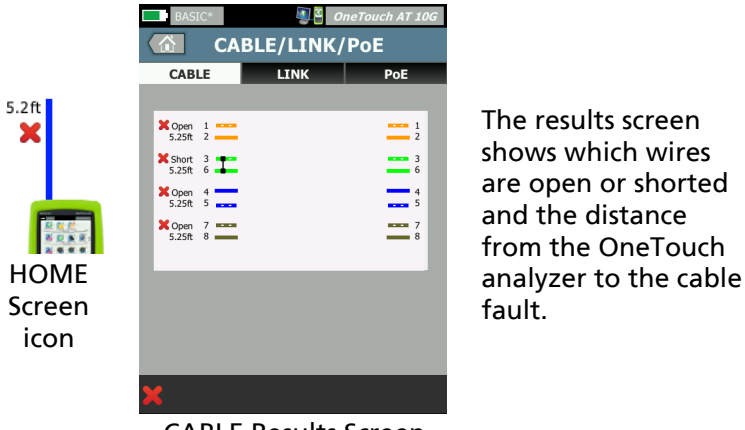


Figure 27. Unterminated Cable with Shorts and Opens

This shows an unterminated cable with shorts and opens connected to the RJ-45 network under test connector.

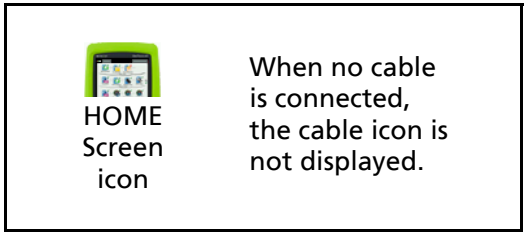


Figure 28. No Cable Connected

Fiber Cable Diagnostics

The analyzer works with fiber cables when connected via a 1000BASE-X SFP/SFP+ or 10G SFP+ adapter. The fiber cable is shown in orange on the HOME screen.

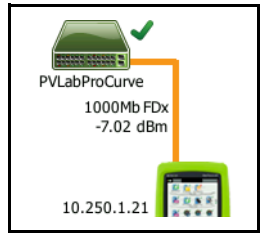


Figure 29. Fiber Cable Shown on HOME Screen

When a DDM (Digital Diagnostics Monitoring) capable SFP/SFP+ is installed in the analyzer, receive (Rx) power is displayed on the HOME screen, along with link speed. Vendor-specific information is displayed on the OneTouch instrument results screen.

Link Test

Description

The analyzer collects and reports link statistics when you run AutoTest.

Configuration

The OneTouch AT 10G analyzer automatically configures itself to work with the port where it is connected.

How it Works

The link test runs when you tap the AutoTest button TEST on the touchscreen or the AutoTest key TEST on the front panel.

Results

Link results are shown on the LINK tab of the CABLE/LINK screen.

Advertised Speed indicates the speed(s) offered by the port where the analyzer is connected.

Actual Speed is the speed that was negotiated when the analyzer connected to the network.

Advertised Duplex is the duplex capability of the port.

Actual Duplex is the duplex that was negotiated when link was established.

Crossover indicates whether the analyzer is using MDI or MDIX (internal crossover) mode when linked on the copper port.

Polarity indicates whether the wires of a pair are swapped. The analyzer automatically compensates for this condition.

Receive Power indicates the strength of the received signal on the fiber optic link.

Nearest Switch Test 

Description

Tap the switch to identify the switch name, model, port, and VLAN of the wired connection. If SNMP is enabled, parameters such as location, description, contact and up time as well as port receive and transmit statistics are reported.

Configuration

To display System Group information and Statistics, they must be available on the network via SNMP and you must configure the analyzer for SNMP. See “SNMP” on **page 158.**

How it Works

Information is displayed based on its availability via Link Level Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP), Extreme

Discovery Protocol (EDP), Foundry Discovery Protocol (FDP), and via SNMP. LLDP, CDP, EDP or FDP is used to identify the nearest switch, the connected port, the switch's address, and other information when available. The analyzer uses SNMP to acquire system group information and packet statistics for the port where the analyzer is connected.

Results

On the HOME screen, a green check mark ✔ next to the Nearest Switch icon indicates that the test passed. A warning icon ⚠ next to the Nearest Switch icon indicates that errors or discards were seen, but the test otherwise passed. A red X ✖ indicates that the test failed.

When the analyzer is connected to an un-powered switch, the un-powered switch icon is displayed.

In this condition test results vary. Apply power to the switch for complete test results.

Run AutoTest, then tap the Nearest Switch icon to show the results. There are two tabs: PORT and STATISTICS.

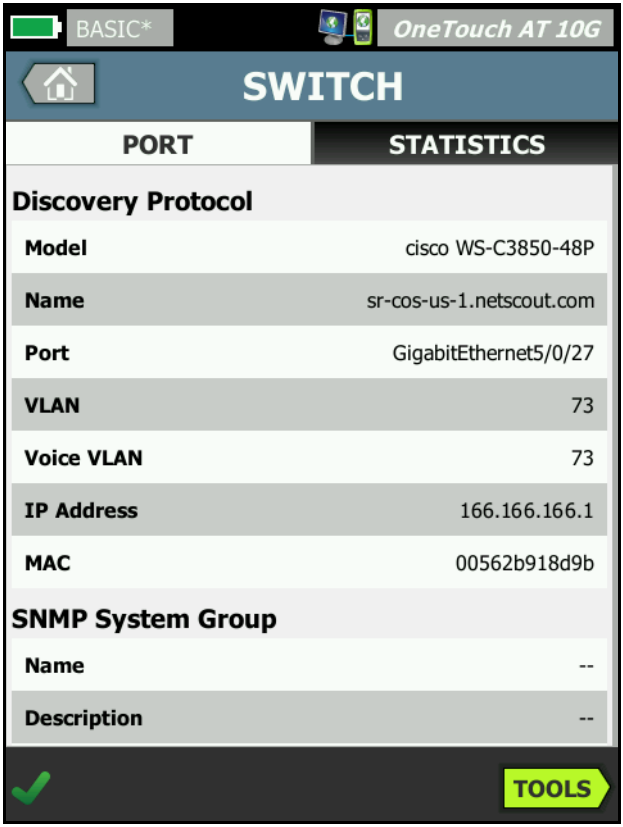


Figure 30. Nearest Switch - PORT Tab

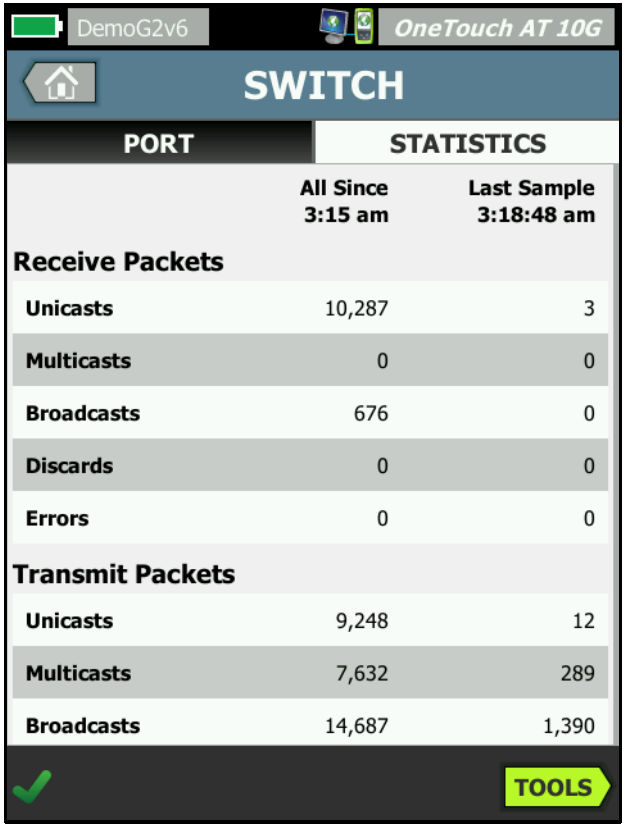


Figure 31. Nearest Switch - STATISTICS Tab

The analyzer uses SNMP to acquire system group information and packet statistics for the port where the analyzer is connected. Statistics monitoring begins when AutoTest completes. AutoTest is complete when the last user test finishes. This is indicated by the AutoTest button on the display changing from the stop button to the check mark TEST.

Statistics are updated every 15 seconds.

Gateway Test 

Description

Tap the gateway icon to identify the IP and MAC addresses of the current IPv4 and IPv6 router. Routing protocols and router ping connectivity are also reported. If SNMP is enabled, parameters such as name, location, description, contact and up time as well as router errors and discards are displayed.

Configuration

To display System Group information and Statistics, they must be available on the network via SNMP and you must configure the analyzer for SNMP. See “SNMP” on **page 158.**

How it Works

The analyzer gets the IP address of the gateway via DHCP or static configuration. Then the analyzer attempts to elicit a response from the gateway.

The analyzer uses SNMP to acquire system group information and statistics for the port that services the analyzer’s subnet.

Information in the Advertisement section of the RESULTS screen is gathered in a variety of ways, including via IPv6 router advertisements.

Results

If the gateway responds, the test passes and a green check mark ✔ is shown next to the Gateway icon on the HOME screen. If the gateway does not respond, a red x ✖ is shown. A warning icon ⚠ is shown if discards or errors were observed, or if the ping failed. The gateway may be configured to ignore pings. The test is considered to have passed even if the warning icon is shown.

Tap the Gateway icon to show gateway information, including wired gateway statistics.

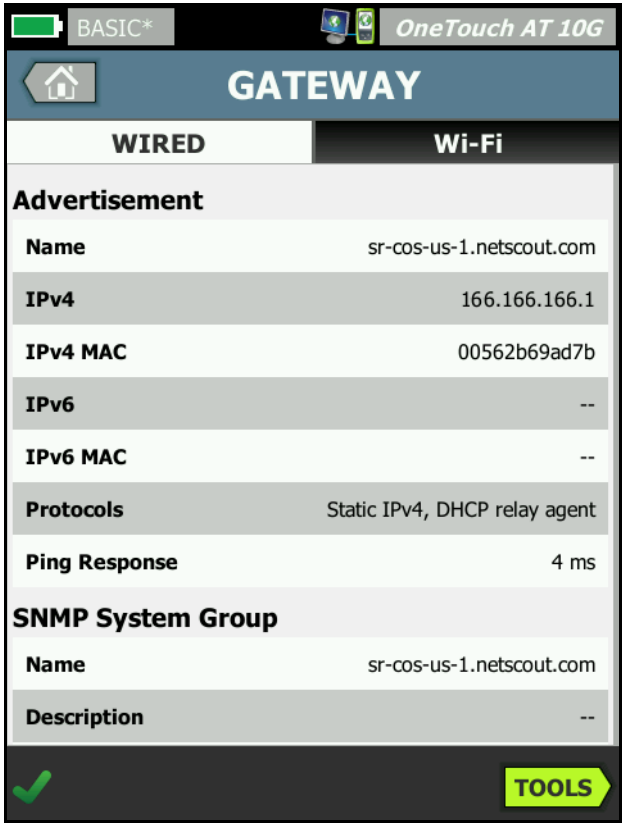


Figure 32. Gateway WIRED Tab

Wired gateway statistics are updated every 15 seconds.

DHCP Server Test 

Description

The DHCP (Dynamic Host Configuration Protocol) server test provides a breakdown of the process of acquiring a DHCP IP address on both the wired connections. The identity of the DHCP server, offer and acceptance timing, and lease information are provided. The analyzer also detects and reports the presence of more than one DCHP server on the network.

Configuration

If the analyzer is configured with a static IP address, the DHCP Server Test will not run. The test's icon will appear faded, and the word "Static" will be displayed under the icon.

If the analyzer is configured for DHCP, this test will run. To enable or disable DHCP, see page 185.

The **Time Limit** determines how much time can elapse before the analyzer receives a response from the server. If the Time Limit is exceeded, the test will fail.

1 On the HOME screen, tap the DHCP server icon  .

2 Tap the **SETUP** tab.

3 Tap the **Time Limit** button and choose a limit.

How it Works

The analyzer broadcasts a message to discover DHCP servers in the broadcast domain. Typically, there should be only one DHCP server in the broadcast domain. It responds with an IP address and lease, and provides other information such as the subnet mask, and the IP address of the default gateway and DNS server.

Results

Figure 33. DHCP Test Results

Server IP is the IP address of the DHCP server.

The **Server Name** field is populated with the name that the analyzer obtains during device discovery. The field is blank until AutoTest has completed and the analyzer has found a name for the server.

Offer is the offered address.

The DHCP process has four parts: discover, offer, request, and acknowledge. **Offer Time** is from the start of the DHCP discover process until an offered IP address is returned by the DHCP server.

The offered address is shown in the **Accept** field when it has been accepted by the analyzer.

Total Time is the total amount of time consumed by the DHCP discover, offer, request, and acknowledge process.

The **Subnet Mask** is provided to the analyzer by the DHCP server.

Subnet ID - This is the combination of the subnet mask and the offered IP address (shown in CIDR notation).

Lease Time - This is the amount of time that the IP address is valid.

Expires - This is the accepted time plus the lease duration.

Relay Agent - If a BOOTP DHCP relay agent is present, this shows its IP address. The relay agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

Offer 2 - If a second address has been offered it is shown here, and a warning icon ⚠ is displayed next to the DHCP test icon on the HOME screen.

MAC Address - The MAC address of the DHCP server.

IPv6 Wired Prefix - The network portion of the IPv6 address, obtained via router advertisement.

DNS Server Test 

Description

The DNS (Domain Name System) server test checks the performance of DNS servers resolving the specified URL. The returned IP address as well as DNS server addresses are also reported.

Configuration

You can configure the URL that will be looked up by the DNS server, and the time limit. You can enter or change the name to be looked up using the **Name to Lookup** button on the SETUP screen. If no name is specified, the DNS test is not graded. (It will neither pass nor fail.)

1 On the HOME screen, tap the DNS server icon 

.

2 Tap the **SETUP** tab.

3 Tap the **Name** tab and enter the domain name to look up.

4 Tap the Time **Limit button** and choose the amount of time you want to allow for the test to complete.

How it Works

The address of the DNS server is obtained through DHCP or by static configuration, via the wired connection. The analyzer contacts the DNS server and requests resolution of the URL to an IP address. If the DNS server does not reply or cannot resolve the name, the test will fail.

Results

If the analyzer can perform a DNS lookup for the configured URL via the wired connection, the test will pass.

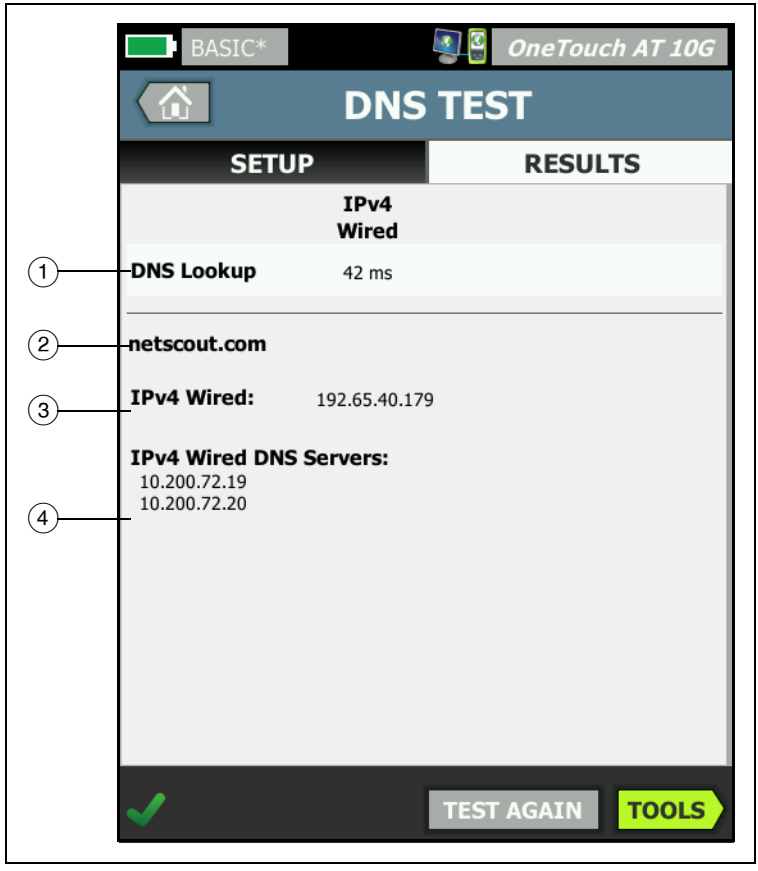


Figure 34. DNS Test Results

① **DNS Lookup** is the time it took to receive the address after the lookup request was sent.

② This is the URL to be resolved, which is configured on the SETUP tab.

③ Resolved IP addresses

④ Primary and secondary DNS servers

Wired Analysis 

Tap the Wired Analysis icon  to see and analyze discovered wired hosts, access devices, and servers.

See Chapter 7: "Wired Analysis," beginning on **page 157** for details.

Chapter 5: User Tests

You can create user tests to assess specific functionality on your network.

To edit a user test, tap its icon on the HOME screen. Two tabs are shown: SETUP and RESULTS. Tap the SETUP tab.

You can save user tests, along with other OneTouch AT 10G analyzer settings, in a Profile. See “Profiles” on **page 151.**

Icons for user tests are located in the Test Tiers. The Test Tiers occupy the top half of the analyzer’s display. See “Test Tiers” on **page 31.**

For instructions on adding user tests, see “Adding User Tests” on page 49.

See also: "Finding User Test Target Servers" on **page 166**.

Each user test is listed below.

Ping (ICMP) Test 

Purpose

Ping sends ICMP echo requests to the selected target to determine whether the server or client can be reached. The target can be an IPv4 address, IPv6 address or named server (URL or DNS).

Configuration

Server - Enter the IP address or the name of the server you want to ping. If you enter an IP address, the DNS lookup portion of the test will be skipped.

Name - The **Name** button allows you to assign a custom name to the test. The test's name appears under the test's icon on the HOME screen and in OneTouch AT 10G Reports. For your convenience, the analyzer automatically names the test based on the URL or IP address. Tap the **Name** button if you want to change the name.

Frame Size - This specifies the total size of the payload and the header to be sent. Valid sizes are 78 bytes to 9600 bytes.

To test the MTU along a route to a target, select the MTU frame size you want to test and set **Don't Fragment** to **On**.

Time Limit - The amount of time allowed for each ICMP echo reply packet to return.

Pass on Test Failure - This feature causes the test to display a Pass symbol (check mark icon) if the OneTouch does NOT successfully connect to the test target or establish communication, based on the parameters of the test. The check mark will be Red rather than Green to indicate that the Pass on Test Failure feature is enabled. Turn this setting On if you want to ensure that the target is NOT accessible at your location.

- Test failed - Connection available or communication established.

- Test passed - No connection available or unable to access.

Count - This is the number of ICMP echo request packets that will be sent. The count can be set from one to Continuous.

In Continuous mode packets are sent once per second. AutoTest is suspended and the link is maintained until you stop the test.

In Continuous mode, the analyzer will send packets over the wired connection if available.

When in Continuous mode, the test's results are shown on the RESULTS tab. The test is not graded as having passed ✔ or failed ✘ until the test is stopped. Press the AutoTest (✔TEST) key to stop the test.

When not in Continuous mode, the analyzer will send pings over all enabled interfaces. Wired IPv4 and wired IPv6 pings run simultaneously.

Don't Fragment - When this option is **On**, the analyzer will set the "don't fragment" bit in the frame. The frame will not be split into smaller frames when passing through switches and routers.

How it Works

The ping test sends echo request packets to a host and awaits replies. Ping responses that do not return within the selected time limit are considered lost.

The analyzer sends ICMP echo request packets to the target host (the server) and waits for a response. The analyzer records the response time and reports whether packet loss occurs. The analyzer uses the ICMP protocol for IPv4 tests, and the ICMPv6 protocol for IPv6 tests.

Results

The results include the current ping response as well as overall response statistics.

The test will fail if any packet loss occurs, or if the selected time limit is exceeded.

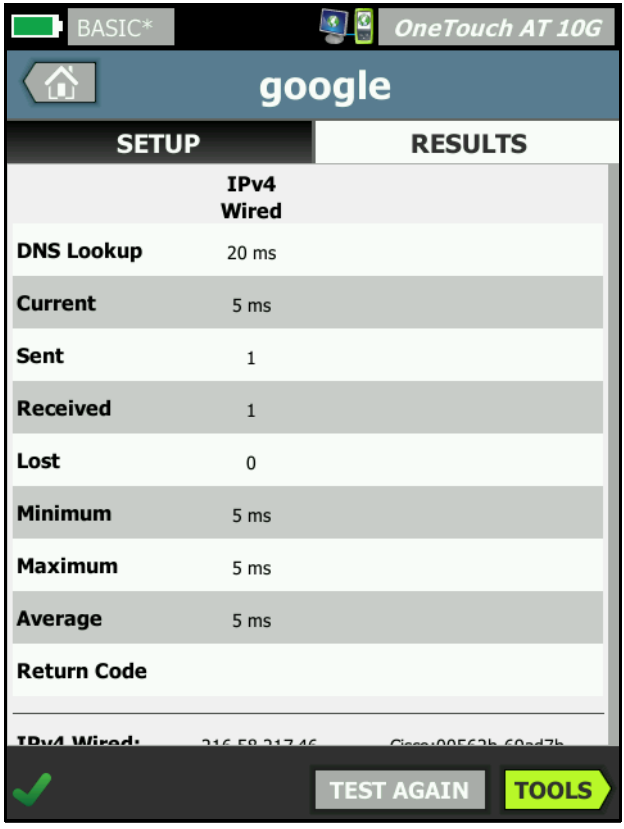


Figure 35. Ping Test Results

DNS Lookup is the amount of time it took to resolve the optional URL into an IP address.

Current is the elapsed time from when the ICMP echo request packet was sent and its reply was received. If **Count** is set to a number greater than one, this number is updated when each reply is received.

Sent is the number of ICMP echo request packets that have been sent.

Received is the number of ICMP echo reply packets that have been received.

Lost is the number of ICMP echo request packets that were sent but not received within the selected time limit.

Minimum is the minimum amount of time it took to receive an ICMP echo reply packet.

Maximum is the maximum amount of time it took to receive an ICMP echo reply packet.

Average is the arithmetic mean time it took to receive ICMP echo reply packets.

Return Code specifies the end-of-test status or an error condition if encountered.

Below the Return Code, the target server addresses are displayed. If the request had to travel to a different network the router's address is displayed. If you specified a target server's URL, these addresses are supplied by DNS servers. The target servers' MACs are also displayed.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test. Tap the **TOOLS** button 

to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

Connect (TCP) Test 

Purpose

The Connect (TCP) test performs a TCP port open to the selected target to test for application port availability. The test verifies basic application port connectivity using a 3-way handshake (SYN, SYN/ACK, ACK). The test can be used to determine whether a service is available. TCP port connectivity can be preferable to ping testing because ping may be blocked or disabled on target devices or their routes.

The target can be an IPv4 address, IPv6 address or named server. The port parameter allows testing for specific application availability on well-known system ports such as port 80 for HTTP or private ports up to 65535. Visit **www.iana.org** for complete list of registered ports.

Configuration

Server - Enter the URL or the IP address of the target server. See also: “Server” on **page 84**.

Name - The Name button allows you to assign a custom name to the test. See also: “Name” on **page 84**.

Port - Specify the TCP port number on which the TCP connection will be established.

Connect Time Limit - Set the amount of time allowed for the TCP connection to be established.

The wired IPv4 and wired IPv6 tests run simultaneously.

Pass on Test Failure - This feature causes the test to display a Pass symbol (check mark icon) if the OneTouch does NOT successfully connect to the test target or establish communication, based on the parameters of the test. The check mark will be Red rather than Green to indicate that the Pass on Test Failure feature is enabled. Turn this setting On if you want to ensure that the target is NOT accessible at your location.

- Test failed - Connection available or communication established.
- Test passed - No connection available or unable to access.

Count - This is the number of times the TCP connection will be established. If Continuous is selected the Time Limit will be ignored.

In Continuous mode, the analyzer will establish the TCP connection over the wired Ethernet connection if available.

When in Continuous mode, the test's results are shown on the RESULTS tab. The test is not graded as having passed ✔ or failed ✘ until the test is stopped. Press the AutoTest TEST key to stop the test.

Proxy - The Proxy control lets you specify a proxy server through which the TCP connection will be established. To specify a proxy server, tap the **Proxy** button, tap **On**, and set the server's address and port. Otherwise, continue to the next step.

How it Works

The TCP test performs a DNS lookup on the specified URL. If you specify an IP address, the DNS lookup is not performed.

The TCP connection is established by executing a three-way handshake (SYN, SYN/ACK, ACK). At this point the test is complete and the analyzer closes the port. No data is transferred after the TCP connection is established.

If you have set the count to a number greater than one, the TCP connection process is repeated.

Results

If the SYN/ACK is not received from the target on all enabled interfaces (wired, IPv4, IPv6) within the time limit, the test will fail.

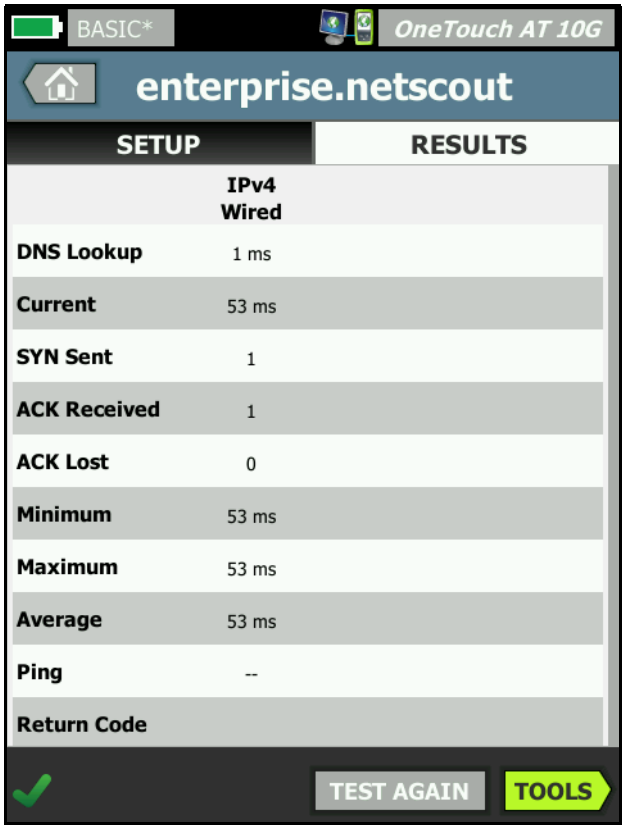


Figure 36. TCP Test Results

DNS Lookup is the amount of time it took to resolve the optional URL into an IP address.

Current shows the amount of time it took to complete the last TCP connection.

SYN Sent shows the number of SYNs sent by the analyzer.

ACK Received shows the number SYN/ACKs received by the analyzer.

ACK Lost shows the number of SYNs for which a SYN/ACK was not received within the selected time limit.

Minimum is the minimum amount of time it took to establish a TCP connection.

Maximum is the maximum amount of time it took to establish a TCP connection.

Average is the arithmetic mean time it took to establish a TCP connection.

A ping test runs simultaneously with the TCP test. If the TCP test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered.

Below the Return Code, the target server addresses are displayed. If the request had to travel to a different network, the router's address is displayed. If you specified a target server's URL, these addresses are supplied by DNS servers. The target servers' MACs are also displayed.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test. Tap the **TOOLS** button 

to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

Web (HTTP) Test 

Purpose

The Web (HTTP) test performs a comprehensive end user response time (EURT) measurement when downloading the specified web page.

The target can be an IPv4 address, IPv6 address or URL. The transfer size allows limiting the amount of data downloaded ranging from the HTML header only to the entire page. Optional proxy support is provided for more sophisticated enterprises.

Results provide a complete breakdown of the overall end user response time into its component parts. If the page is not downloaded within the time limit the test fails.

Configuration

Server - Enter the URL or the IP address of the target server.

By default, the HTTP test tries to reach the target server on port 80. To reach web servers that operate on a different port, type a colon (:) and specify the port number after the URL. For example, to reach a web server on port 8080 use the following format: www.website_name.com:8080. See also: “Server” on **page 84**.

Name - The Name button allows you to assign a custom name to the test. See also: “Name” on **page 84**.

Transfer Size lets you limit the amount of data that will be downloaded from the target server.

Time Limit - Set the amount of time allowed to transfer the web page. If the total test time exceeds the time limit, the test will fail.

When running the test via multiple network connections, the Time Limit applies to each individual network connection.

Pass on Test Failure - This feature causes the test to display a Pass symbol (check mark icon) if the OneTouch does NOT successfully

connect to the test target or establish communication, based on the parameters of the test. The check mark will be Red rather than Green to indicate that the Pass on Test Failure feature is enabled. Turn this setting On if you want to ensure that the target is NOT accessible at your location.

-  Test failed - Connection available or communication established.
-  Test passed - No connection available or unable to access.

Proxy - The Proxy control lets you specify a proxy server through which the TCP connection will be established. To specify a proxy server, tap the **Proxy** button, tap **On**, and set the server's address and port. Otherwise, continue to the next step.

Return Code - Functions as pass/fail test criteria with focus on the return code value of a specified server or URL.

Select a return code from the list of available return codes. If your selected return code value matches the actual return code value, the test will pass.

HTML Must Contain - Functions as pass/fail test criteria with focus on the presence of a text string on a specified server or URL. For example, this criteria can be used to ensure that the expected page is being tested versus an intermediate portal.

To construct a text string, enter a word or several words with exact spacing. When specifying several words, the expectation is that these must be located consecutively at the source. The test will pass if the text string is found. If the string is not found, the test will fail with the return code: HTML did not contain expected content.

HTML Must Not Contain - Functions as pass/fail test criteria with focus on the absence of a text string on a specified server or URL.

To construct a text string, enter a word or several words with exact spacing. When specifying several words, the expectation is that these will be located consecutively at the source. The test will

pass if the text string is not found. If the string is found, the test will fail with the return code: HTML did contain expected content.

How it Works

When you execute an HTTP test, the analyzer:

- Contacts the DNS server to resolve the target's name (if a URL was specified rather than an IP address)
- Runs a ping test concurrently with the HTTP Test
- Establishes a TCP connection and attempts to get the web page
- Checks for any user-specified test criteria

Results

The test passes if the amount of data specified using the Transfer Size control is downloaded within the time specified using the Time Limit control.

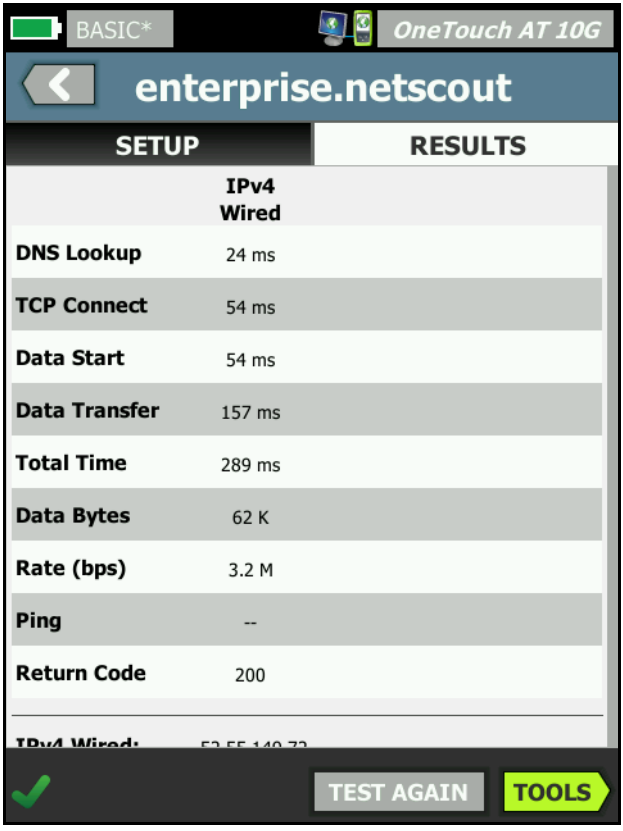


Figure 37. Web (HTTP) Test Results

DNS Lookup is the amount of time it took to resolve the URL to an IP address. If you enter an IP address, DNS lookup is not required, so dashes -- will be displayed to indicate that this part of the test was not executed.

TCP Connect is the amount of time it took to open the port on the server.

Data Start is the time it took to receive the first frame of HTML from the web server.

Data Transfer is the amount of time it took to receive the data from the target server.

Total Time is the end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Time Limit you selected the test will fail.

If the Time Limit is exceeded during test, the current phase of the test (DNS, Lookup, Data Start, or Data Transfer) is marked with a red X and the test is aborted.

Data Bytes is the total number of data bytes transferred. Header bytes are not included in the measurement.

Rate is the data transfer rate.

A ping test runs simultaneously with the HTTP test. If the HTTP test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered. Plain text descriptions of the errors are displayed at the bottom of the screen.

Below the Return Code, the target server address(es) are displayed. If you specified a target server's URL, these addresses are supplied by DNS servers.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test. Tap the **TOOLS** button 

to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

File (FTP) Test 

Purpose

The File (FTP) test performs a file upload or download, allowing verification of WAN, server and network performance. The target can be an IPv4 address, IPv6 address or URL. Optional proxy support is provided for more sophisticated enterprises. Results provide a complete breakdown of the overall file transfer time into its component parts.

Configuration

Server - Enter the URL or the IP address of the target server.

The **Name** button allows you to assign a custom name to the test.

Transfer Size lets you limit the amount of data that you will download (Get) from the target server when **Direction** is set to **Get**. It also sets the amount of data that will be uploaded (Put) to the server when the Direction control is set to **Put**.

Specifying a transfer size that is greater than the amount of data than can be retrieved from the target server will not cause the test to fail. The test will terminate when the file has finished downloading.

All, which is available when Getting data, causes the download to continue until the entire file has been downloaded or until the time limit has been reached.

Time Limit - If the amount of data selected in “Transfer Size” is not downloaded from the target server within the specified time, the test will fail. When running the test via multiple network connections, the Time Limit applies to each individual network connection.

Pass on Test Failure - This feature causes the test to display a Pass symbol (check mark icon) if the OneTouch does NOT successfully connect to the test target or establish communication, based on the parameters of the test. The check mark will be Red rather

than Green to indicate that the Pass on Test Failure feature is enabled. Turn this setting On if you want to ensure that the target is NOT accessible at your location.

-  Test failed - Connection available or communication established.
-  Test passed - No connection available or unable to access.

Proxy - The Proxy control lets you specify a proxy server through which the FTP connection will be established. To specify a proxy server, tap the **On** button on the PROXY screen. Then specify the proxy server's address and port.

Direction - Use the Direction control to specify a Get (download data from a server) or Put (upload data to a server) operation.

User and Password: Enter these credentials to access the target server you specified. If left blank, the FTP server will assume you wish to establish an anonymous connection. The test will fail if the configured user name and password are not valid on the target FTP server.

File: The function that the File field implements depends on whether you've chosen to Get or Put data.

If **Direction** is set to **Get**, File specifies the name of the file to be downloaded from the server. The file will be retrieved and the size and data rate will be calculated. Data is discarded as soon as it is downloaded. It is not written to a file and it is not retained on the analyzer.

If **Direction** is set to **Put**, File specifies the name of the file that is created on the server. The size of the file is determined by the Transfer Size control. The file contains a text string that indicates the file was sent from the analyzer. The text string is repeated to produce the desired file size.

How it Works

The analyzer establishes a control connection with the FTP server on port 21 in order to negotiate the data that will be transferred,

and to authenticate to the FTP server. Next, a data connection is established with the FTP server. This connection serves to transfer the data. Upon completion of data transfer the data transfer connection is released and then the control connection is released. The test runs on each configured network interface.

Results

If the Total Time is less than the selected Time Limit the test passes. If the Time Limit is exceeded during test, the current phase of the test is marked with a red X and the test is aborted.

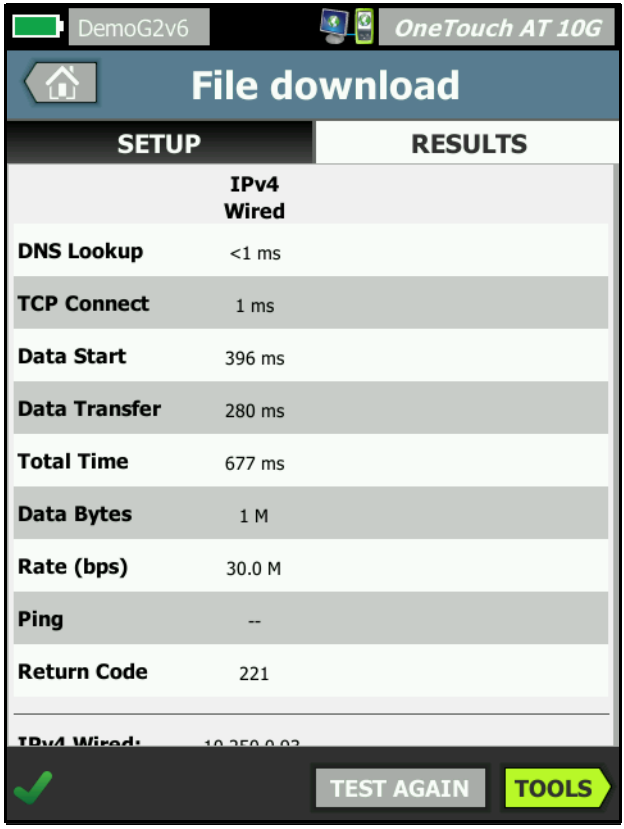


Figure 38. FTP Test Results

DNS Lookup is the amount of time it took to resolve the optional URL into an IP address.

TCP Connect is the amount of time it took to open the port on the server.

Data Start time is measured from when the port was opened until the first file data was received.

Data Transfer is the amount of time it took to receive the data from the target server.

Total Time is the end user response time (EURT), which includes DNS lookup time, TCP connect time, Data Start time, and the time it took to upload/download the specified amount of data to/from the target server.

Data Bytes is the total number of data bytes transferred.

Rate is the measured bit rate, based on frames sent or received.

A ping test runs simultaneously with the FTP test. If the FTP test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered.

Below the Return Code, the target server addresses are displayed. If you specified a target server's URL, these addresses were supplied by DNS servers.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test. Tap the **TOOLS** button 

to run path analysis to the target server,

launch a browser against the target server, or Telnet/SSH to the server.

1G Wired Performance Test (RFC 2544)

Purpose

The 1G Wired Performance (RFC 2544) test provides point-to-point performance testing of a traffic stream across wired IPv4 network infrastructure. This test is typically used to validate network performance. It quantifies network performance in terms of throughput, loss, latency, and jitter.

The analyzer exchanges a stream of traffic with Peers or Reflectors and measures the performance of the traffic stream. You can run the test at a full line rate of up to 1 Gbps for performance validation, or at lower speeds to minimize disruption when troubleshooting operational networks.

The test is based on the Internet Engineering Task Force (IETF) RFC 2544 Benchmarking Methodology for Network Interconnect Devices.

You can use the Wired Performance Test to

- verify that a network configuration delivers the expected performance
- evaluate newly deployed equipment
- evaluate network performance prior to deployment of new services such as VoIP

Configuration

Network performance is measured between two points using two analyzers. Therefore, configuration includes setting up source and endpoint analyzers. Traffic is exchanged and measured between the source and the endpoint.

- The source is the OneTouch AT 10G analyzer on which the test is configured and controlled.
- The endpoint is the remote device that exchanges traffic with the source.

There are two types of endpoints for this test:

Peer - A peer is another OneTouch AT 10G analyzer or a OneTouch AT analyzer. When using a peer endpoint, separate upstream and downstream measurements are shown for throughput, frames sent, frames received, and frames lost. Latency and jitter measurements are made on roundtrip traffic.

Reflector - A reflector can be a LinkRunner AT, LinkRunner G2, or NETSCOUT NPT Reflector software installed on a PC. Frames are sent from the analyzer and returned from the reflector to the analyzer. When using a reflector, the analyzer uses roundtrip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

To run this test:

- **Set up the peer or reflector for the test**.
  - "To Configure a OneTouch AT Analyzer as a Peer" on **page 107**
  - "To Configure a LinkRunner AT (2000) as a Reflector" on **page 110**
  - "To Configure a LinkRunner G2 as a Reflector" on **page 112**
  - "To Use the NETSCOUT Network Performance Test (NPT) Reflector Software" on **page 112**
- **Set up the source OneTouch AT 10G.** See "To Configure a OneTouch AT 10G Analyzer as the Source" on **page 109**.

SETUP Parameters

The following configuration settings are available in the SETUP tab of the 1G Wired Performance (RFC 2544) test:

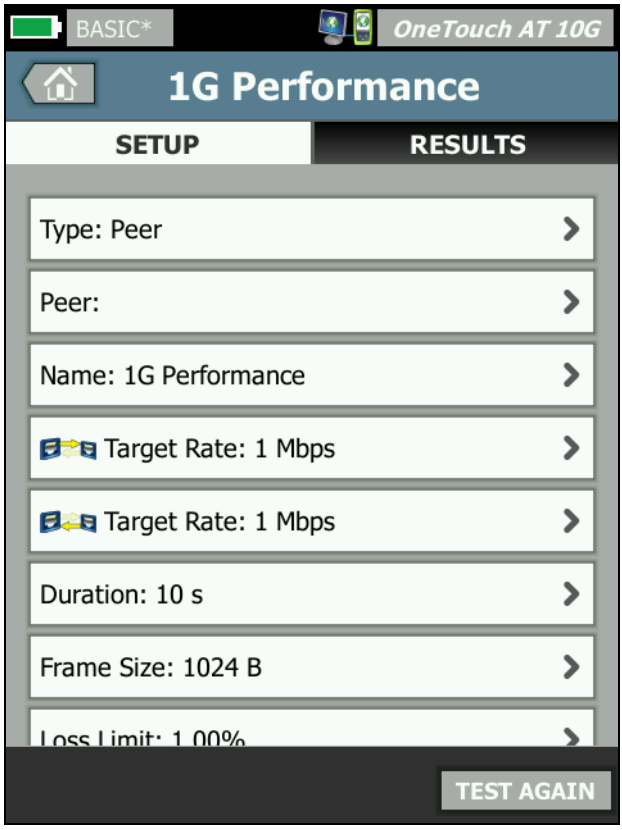


Figure 39. 1G Wired Performance Test Setup Tab

Type - specifies that the endpoint device will behave as a performance peer or reflector.

Peer/Reflector - specifies the IP address of the endpoint device.

Name - allows you to assign a custom name to the test. See also: “Name” on page 84.

Target Rate - the requested rate of upstream traffic (from the source analyzer to the peer). Valid rates are from 100 Kbps to 1 Gbps. If the actual rate is less than 99% of the requested rate, the test will fail.

Target Rate - the requested rate of downstream traffic (from the peer to the source analyzer). Valid rates are from 100 Kbps to 1 Gbps. If the actual rate is less than 99% of the requested rate, the test will fail.

Note

The above description applies when using a peer. When using a reflector, upstream and downstream traffic are not individually measured. Results are based on roundtrip traffic, and only one rate can be specified.

Duration - the length of time the test will run. You can run a quick one-second test or up to a full minute of testing.

Frame Size - the size of the frames that the analyzer will exchange with the endpoint. The header is included in the frame size. **Sweep** performs an RFC 2544 sweep test. The test runs for the specified duration at each frame size: 64 B, 128 B, 256 B, 512 B, 1024 B, 1280 B, and 1518 B. Results can be viewed in tabular or graphical format. See “Results” on **page 114.**

Loss Limit - the percentage of frames that can be lost. If this value is exceeded, the test will fail.

DSCP (Differentiated Services Code Point) - allows you to specify a priority for the generated traffic by changing its classification. This is a six-bit field. The default value of zero specifies “best effort.”This configuration parameter lets you verify higher quality of service (QoS) for applications such as VoWiFi.

Port - specifies the UDP port for the test’s control connection. The same port must be specified on the peer endpoint. The next two higher port numbers are also used for the test. See “How it Works,” below.

To Configure a OneTouch AT Analyzer as a Peer

Follow these steps to configure a OneTouch AT, G2, or 10G as a peer endpoint.

1 Connect AC power to the analyzer. This ensures that the unit will not run out of battery power, and will not automatically power-down if a Timeout Period is set.

2 Tap the **TOOLS** icon  on the HOME screen.

3 In the Testing Tools section, tap the **Performance Peer** button.

4 Set the **Port** number, and turn **Enable AutoStart** on or off.

Port - Select the appropriate UDP port number. Whether you use the default port or select another port number, the port must not be blocked by network security. Note that you must select the same port in the source OneTouch AT 10G Wired Performance Test configuration.

Enable AutoStart - If set to On, the Peer will start automatically every time the OneTouch is turned on. To start the Peer manually, tap the Start button in the lower right corner of the PERFORMANCE PEER screen.

5 Run the test. See "Run the Test" on **page 113** for more information.

The following information is displayed in the PERFORMANCE PEER screen once you have started the analyzer as a peer:

Utilization graph - Shows the utilization as a percentage of line rate as measured by the peer OneTouch AT.

Address - Shows the peer link information, IP address, port number, and MAC address.
Note: You need to supply the peer IP address to the source OneTouch AT 10G analyzer.

Connections - Shows information about the connection to the source OneTouch AT 10G analyzer:
- IP address of the last source analyzer to which the peer was connected.

- IP address of the currently connected source is shown.
- Test state: Ready, Running, Finishing, Linking, Stopped.

Instrument - Shows the management port IP address.

SFP Information - Shows vendor and model info for the SFP/SFP+ connected to the analyzer.

The state is also shown in the bottom-left corner.

- Linking indicates that the peer is getting an IP address and connecting to the network.
- Ready indicates that the peer is ready to exchange traffic with the source.
- Running indicates that traffic is being exchanged.

Note

You must leave the OneTouch on the PERFORMANCE PEER screen while using it as a peer.

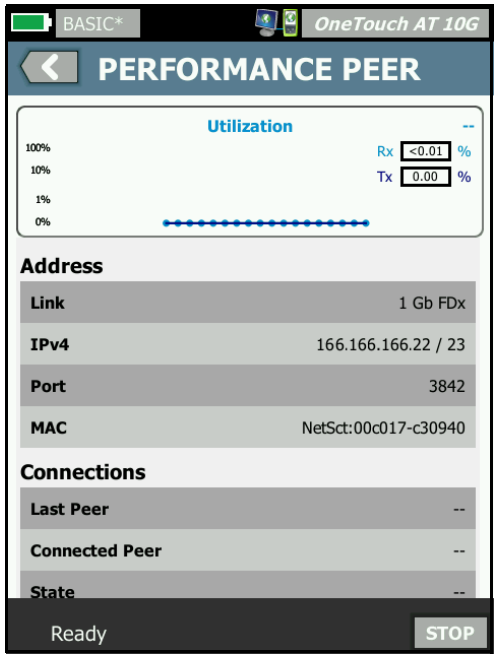


Figure 40. Performance Peer Screen

To Configure a OneTouch AT 10G Analyzer as the Source

Follow these steps to configure the source OneTouch AT 10G for the 1G Wired Performance (RFC 2544) test.

1 Connect AC power to the analyzer. This ensures that the unit will not run out of battery power, and will not automatically power-down if a Timeout Period is set.

2 Create a 1G Wired Performance (RFC 2544) test, and view its setup tab. See "Adding User Tests" on **page 49**.

3 Select the configuration values in the SETUP tab of the test. In particular, set the **Type** value to Peer. See "SETUP Parameters" on **page 105** for definitions of configuration parameters.

4 Run the test individually or as part of a test profile. See "Run the Test" on **page 113** for more information.

Test results are described in "Results" on **page 114**.

To Configure a LinkRunner AT (2000) as a Reflector

You can configure the LinkRunner AT as a reflector for OneTouch AT 10G.

Note

The LinkRunner AT 2000 Reflector feature only operates on a full duplex link.

1 Connect the AC adapter to the LinkRunner AT (2000) or ensure that the battery has enough charge to complete the test.

2 On the LinkRunner AT 2000 home screen, select **Tools**.

3 Select **General Configuration**.

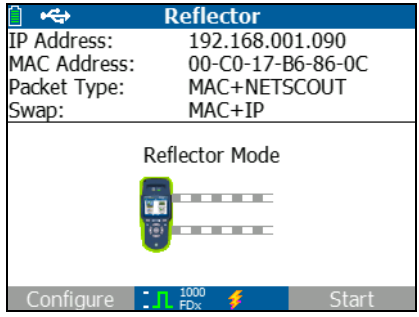
4 Under the Manage Power section, ensure that the **Auto Shutoff Enabled** check box is unchecked. This will prevent the LinkRunner from powering down while reflecting traffic.

5 Select **Save**.

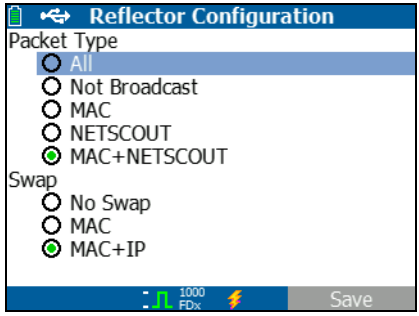
6 In the Tools menu, select **Reflector**. The LinkRunner will acquire an IP address. Note the IP address. You will enter this address when setting up the source analyzer.

If the tester does not acquire an IP address, go to the **Tools > IP Configuration** screen and verify that DHCP has been selected or

a static IP address has been entered.



7 Select **Configure**. The default reflector settings are displayed below. These settings are required for the Wired Performance test.



MAC + NETSCOUT - This filter setting allows the LinkRunner to only reflect frames when the destination MAC address field matches the LinkRunner's own MAC address and NETSCOUT payload.

MAC + IP - This swap setting allows the LinkRunner to swap the source and destination MAC and IP addresses for frames that are reflected back to the analyzer.

Caution

Any other LinkRunner Reflector settings may cause undesired traffic on your network.

8 Select **Save**.

9 Select **Start** (F2 button) to run the Reflector. It will run until Stop is pressed or link is dropped.

Refer to the LinkRunner AT User Manual for additional information.

To Configure a LinkRunner G2 as a Reflector

1 Connect the AC adapter to the LinkRunner G2 or ensure that the battery has enough charge to complete the test.

2 Start the LinkRunner G2 testing application.

3 To open the Reflector screen, touch the navigation menu icon at the top left of the LinkRunner G2 application screen, and then touch **Reflector**.

4 The LinkRunner will acquire an IP address. Note the IP address. You will enter this address when setting up the source analyzer.

5 Configure the **Packet Type** and **Swap** settings as required. The default settings **Packet Type: MAC + NETSCOUT** and **Swap: MAC + IP** are recommended.

Caution

Any other LinkRunner Reflector settings may cause undesired traffic on your network.

6 To start the Reflector, tap the purple Floating Action Button (FAB) at the lower right on this screen.

Refer to the LinkRunner G2 User Guide for additional information.

To Use the NETSCOUT Network Performance Test (NPT) Reflector Software

Note

The Reflector software has been tested on Windows 7, 8, 10, and Server 2012.

1 Download the free NETSCOUT NPT Reflector software onto a PC:

- Download from **http://enterprise.netscout.com/support/downloads**
- Or enter the OneTouch's Management Port IP address into a web browser to download the NPT Reflector Software from the OneTouch Web Server. See "Remote File Access Using a Web Browser" on **page 236.**

2 Install the Reflector on your PC by running the .exe file.

3 Open the Reflector application.

Once the Reflector application is installed and opened on your PC, it automatically detects available network interfaces and their link status.

4 Check the box next to **Enable Reflection** for each network interface you want to use as a Reflector for your network performance test.

5 Leave the Reflector application window open on your PC during testing.

Refer to the Help in the NPT Reflector software for additional information.

Run the Test

To run the test, ensure that you have started the endpoint (or configured it for AutoStart if available). Then, on the source OneTouch, start the Wired Performance Test by tapping AutoTest or TEST AGAIN on the Wired Performance Test RESULTS tab.

How it Works

A TCP control connection is established on the port that is specified in the test configuration. A UDP connection is established on the next higher port number (configured port + 1) for test traffic flow. On the next higher port (configured port + 2) a UDP connection is established for exchanging latency measurement frames.

When using a peer endpoint (a OneTouch AT 10G or OneTouch AT analyzer), separate upstream and downstream measurements

are provided for rate, frames sent, frames received, and lost frames. Latency and jitter measurements are always made on the roundtrip.

When using a reflector endpoint all measurements are made on the roundtrip.

Results

The test will fail if the upstream or downstream connection fails or cannot be established, or if the configured Allowed Loss value is exceeded.

When you select a frame size other than "RFC 2544 sweep" in the test configuration, the results screen looks like the image below.

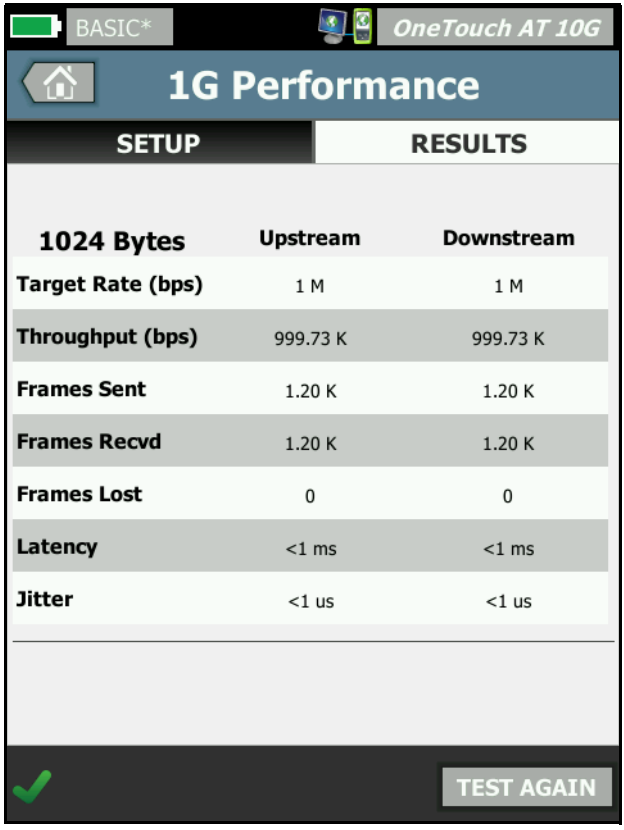


Figure 41. 1G Wired Performance Test (RFC 2544) Results Using a Single Frame Size

When you select Sweep in the frame size configuration, an RFC 2544 sweep test is performed. By default, results are shown in tabular view. Scroll down to see all of the results.

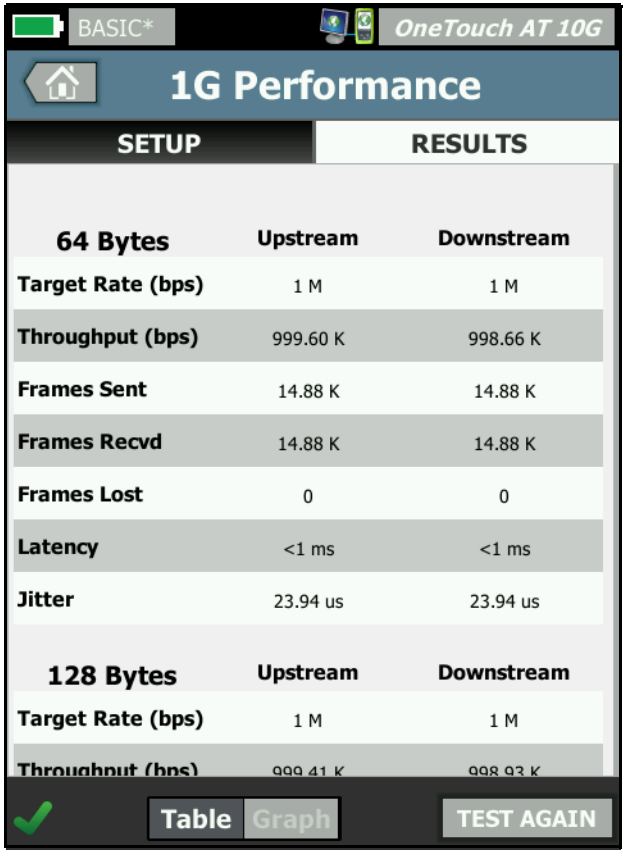


Figure 42. 1G Wired Performance Test (RFC 2544) Results RFC 2544 Sweep, Tabular View

You can also view the RFC 2544 sweep test results in graphical format. Tap the **Graph** button at the bottom of the screen.

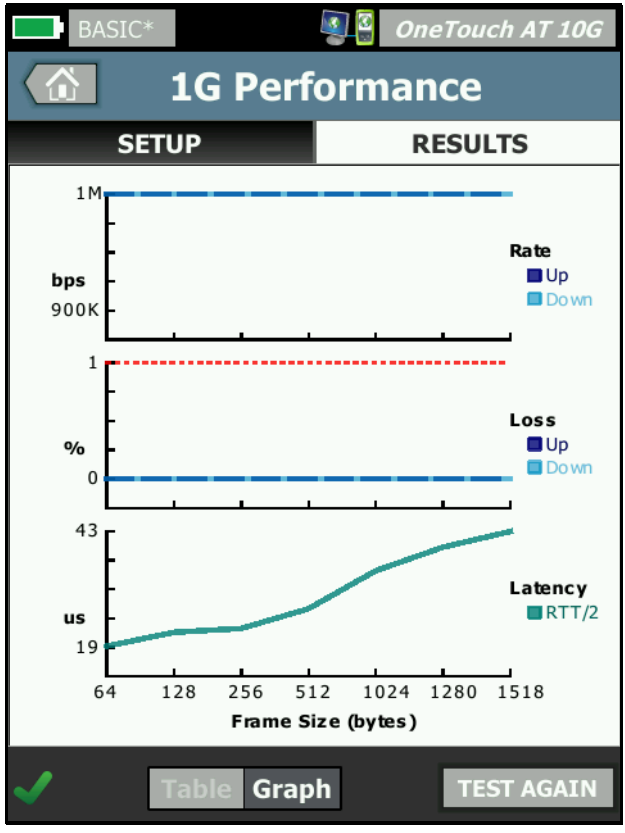


Figure 43. Wired Performance Test Results RFC 2544 sweep, Graphical View

Target Rate (bps) is the requested bit rate from the SETUP tab.

Throughput (bps) is the measured bit rate based on frames sent and the actual number of frames received. This rate includes inter-frame gap and preamble time.

Actual (bps) shows the actual utilized line rate in bits per second. This rate includes inter-frame gap and preamble time.

Frames Sent is the actual number of frames sent by the source.

Frames Recvd is the actual number of frames received at the source.

Frames Lost is the number of frames sent less the number of frames received.

Latency Measurement

Latency is measured from the time that the first bit of a latency frame is sent to the time that the last bit of that latency frame is received. The values shown are the average of 20 individual latency frame measurements.

Peer Latency Measurement - When using a peer endpoint, the delay that is introduced by the endpoint's turnaround time is subtracted from the measurement. The roundtrip time is measured, then divided by two to provide upstream and downstream values.

Reflector Latency Measurement - When using a reflector endpoint, the delay that is introduced by the endpoint's turnaround time cannot be measured. Therefore; it cannot be subtracted, and is included in the measurement.

Jitter Measurement

Jitter is a measure of the variation of frame-to-frame latency.

Peer Jitter Measurement - When using a peer endpoint, it is the average variation of twenty successive latency measurements.

Reflector Jitter Measurement - When using a reflector endpoint, jitter is the arithmetic range (the difference between the largest

value and the smallest value) of variation in twenty successive latency measurements.

Total Time is the total amount of time it took to complete the test.

At the bottom-left corner of the source's screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test.

10G Wired Performance Test (Y.1564)

Purpose

The 10G Wired Performance (Y.1564 compatible) test provides point-to-point performance testing of a traffic stream across a wired IPv4 network infrastructure. This test is typically used to validate network performance of newly provisioned links up to 10 Gbps and to assess existing or new services, such as VoIP. It quantifies network performance in terms of throughput, loss, latency, and jitter.

The 10G Wired Performance (Y.1564 compatible) test allows two *source* test suite configurations:

- If you set up a test suite on the OneTouch AT 10G, you can perform a simple throughput test to measure Throughput, Frame Loss, Latency, and Jitter.
- If you choose a test suite that has been configured on an OptiView XG, you can perform a more complicated performance test by using a test suite from the OptiView XG to validate that QoS has been properly configured within the network under test. Up to four Services can be configured to run concurrently to test service performance in the presence of background traffic. These services can be configured for different VLANs, VLAN priority, TOS/DSCP, IP Address, and Port number to conform to the way QoS is provisioned in the network. The analyzer exchanges up to four streams of traffic with the OptiView XG at a full line rate of up to 10 Gbps for performance validation, or at lower speeds to minimize disruption when troubleshooting operational networks.

The test is based on the ITU-T Y.1564 Ethernet Service Activation Test Methodology.

See "How it Works" on **page 133** to learn more.

Configuration

Network performance is measured between two points. Therefore, configuration includes setting up both the source and endpoint analyzers. The source is the OneTouch AT 10G analyzer on which the test is configured and controlled. For this test, there are three possible endpoint types:

- An **OptiView XG** that is appropriately connected and configured to receive instructions from a OneTouch AT 10G.
- A **Peer** OneTouch AT 10G.
- A **Reflector** that is either a NETSCOUT LinkRunner or NETSCOUT NPT Reflector software installed on a PC.

When an OptiView XG is used as the endpoint, the OneTouch AT 10G tester initially operates as the controller, then transfers control to the OptiView XG - the OneTouch 10G then operates as a Performance Peer. Note that separate upstream and downstream measurements are shown for throughput, frames lost, and jitter, while latency shows results based on roundtrip traffic/packets.

When another OneTouch 10G is used as a Peer endpoint, the source OneTouch 10G maintains control of the performance test, and the peer OneTouch 10G displays the Performance Peer screen (see **Figure 40**).

When a LinkRunner or NETSCOUT NPT Reflector software is used as the Reflector endpoint, the source OneTouch 10G maintains control of the performance test, and the Reflector simply displays the Reflector mode screen. When using a reflector, upstream and downstream traffic are not individually measured. Results are based on roundtrip traffic, and only one rate can be specified.

Note

For information on obtaining the Reflector PC application, see "To Use the NETSCOUT Network Performance Test (NPT) Reflector Software" on **page 112***.*

OptiView XG Endpoint SETUP Parameters

This section describes the SETUP tab of the 10G Wired Performance (Y.1564) test when using an OptiView XG as the endpoint.

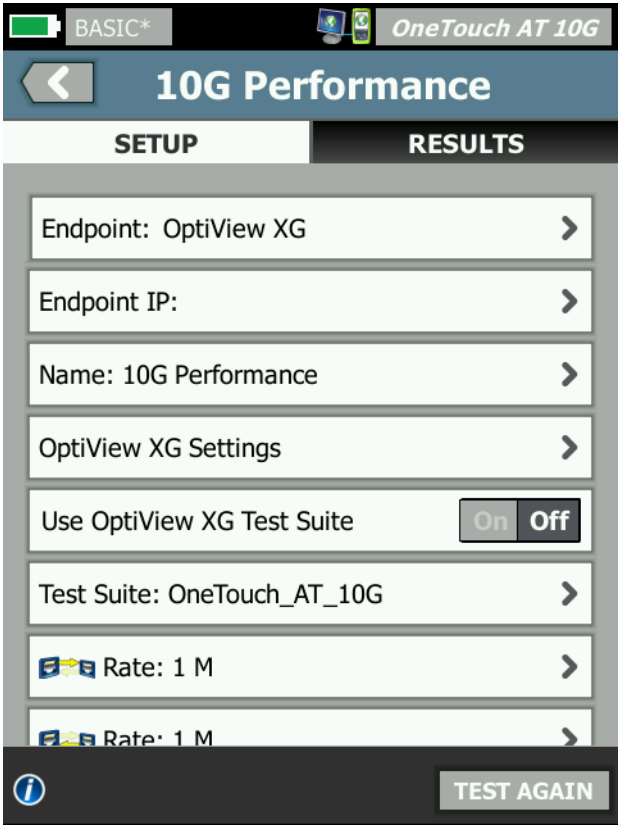


Figure 44. 10G Wired Performance Test Setup Tab Using OptiView XG

Endpoint - Specifies the type of endpoint to be used: **OptiView XG**, **Peer**, or **Reflector**.

Endpoint IP - Specifies the IP address of the endpoint that is used in the test.

Name - Names the test. This name will be seen on the Home Screen and in reports.

OptiView XG Settings - Specifies the user name, password, and encryption key required for the OneTouch analyzer to communicate with the OptiView XG. You set these values to match what has already been configured on the OptiView XG. This setting is used only when accounts and/or encryption are enabled on the OptiView XG.

Use OptiView XG Test Suite - Turn this on when you want to use a specific test suite that exists on the OptiView XG. Turn it **Off** when you want to set the configuration parameters on the OneTouch to run a simple version of the 10G Wired Performance (Y.1564) test. See "How it Works" on **page 133** to learn more about test suites. When this feature is turned **On**, only the **Test Suite** and **Port** parameters are available.

Note

The Test Suite must be configured appropriately to work as a 10G Y.1564 Performance test. See "How it Works" on **page 133** *for more information.*

Test Suite - Specifies the name of the test suite on the OptiView XG that will be used.

- If the OneTouch AT 10G can connect to the OptiView XG, when you tap this button, the list of Test Suites saved on the OptiView XG will appear. You can then select a Test Suite that has already been named on the OptiView XG.
- If the OneTouch AT 10G cannot connect to the OptiView XG, a keyboard will appear, allowing you to enter the name of the of the Test Suite you plan to use.

Note

The rest of the configuration parameters for an OptiView XG endpoint are not visible when the ***Use OptiView XG Test Suite*** *option is turned on.*

 **Rate** - Configures the desired bit rate of upstream traffic (from the source analyzer to the peer). Valid rates are from 100 Kbps to 10 Gbps.

 **Rate** - Configures the desired bit rate of downstream traffic (from the peer to the source analyzer). Valid rates are from 100 Kbps to 10 Gbps.

Duration - Configures the desired duration of the test.

Interval - Determines how often the display of the OneTouch AT 10G is updated. Data points are also collected every Interval on the OptiView XG to create a trend.

Frame Size - Configures the desired / expected frame size of transmitted and received traffic.

Loss Limit - Configures the frame / packet loss percentage lower limit below which the test will fail.

Latency Limit - Configures the frame / packet latency (in milliseconds) upper limit above which the test will fail.

Jitter Limit - Configures the maximum jitter level (in milliseconds) above which the test will fail.

Port - Configures the UDP port number used by the OneTouch AT 10G. The default value is 3842.

Peer and Reflector Endpoint SETUP Parameters

This section describes the SETUP tab of the 10G Wired Performance (Y.1564) test when using a Peer or Reflector as the endpoint.

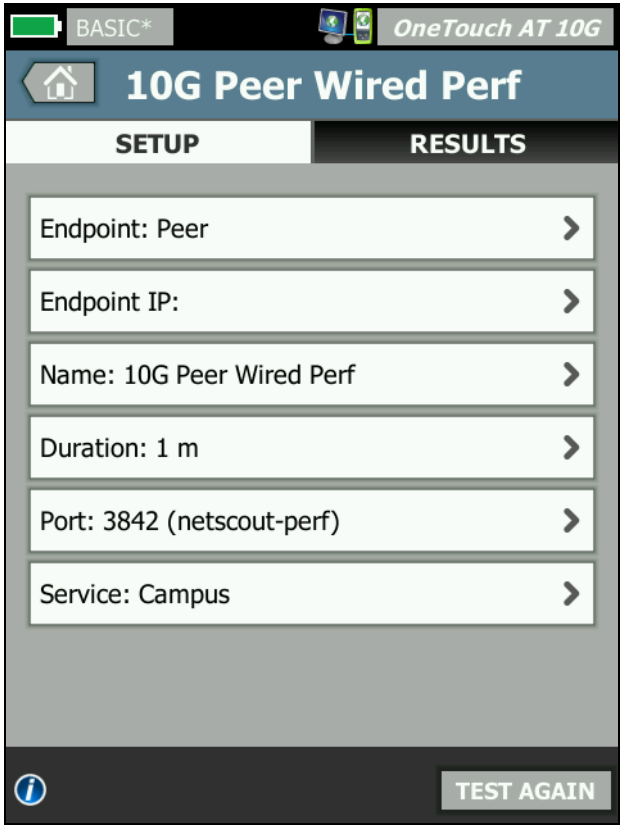


Figure 45. 10G Wired Performance Test Setup Tab Using Peer Endpoint

Endpoint - Specifies the type of endpoint to be used: **OptiView XG**, **Peer**, or **Reflector**.

Endpoint IP - Specifies the IP address of the endpoint that is used in the test.

Name - Names the test. This name will be seen on the Home Screen and in reports.

Duration - Configures the desired duration of the test.

Port - Configures the UDP port number used by the OneTouch AT 10G. The default value is 3842.

Service - Configures BASIC or ADVANCED Service options for the performance test.

- Tap the information icon next to each service parameter to view an explanation.
- Touch the DEFAULT SERVICE button to return all service parameters to the default configuration.
- When using a PEER endpoint, Bidirectional Traffic Flow, Upstream and Downstream Target Rates, and Upstream and Downstream Latency, Jitter, and Frame Loss thresholds are all configurable.
- When using a REFLECTOR endpoint, only the roundtrip Target Rate and Latency, Jitter, and Frame Loss thresholds are configurable.

Service Configuration for Peer or Reflector Endpoints

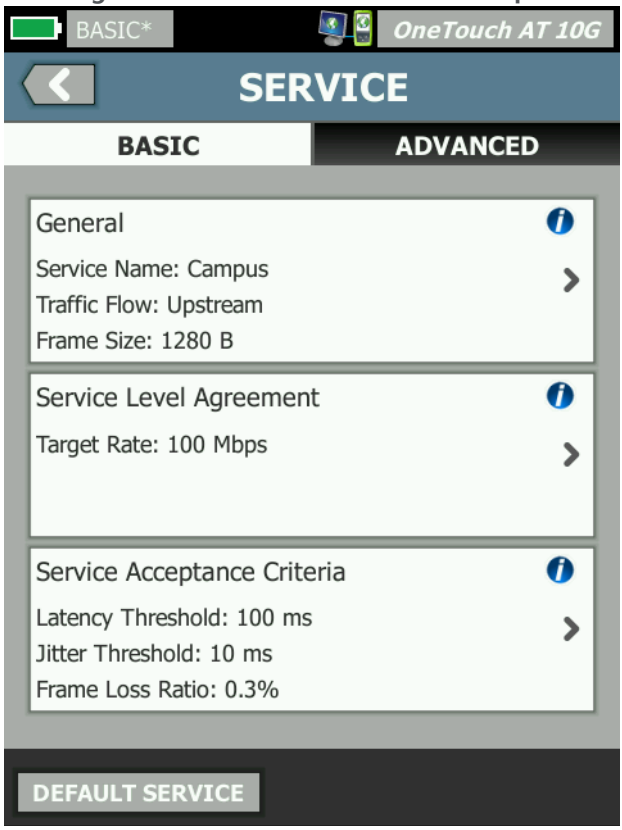


Figure 46. 10G Performance Peer/Reflector Service Configuration Screen

BASIC

General

Service Name - Enter a name for your Service parameters. It will appear on the RESULTS tab and in generated reports.

Traffic Flow - Define the direction of the data stream(s) to be tested. (4 options)

- Bidirectional: Apply different target rates to upstream and downstream testing, and compare each stream against the configured Service Acceptance Criteria (SAC).
- Bidirectional (same up/down values): Apply the same target rate to both upstream and downstream tests, and compare both against the SAC.
- Upstream: Apply the same target rate to both upstream and downstream, but only compare upstream against the SAC.
- Downstream: Apply the same target rate to both upstream and downstream, but only compare downstream against the SAC.

Frame Size - Define the size of the test frame sent. (3 options)

- User Defined: Enter a frame size between 64 and 9300 bytes, or select one of the standard RFC 2544 frame sizes.
- RFC 2544 Sweep: Run 7 performance tests using each of the RFC 2544 frame sizes: 64, 128, 256, 512, 1024, and 1518 bytes.
- EMIX: Create test traffic with variable frame size patterns, generated in a repeating sequence. When selected, the Define EMIX keyboard displays. Each letter is associated with a size, as shown on the keyboard. Letter H uses the frame size set in the User Defined field on the Frame Size screen. Touch the letters to enter your desired frame size mix, up to 8 sizes. Touch DONE to save your mix. The sequence repeats during the performance test duration.

Service Level Agreement (SLA)

Enter or select a **Target Rate** for your performance test. The Target Rate is the average bit rate of transmitted or received frames, starting with the first MAC address bit and ending with the last frame check sequence (FCS) bit. On a 10-Gbps link, the actual achievable rate is less than 10 Gbps due to the Ethernet protocol overhead. Overhead is a significant part of a 64-byte packet but a less significant part of a 1518-byte packet.

Service Acceptance Criteria (SAC)

Define the Latency, Jitter, and Loss thresholds for your performance test. These performance parameters determine the Pass/Fail criteria for the test. Statistical results for each parameter

are displayed on the Performance Test RESULTS screen and in generated reports.

- Latency Threshold: Enter or select a maximum allowed latency in milliseconds (ms). Also called Frame Transfer Delay, Latency is the amount of time it takes for a packet to travel from the source to the destination. To display the one-way delay, OneTouch 10G measures the roundtrip time for a packet to travel to the endpoint and back, and then divides that value by two. The test fails if the measured average latency (for a 1-second sample interval) exceeds the Latency Threshold.
- Jitter Threshold: Enter or select the maximum allowed jitter in milliseconds (ms). Jitter is a measure of the variation in packet-to-packet latency. The test fails if the measured average jitter (for a 1-second sample) exceeds the Jitter Threshold.
- Frame Loss Ratio Threshold: Enter or select the maximum allowed frame loss, expressed as a percentage of total frames (number of frames transmitted, minus number of frames received, divided by total transmitted frames). The test fails if the measured frame loss exceeds the Frame Loss Ratio Threshold.

ADVANCED

Layer 2 Frame Options

Use these options to test VLAN priority on your network.

- Override VLAN Priority: Create a traffic stream to verify that loss does not occur on the higher priority system. VLAN priority is set to 0 (Best Effort) by default. You can alter the VLAN priority to simulate a type of traffic stream (e.g. voice or video).
- Validate VLAN Priority: Switch ON to check that received packets maintained the same priority field from the source to the destination. If the priority field changes, packets are counted as lost.
- Override VLAN: Switch ON to tag test frames with a specific VLAN (e.g. a VLAN used for voice, video, or data) to simulate a type of traffic stream. If you override the VLAN ID, you must configure the IP address in the Layer 3 Frame Options for the VLAN's subnet address range, and you may need to override the destination MAC for the first hop router.

- Override MAC: If necessary, switch this setting ON to specify a first hop router other than the default router or when no default router exists. Use this setting in conjunction with overrides for IP Address or VLAN ID. Enter the correct MAC address for the router or endpoint if both endpoints reside in the same IP subnet. When left blank, the default MAC address of the endpoint is used.

Layer 3 Frame Options

Use these options to test QoS on your network. You can create a traffic stream to verify that loss does not occur on a higher priority stream.

- QoS with DSCP or IP Precedence: Select the methodology used on your network - QoS with DSCP (Type of Service with Differentiated Services Code Point) or QoS with IP Precedence (legacy).
- Validate QoS: Switch ON to check that received packets maintained the same QoS field from the source to the destination. If the QoS field has changed, packets are counted as lost.
- Override IP: Switch ON to manually designate the source IP address of the generated test traffic. Use this setting to simulate traffic from a certain device (e.g. a VoIP phone). This setting is often used in conjunction with a VLAN ID override. When OFF, the IP address of the Network Under Test port is used.

To Run the 10G Wired Performance Test Using an OptiView XG Endpoint

You can run either a simple throughput test with default test parameters to measure throughput, frame loss, latency, and jitter, or you can run a more complex text suite (set up on the OptiView XG) as described earlier.

Note

If you intend to run a more complex test suite that has already been set up on the OptiView XG, please first read "How it Works" later in this section.

1 Connect and configure the endpoint OptiView XG. Refer to the OptiView XG's Getting Started Guide and online Help for detailed procedures. Pay particular attention to the following:

- **Connect:** Physically connect your OptiView XG to the network. Power it on. And if the OptiView XG is at a remote location, ensure it is powered with its AC adapter.
- **Configure:**
  - The OptiView XG must be configured to allow Remote UI connections.
  - Note whether the OptiView XG has encryption and user accounts enabled. You will need this information for the OneTouch AT 10G configuration.
  - IF the OptiView XG has user accounts enabled, the user account on OptiView XG must be configured to allow Remote UI and Performance Tests.
- **Results/File Management:** The test causes a new test suite to be created and/or overwritten on the OptiView XG. See "How it Works" on **page 133** to learn more.
- **Ports and Firewalls:** The following ports must be open in firewalls between the OneTouch and the OptiView XG:
  - TCP port 1695.
  - UDP port number to match the **Port** value set on the OneTouch and OptiView XG. The default is 3842.

2 Connect AC power to the OneTouch AT 10G analyzer. This ensures that the unit will not run out of battery power, and will not automatically power-down if a Timeout Period is set.

3 On the OneTouch AT 10G, press and hold one of the test tiers to open the ADD TEST screen. Tap the 10G Wired Performance (Y.1564) test.

4 Set the test parameters described in the previous section. In particular, you will set **Use OptiView XG Test Suite** to Off if you want to create a new simple performance test, or On if you want to run a more complex performance test suite that already exists on the OptiView XG.

5 Run the test individually or as part of a test profile. See "Run the Test" on **page 133** to learn more. Link will automatically be established if you have not yet run AutoTest (which establishes link). It may take up to a minute to establish link.

6 Tap the Results tab when the test is finished to see test results. Go to "Results" on **page 135** to learn more.

To Run the 10G Wired Performance Test Using a Peer or Reflector Endpoint

1 Physically connect your source and peer OneTouch AT 10G units to the network. Power them on, and ensure they are powered with an AC adapter.

2 Configure your Endpoint:

- **For a Peer Endpoint:** Configure the endpoint OneTouch 10G to act as a Performance Peer. See “To Configure a OneTouch AT Analyzer as a Peer” on **page 107.**
- **For a LinkRunner AT Reflector Endpoint:** Configure the endpoint LinkRunner AT to act as a Reflector. See “To Configure a LinkRunner AT (2000) as a Reflector” on **page 110.** If needed, refer to the LinkRunner AT Network Auto-Tester User Manual for information on configuring advanced network settings. Download it from **http://enterprise.netscout.com/support/manuals**.

- **For a LinkRunner G2 Reflector Endpoint:** Configure the endpoint LinkRunner G2 to act as a Reflector. See “To Configure a LinkRunner G2 as a Reflector” on **page 112.**
- **For NETSCOUT NPT Reflector software installed on a PC:** Configure the software as required, referring to the software’s included Help. Note the IP address of the network interface on which you want to run the test, and enter it into the **Endpoint IP** field on the source OneTouch 10G. See “To Use the NETSCOUT Network Performance Test (NPT) Reflector Software” on **page 112.**

3 On the OneTouch AT 10G, press and hold one of the test tiers to open the ADD TEST screen. Tap the 10G Wired Performance (Y.1564 compatible) test.

4 Set the test parameters described in the previous section, "Configuration" on **page 121**.

5 Run the test individually or as part of a test profile. See "Run the Test" on **page 133** to learn more. Link will automatically be established if you have not yet run AutoTest (which establishes link). It may take up to a minute to establish link.

6 Tap the Results tab when the test is finished to see test results. Go to "Results" on **page 135** to learn more.

Run the Test

To run the test, ensure that you have started the endpoint, then start the 10G Wired Performance (Y.1564) test (on the source OneTouch AT 10G) by tapping AutoTest or TEST AGAIN on the test RESULTS tab.

How it Works

When using an OptiView XG as the endpoint, the 10G Performance (Y.1564) test works like this:

1 **You configure the test** either...
- by setting up specific test parameters on the *source* OneTouch AT 10G (a simple performance test), or...
- by selecting a test suite on the *peer* OptiView XG (typically, a more complex test).

2 **When the test is executed,** usually as part of a OneTouch AT 10G test profile and an AutoTest run, the following operations take place:

- A test suite is created on the OptiView XG.
- If a test suite from the OptiView XG is used:
  - The selected test suite's configuration is copied to a new test suite with "_OneTouch_AT_10G" appended to its name.
  - You can select ANY test suite on the OptiView XG but it must contain, at most, one active endpoint and four active Services.
  - The test suite you select is not altered.
- If a "simple" performance test is used, the configuration settings and the name entered on the OneTouch AT 10G are transferred to the OptiView XG.
  - If the test suite above already exists on the OptiView XG (from a previous run), its configuration and test results (on the OptiView XG) are overwritten.
- In all cases, the new test suite is populated with the endpoint address and port number of the *source* OneTouch AT 10G.

3 **A remote UI channel is opened between the OneTouch AT 10G and the OptiView XG**, and the OneTouch hands over control of the test to the OptiView XG. The OptiView XG then behaves as a source, running a standard performance test, with the OneTouch acting as a peer. Then:

- According to the Y.1564 specification, an initial short configuration test is run for the upstream and downstream traffic of each service to validate that the service is properly configured and provisioned before committing to the full duration of the performance test. This initial configuration test stage can be observed in the status line of the 10G Performance Test (Y.1564) Results tab. The full results of the configuration tests can be viewed on the OptiView XG.
- After the configuration tests pass, the full performance test runs. At the end of every test interval, the average of Throughput, Frame Loss, Latency, and Jitter for all intervals is updated on the Results tab of the 10G Performance (Y.1564) test and a new trended data point is created on the OptiView XG.
- When the test completes, an overall Pass/Fail indication is given. Any values that caused the measurement to fail are indicated on the Results tab of the 10G Performance (Y.1564) test.

When using a Peer or Reflector as the endpoint, the source OneTouch 10G maintains control of the performance test while the Peer or Reflector device simply reflects the data packets at the rate at which it is capable of sending data. Results are displayed on the source OneTouch AT 10G.

Results

Test results for the 10G Performance (Y.1564) test are displayed in multiple stages.

Figure 47 shows the RESULTS tab right after the test is started. The initial configuration test runs with the status shown in the lower left portion of the screen.

No test results are reported during this phase of the test.

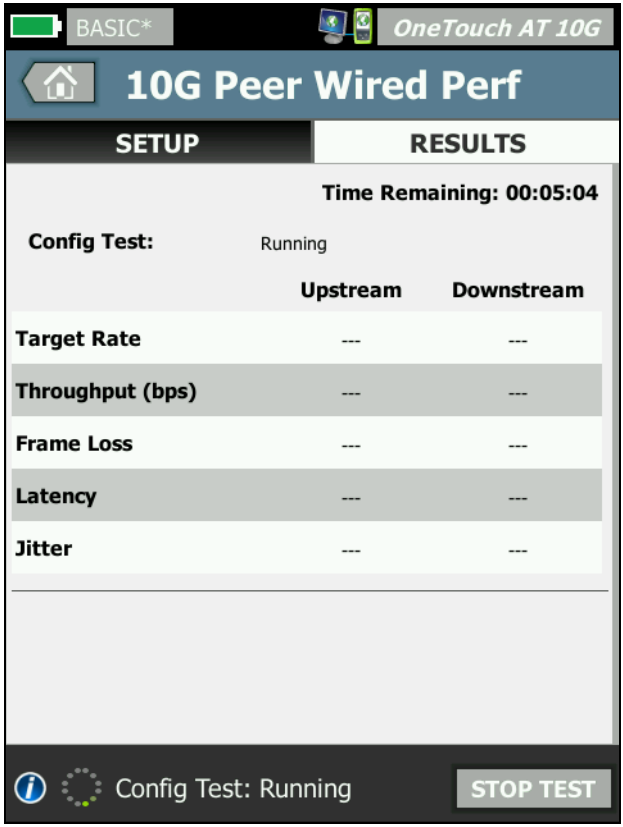


Figure 47. 10G Performance (Y.1564) test - initial configuration test phase

After the initial configuration test runs and passes, the full performance test runs. At the end of every test interval, the average of throughput, frame loss, latency and jitter for all

intervals, and for services being tested, is updated on the RESULTS tab.

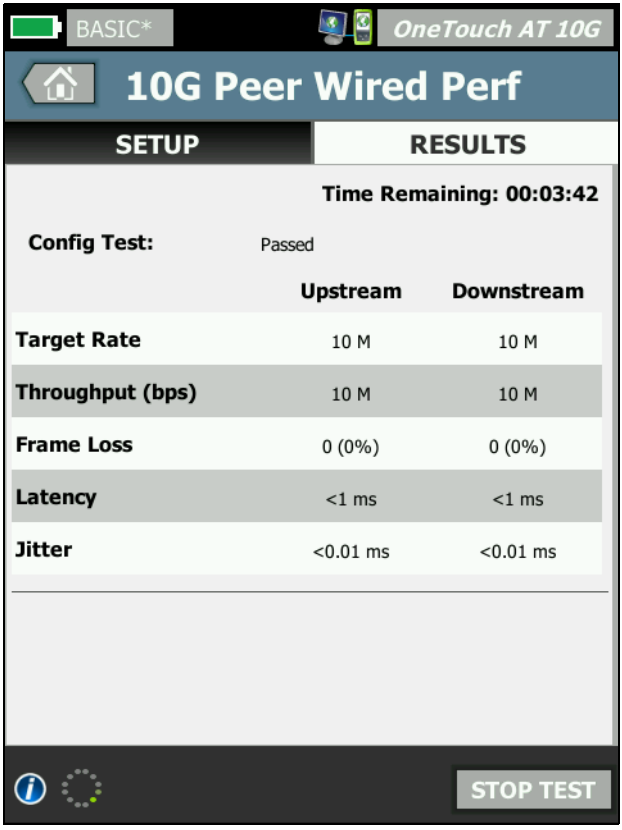


Figure 48. 10G Performance (Y.1564) test - full performance test phase

The following test results start accumulating once the full performance test phase begins.

Target Rate is the requested bit rate from the SETUP tab.

Throughput (bps) is the measured bit rate based on frames sent and the actual number of frames received. This rate includes inter-frame gap and preamble time.

Frame Loss is the percentage of total frames sent that were not received back from the endpoint by the OneTouch 10G.

Latency is measured from the time that the first bit of a latency frame is sent to the time that the last bit of that latency frame is received. The values shown are the average of all latency frame measurements.

For this test, the delay that is introduced by the endpoint's turnaround time is subtracted from the measurement. The roundtrip time is measured, then divided by two to provide upstream and downstream values.

Jitter is a measure of the variation of frame-to-frame latency. For this test, jitter is measured one way in each direction.

At the bottom-left corner of the source's screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button TEST AGAIN to re-run the test.

Multicast (IGMP) Test 

Purpose

The Multicast (IGMP) test verifies the ability to subscribe to an IGMP multicast group and verifies the flow of multicast data to the OneTouch AT 10G analyzer. Multicasts are used for online streaming of data from devices such as security video cameras, industrial sensors, and ticker tape data.

The test verifies the availability of the multicast group and port, as well as the provisioning of multicast support along the route, such as IGMP snooping in switches.

Configuration

IGMP Group is the IP address of the multicast group.

The **Name** button allows you to assign a custom name to the test. See also: "Name" on **page 84**.

Transfer Size and **Time Limit** - The test will end when the selected Transfer Size has been streamed or when the time limit has been reached.

- If the Transfer Size has not been streamed before the Time Limit is reached, the test will fail.
- If the Transfer Size is **Unlimited**, the test will run until the time limit is reached.
- If the Time Limit is **None**, the test will run until the amount of data specified by the Transfer Size setting has been streamed.
- If you select no time limit and unlimited transfer size, the test will not automatically end.

Port is the UDP port on which the multicast is received.

Version - If IGMP traffic other than the specified version is received, the test will fail. Note that in IGMPv3 the multicast source may be specified, thereby reducing the risk that an unauthorized party could supply the multicast data.

How it Works

The analyzer joins the specified multicast group and listens for traffic. If a source address is specified, it will only listen for traffic from that IP address. The test runs in turn on each configured network connection.

Results

Pass/Fail conditions are described in “Transfer Size and Time Limit” and in “Version” on page 139.

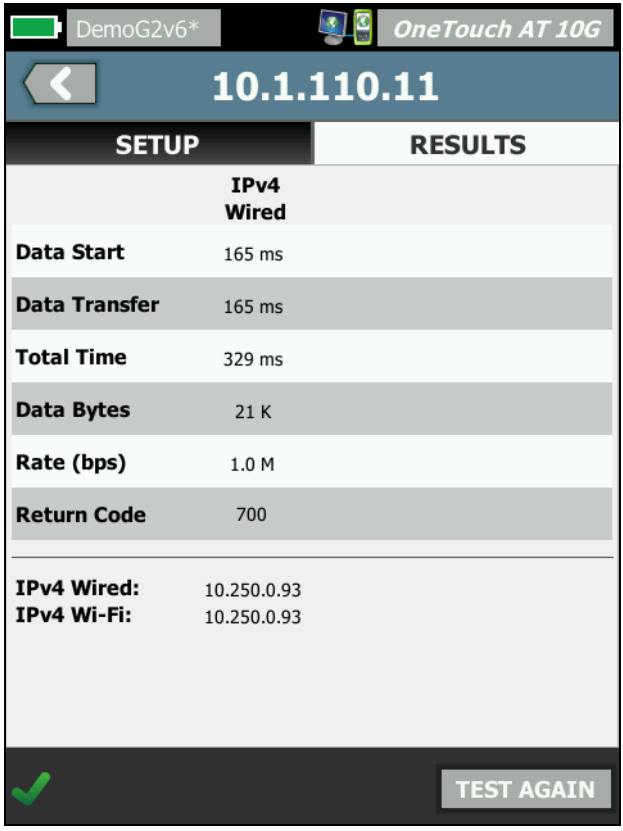


Figure 49. Multicast (IGMP) Test Results

Data Start is the amount of time it took to receive the first data byte after the analyzer sent the IGMP join message.

Data Transfer is the amount of time it took to receive the data from the target server.

Total Time is the sum of data start and data transfer time. It is the total test time from beginning to end.

Data Bytes indicates the total number of data bytes transferred.

Rate is the measured bit rate, based on frames sent and the number of bytes received.

If a source address is specified a ping test runs simultaneously with the IGMP V3 test. If the IGMP V3 test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test.

Video (RTSP) Test 

Purpose

The Video (RTSP) test verifies the ability to access video content from on-demand streaming media servers. The test uses the RTSP protocol to establish and play the designated video file from the specified RTSP Server. The target server can be an IPv4 address, IPv6 address or named server. The test verifies the ability to playback the specified media file from the server using the designated Port.

Configuration

Server - Enter the URL or the IP address of the target server. See also: “Server” on **page 84**.

The **Name** button allows you to assign a custom name to the test. See also: “Name” on **page 84**.

Transfer Size and **Time Limit** - The test will end when the selected Transfer Size has been streamed or when the time limit has been reached.

- If the Transfer Size has been streamed before the Time Limit is reached, the test will pass.
- If the Transfer Size has not been streamed before the Time Limit is reached, the test will fail.
- If the Transfer Size is **All**, the test will run until the time limit is reached or until the entire stream is received, and the test will pass.
- If the stream is interrupted, the test will fail.

Port specifies the port on which RTSP communication will be established. RTP is automatically set up using port 1386 for Data and 1387 for Control.

File is the name of the file that will be received (streamed).

How it Works

The analyzer requests a session with the RTSP server. The file specified on the **File** button is streamed to the analyzer. The amount of data streamed is checked against the specified Transfer Size and Time Limit to determine whether the test passed or failed. The streamed file is not saved.

Results

If the Transfer Size has not been streamed before the Time Limit is reached, the test will fail.

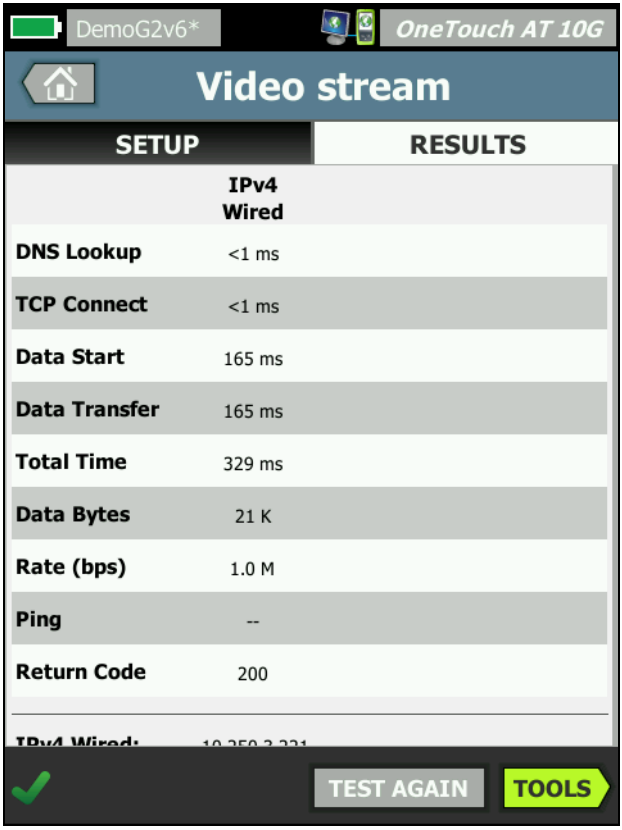


Figure 50. Video (RTSP) Test Results

DNS Lookup is the amount of time it took to resolve the optional URL into an IP address.

TCP Connect is the amount of time it took to open the port on the server.

Data Start is the amount of time from when the port was opened until the first video data was received. This is commonly referred to as "Zap Time."

Data Transfer is the amount of time it took to receive the data from the target server.

Total Time is the amount of time it took to transfer the video file to the analyzer. It is the sum of DNS lookup, TCP connect, data start time, and data transfer.

Data Bytes indicates the total number of data bytes transferred.

Rate is the measured bit rate, based on frames sent and the number of frames received.

A ping test runs simultaneously with the RTSP test. If the RTSP test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered.

Below the Return Code, the target server addresses are displayed. If you specified a target server's URL, these addresses were supplied by DNS servers.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button TEST AGAIN to re-run the test. Tap the **TOOLS** button TOOLS to run path analysis to the target server,

launch a browser against the target server, or Telnet/SSH to the server.

Email (SMTP) Test 

Purpose

The Email (SMTP) test provides digital notification of wired connectivity using SMTP mail service.

This test is useful for sending a text message to the user's phone for complete Internet connectivity feedback, or allowing a test supervisor to maintain a repository of all analyzer testing being performed in the field. The message identifies the analyzer being used, and the wired link used such as the nearest switch.

The SMTP Server may be a private server or a universally available free email service such as Gmail. Refer to the SMTP service provisioning information for the SMTP server name and port.

Configuration

SMTP Server - Enter the name of the SMTP mail server that will process the email.

The **Name** button allows you to assign a custom name to the test. See also: “Name” on **page 84**.

Time Limit - The amount of time allowed for the SMTP server to acknowledge that the email was successfully sent.

From Email - If your SMTP server blocks invalid addresses, this will need to be a valid address. Otherwise, any name is acceptable. This address will appear in the from field of the email that the analyzer will send.

To Email - Enter the recipient’s address here.

SMTP Server Port - Usually port 25 for non-SSL, or port 587 for SSL/TLS.

Login - If the SMTP server requires authentication, set **Login** to **On** and enter the username and password.

How it Works

The analyzer adds the nearest switch information to the body of the email if it is sent via the wired interface. The analyzer looks up the SMTP server name, contacts the server, sets up SSL or TLS communications if necessary, authenticates if necessary, and uses the SMTP protocol to send the email. The SMTP protocol provides confirmation that the email was sent, and provides a return code if an error occurs. Additional verification of test success is available by checking the inbox of the email account you specified in the **To Email** setting.

Results

Results provide a complete breakdown of the total time it took to send the email.

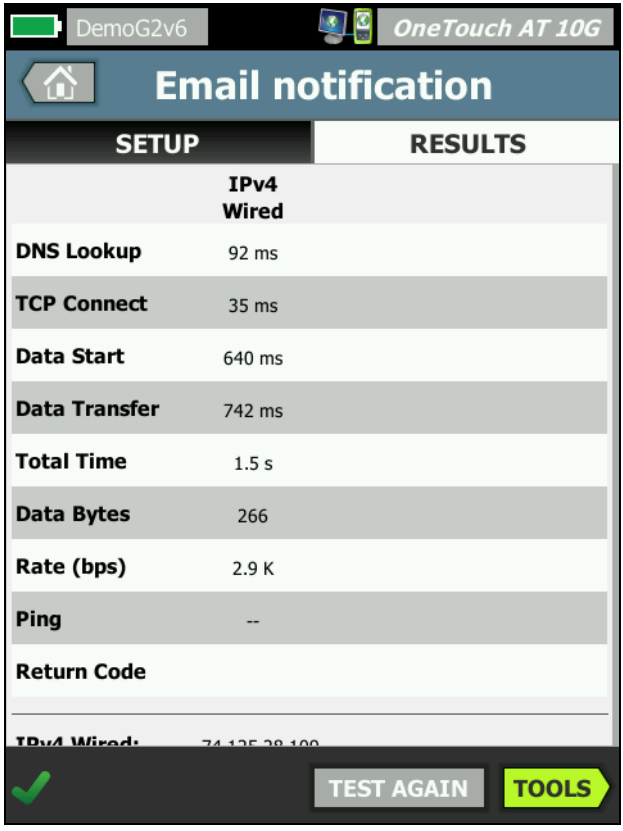


Figure 51. Email (SMTP) Test Results

DNS Lookup is the amount of time it took to resolve the optional URL into an IP address.

TCP Connect is the amount of time it took to open the port on the server.

Data Start is the amount of time from when the port was opened until the server allowed the email to be uploaded.

Data Transfer is the time it took to send the email header and payload to the target server.

Total Time is the sum of DNS lookup, TCP connect, data start, and data transfer time. It is the total amount of time it took to send the email from the analyzer.

Data Bytes indicates the total number of data bytes transferred.

Rate is the measured bit rate, based on frames sent and the number of frames received.

A ping test runs simultaneously with the SMTP test. If the SMTP test finishes before the ICMP echo reply packet arrives, dashes will be displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

Return Code specifies the end-of-test status or an error condition if encountered.

Below the Return Code, the target server addresses are displayed. If you specified a target server's URL, these addresses were supplied by DNS servers.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

Tap the **TEST AGAIN** button 

to re-run the test. Tap the **TOOLS** button 

to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

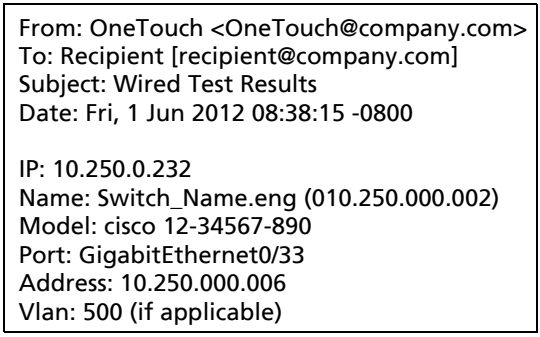


Figure 52. Email Sent From IPv4 Wired Connection

Chapter 6: Profiles

OneTouch AT 10G analyzer profiles are named configurations that can be used in a variety of ways to streamline analyzer operation. The use of profiles allows an organization to create standard test procedures that encapsulate expected network operation from any locale or segment.

The use of profiles to create standard work in an organization allows for a consistent and thorough testing process as well as allowing less skilled personnel to perform sophisticated network testing.

Profiles can be quickly recalled or managed by tapping the profile name in the title bar. Some possible uses of profiles include:

- Location based profiles that allow standard work from a given site or branch office by testing a combination of servers residing in the premise, private intranet, and public internet.
- Departmental profiles to encapsulate the network services and applications needed by a specific function in the corporation such as marketing, manufacturing or R&D.
- User type profiles such as testing guest login and expected network accessibility.
- End device emulation profiles such as emulating a VoIP phone by testing TCP port connectivity to the call manager. Additional features such as static addressing, VLAN membership and MAC spoofing can also be used to emulate network end points.
- Infrastructure testing for verifying specific network operation such as:
    - IP Surveillance testing using multiple IGMP multicast user tests.
    - Performance testing to verify acceptable bandwidth of the wired network.

Profiles are further customized by allowing the user test tiers to be named for the application. The tiers allow grouping of similar

tests to aid in network diagnostic triage. The default names "Private/Intranet" and "Public/Internet" can be modified by tapping the dividers and renaming for the application. For example, a manufacturing site test might rename the tiers "Production Floor" and "Back Office" and place the appropriate tests in their respective tiers.

All user-configurable aspects of the analyzer, with the exception of Maintenance Tools, are stored in Profiles.

Asterisk (*) After the Profile Name

- When you make changes to the current profile (add or modify tests, enter security keys, etc.) an asterisk appears after the profile name in the shortcut bar, indicating that changes have not been saved.
- If you cycle power, the OneTouch AT 10G analyzer will retain the changes and the asterisk will still be displayed. However, if you load a different profile before saving the current profile, the changes to the current profile will be lost.

Open the Profiles Screen

You can tap the Profile name, which is in the shortcut bar at the top of the screen.

Or you can tap the **Tools** icon  on the Home screen, then tap the **Profiles** button.

Save a Profile

To save a Profile:

1. Configure the analyzer as desired (add user tests, change settings, etc.).
2. Tap the Profile name, which is in the shortcut bar at the top of the screen.
3. Tap the **SAVE** button.

4 To create a new profile, enter its name and tap the **DONE** button. To use the existing name, tap the **DONE** button.

Load a Profile

After saving more than one profile, you can scroll through the list, select a profile, and tap the **LOAD** button on the PROFILE screen. After loading a Profile, run AutoTest to obtain test results.

Rename or Delete a Profile

Tap the **MANAGE** button on the PROFILE screen to rename or delete a profile.

Export and Import Profiles

To import or export a group of Profiles quickly, use FTP or the Cloud Service, or map the analyzer's user file system as a network drive.

- See "Remote File Access Using an FTP Client" on **page 237.**
- See "Remote Access from the Cloud" on **page 250.**
- See "Remote File Access Using a Mapped Network Drive (WebDAV)" on **page 238.**

To export a profile to a different OneTouch AT 10G analyzer using a USB flash drive:

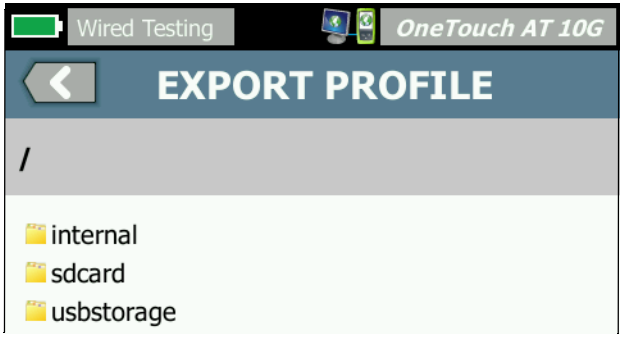
1 Connect a USB flash drive to the analyzer. (You must do this before tapping the **MANAGE** button in step 3 so the USB flash drive will appear on the list.)

2 Tap the Profile name, which is in the shortcut bar at the top of the screen.

3 Tap the **MANAGE** button.

4 Select the profile to export.

5 Tap the **EXPORT** button.



6 Tap **usbstorage**.

7 Tap **OK**.

8 Remove the USB flash drive from the source analyzer.

9 Connect the USB flash drive to the destination analyzer.

10 On the destination analyzer, tap the Profile name, which is in the shortcut bar at the top of the screen.

11 Tap the **MANAGE** button.

12 Tap the **IMPORT** button.

13 Navigate to the profile on the USB flash drive. Highlight the profile by tapping it.

14 Tap the **OK** button. The profile is saved to the analyzer in the /internal/Profiles directory.

To load the imported profile:

15 Tap the back button .

16 Select the imported profile.

17 Tap the **LOAD** button.

View a Profile File

To view a saved Profile, use one of the file management methods to open the Profiles directory, then select a Profile. (See “Managing Files” on **page 229.**) The Profile is a plain text file with a .profile extension that can be displayed in a web browser or a text editor.

Editing Profiles

You can edit and save Profiles using the OneTouch AT 10G analyzer. Profiles are not intended to be edited with a text editor. If they are edited outside the analyzer they cannot be used because they are protected by a checksum.

Chapter 7: Wired Analysis

Wired Analysis 

Description

The OneTouch AT 10G analyzer discovers...

- Devices in the broadcast domain
- Wi-Fi devices that are connected to APs in the broadcast domain
- The server specified in the DNS test
- The servers specified in user tests

Additional devices can be found through passive discovery.

When the analyzer is connected to a trunk port and is not configured for a VLAN, all devices on the trunk are discovered. When the analyzer is connected to a trunk port and is configured for a VLAN, only devices in the same VLAN are discovered.

Devices are categorized and displayed on the WIRED ANALYSIS screen.

A summary view of hosts, access devices, and servers provides an overview of devices on the network along with relevant details such as IP address, MAC address, switch slot and port, utilization, and problems.

Devices can be sorted according to IP address, MAC address, problems, utilization, or other attributes.

Tap a device on the summary list to view its details, such as its names, IP addresses, attributes (server type), SNMP information, and problems. From the device detail view of a device that is displayed on the HOST or ACCESS tab, you can tap TOOLS to:

- Add a new user test for the device.

- Scan the device for open ports.
- Run path analysis to the device.
- Launch a web browser using the device as the target.
- Open a Telnet/SSH session with the device.

Configuration

To configure wired analysis:

1 On the HOME screen, tap **TOOLS** .

2 Tap the **Analysis** button. The ANALYSIS setup screen is displayed.

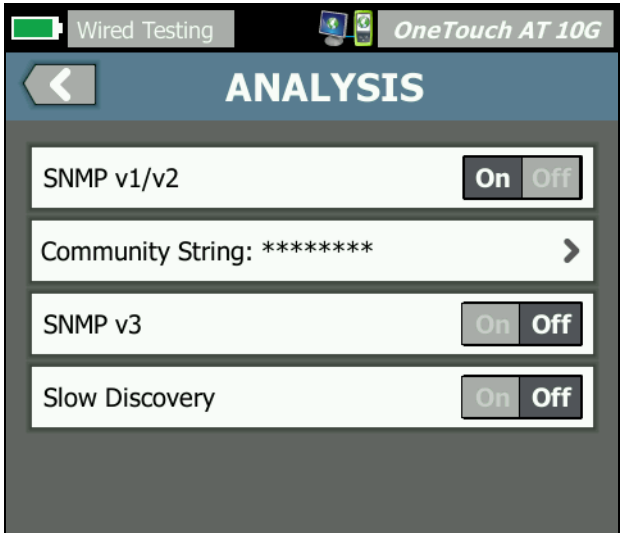


Figure 53. WIRED ANALYSIS Setup Screen

SNMP

To obtain the most complete wired analysis, configure SNMP v1/v2 community strings and SNMP v3 credentials. By default, the SNMP v1/v2 community strings are “public, private”.

1. On the ANALYSIS setup screen, tap the **SNMP v1/v2** button and enter community string(s). When entering multiple community strings, separate them with a comma and a space. For example: public, private.
2. You can view the characters as you enter them. See "Entering Passwords and Other Hidden Text" on page 35.
3. Tap the **SNMP v3** button and add v3 credentials.

Slow Discovery

By default, the analyzer probes the network to discover devices at the rate of 100 transmissions per second. Some intrusion detection systems may trigger an alarm and shut down the port when the analyzer probes at this rate. To slow the analyzer's discovery to 14 transmissions per second, set **Slow Discovery** to **On**.

How Wired Analysis Works

Wired analysis begins when you establish a copper or fiber Ethernet connection and start AutoTest.

Devices are discovered using active and passive analysis methods.

The analyzer classifies each device as soon as it is found. Each wired device is classified as a host, access device, or server.

During AutoTest, a DNS lookup is done for devices on the HOME screen that are identified by URL (e.g. www.google.com). The HOME screen devices and their IP addresses are included in Wired Analysis results

Results

The number of discovered devices is shown under the Wired Analysis icon  on the HOME screen. Tap the icon to display the WIRED ANALYSIS summary screen.

Figure 54. WIRED ANALYSIS Screen

① The HOSTS, ACCESS DEVICES, and SERVERS tabs let you filter the Wired Analysis results. Access devices are switches, routers, etc. The ALL DEVICES tab displays devices in all three categories.

② Each device is displayed on a button. An icon at the left side of the button indicates the device type.


Wired host


Switch


Router


Server


Printer


NETSCOUT tool


VoIP call manager or VoIP TFTP server


VoIP phone


Virtual switch


Virtual machine


Hypervisor


Wireless LAN controller


Wireless access point


Wi-Fi client

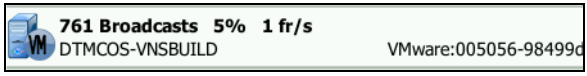
Note

Wi-Fi infrastructure devices are discovered via their wired network connections. Wi-Fi devices in the broadcast domain are discovered through Link Layer and Network Layer discovery techniques.

The information displayed on device buttons changes based on the sort key.

For example, when devices are sorted based on IP address, the IP address is displayed in bold characters, the best name is shown below the IP address, and the MAC address is shown on the right.

When devices are sorted based on "Top Broadcast" the percentage of broadcasts sent by the device is shown in bold text, the best name is shown below that, and the manufacturer MAC is shown on the right side of each device button.



The sort key is displayed on the device buttons in a bold font.

If a problem is detected a warning icon ⚠ is shown on the right. Tap the button to show detailed information.

③ The status bar is displayed on all WIRED ANALYSIS screens. It shows the number of hosts, access devices, and servers found. It also shows the total number of devices discovered.

④ The currently selected sort key is displayed above the **SORT** button SORT.

⑤ The **SORT** button SORT lets you sort the list of hosts, access devices, servers, or all devices. See "Wired Device Sorts" on page 165.

⑥ The Sort Order button determines whether the sorted results are shown in ascending or descending order.

⑦ The **REFRESH** button clears all wired analysis results and restarts wired analysis.

To Show Wired Device Details

- Tap a device to show its details.
- Tap the device again to return to a summary view of devices.
- Tap a different device to show its details. Only one device's details are shown at a time.

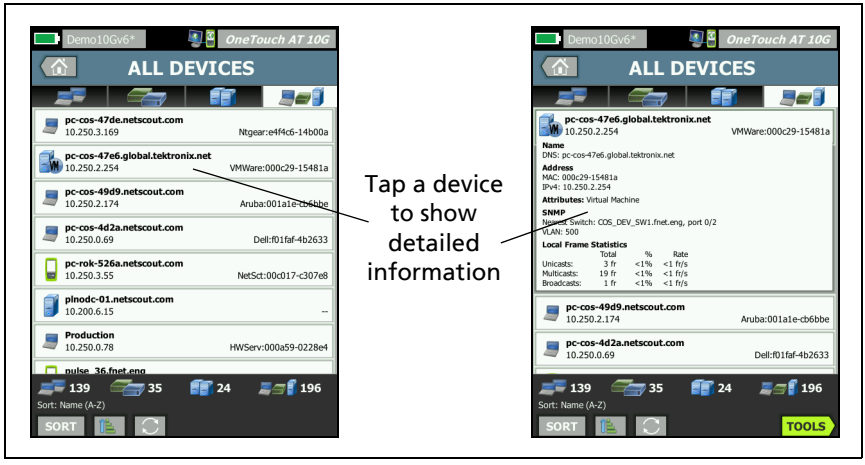


Figure 55. Displaying Wired Device Details

The following section describes the device button after it has been tapped to display details.

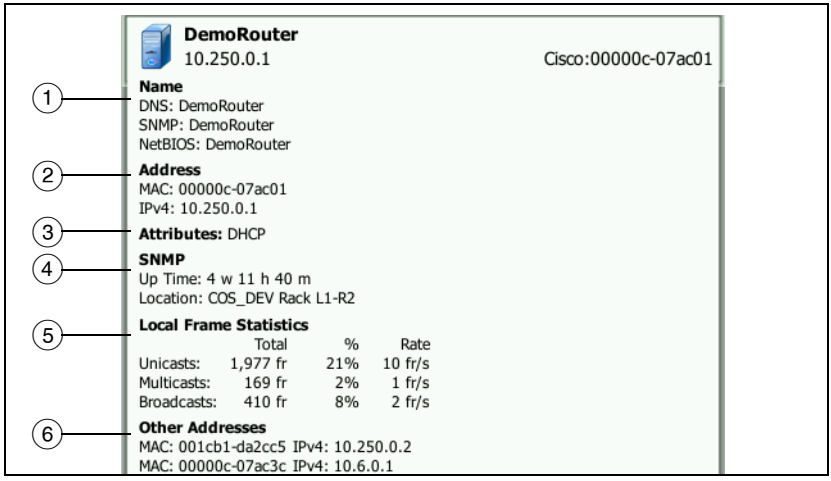


Figure 56. Wired Device Details

① This shows the device's best name in bold characters. It shows additional address information if available.

② The device's IP addresses

③ The server's attributes (e.g. virtual machine, hypervisor, domain controller, HTTP, SMTP, MS Exchange, Oracle, etc.)

④ Information gathered via SNMP is displayed here if available.

⑤ Local Frame Statistics provides the following information for unicasts, multicasts, and broadcasts:

Total - This is the total number of frames sent from the wired device and observed by the OneTouch AT.

% - The percentage of all observed frames that the wired device has sent.

Rate - This is the rate at which the OneTouch observes the wired device sending frames in frames per second.

⑥ Shows all the other IP addresses that are associated with the device, if any. Scroll down the screen to view any additional addresses, if available.

Wired Device Sorts

Wired devices can be sorted based on the following sort keys.

- Name - Sorts alphabetically according to the device's best name. The device's Best Name has the following order of precedence.
  - DNS name
  - NetBIOS name
  - SNMP name
  - IPv4 address
  - IPv6 address
  - MAC address
- IPv4 Address - A numerical sort
- IPv6 Address - A numerical sort
- MAC Manufacturer - the first three octets (the manufacturer's Organizationally Unique Identifier) are replaced by the manufacturer's name. The results are sorted alphabetically.
- MAC Address - A numerical sort
- Problems - Devices are sorted according to how many problems are detected for the device.
- Device Type - This sorts devices in the following order:
  - Virtual machines
  - Hypervisors
  - Servers
  - VoIP TFTP server
  - VoIP phone
  - VoIP call manager

  - Wireless LAN controller
  - NETSCOUT tool
  - Printer
  - Switch
  - Router
  - Client
- Domain - An alphabetic sort based on the Windows NetBIOS domain name
- Top Unicast - A numerical sort based on the number of unicast frames sent
- Top Multicast - A numerical sort based on the number of multicast frames sent
- Top Broadcast - A numerical sort based on the number of broadcast frames sent
- Switch Name/Slot/Port - An alphabetic sort based on the switch's best name, slot, and port
- VLAN - A numerical sort based on VLAN number

Finding User Test Target Servers

A reverse DNS look-up is done for all discovered devices.

When you set up a User Test you may enter a URL (the common name of a web site) such as www.google.com to specify the user test's target.

When the user test runs, a DNS lookup is performed to resolve the target's IP address. This IP address will appear on the HOST tab (and on the ALL tab) of the Wired Analysis results.

The analyzer performs a reverse DNS lookup on the resolved IP address. The resulting name may be different from the URL you entered in the User Test setup because some entities have multiple DNS names. For example, the reverse DNS lookup may produce a name such as dfw06s03-in-f18.1e100.net rather than google.com.

To find the Wired Analysis results for a user test's target server, you may need to search for it in the Wired Analysis results by its IP address, as follows.

1 Ensure that AutoTest has been run.

2 Tap the user test's icon on the HOME screen. The user test's RESULTS tab is displayed.

3 Scroll to the bottom of the screen to view the IP address of the user test's target server.

4 Now return to the wired analysis results, sort by IP address, and find the user test's target server.

5 If the user test does not complete successfully, its target server may not be displayed in the wired analysis results.

Wired Analysis Tools

Add Test

The Add Test feature provides an easy way to add a user test (ping, TCP, HTTP, etc.) using the currently selected device as the test target. To use the Add Test feature:

1 Run AutoTest.

2 Tap the Wired Analysis icon  on the HOME screen.

3 Tap a device's button to expand it.

4 Tap the wired analysis TOOLS button  .

5 Tap the **Add Test** button.

6 Select the type of test that you'd like to add.

- The test's setup screen is displayed.
- The wired device's IP address and name have been automatically entered in the test's SETUP screen.
- The test's icon has been added to the HOME screen.

7 Make other changes to the test setup as needed.

8 Tap the **TEST AGAIN** button TEST AGAIN to run the test immediately, or press the HOME key on the front panel and run AutoTest to run all configured tests.

Port Scan

The Port Scan feature scans the target device for many commonly-used open ports. Results are reported on the device's button on the WIRED ANALYSIS screen. The device's button must be expanded to view the port scan results. To use the Port Scan feature:

1 Run AutoTest.

2 Tap the Wired Analysis icon  on the HOME screen.

3 Tap a device's button to expand it.

4 Tap the wired analysis TOOLS button TOOLS.

5 Tap the **Port Scan** button. The analyzer scans the target device for open ports. Results are reported on the device's expanded button.

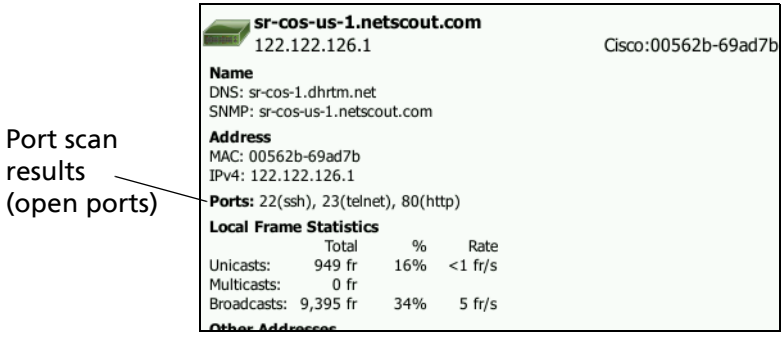


Figure 57. Port Scan Results

AutoTest Clears Wired Analysis Results

When you run AutoTest, wired Analysis results are cleared and wired analysis begins again.

Path Analysis

Path Analysis traces the connection points, including intermediate routers and switches, between the OneTouch AT 10G analyzer and a target device. You can use path analysis to identify issues such as overloaded interfaces, overloaded device resources, and interface errors.

Path Analysis combines Layer 3 and Layer 2 measurements. The Layer 3 measurement combines the classic Layer 3 IP (UDP, ICMP, or TCP) trace route measurement with a view of the path through the Layer 2 switches. SNMP queries are used to discover all switches. When the measurement is complete, the number of hops to the last device is shown. A maximum of 30 hops can be reported.

Running Path Analysis from the Wired Device Discovery Screen

1. To obtain details of SNMP-enabled devices, configure SNMP community strings or credentials for the network under test. See "SNMP" on page 158.
2. Run AutoTest.
3. Tap the Wired Analysis icon  on the HOME screen.
4. Optional: Tap the **HOSTS**, **ACCESS DEVICES**, or **SERVERS** tab to narrow your view.
5. Tap a device's button to expand it and view its details. The wired analysis TOOLS button 

appears at the lower-right corner of the screen.

6 Tap the wired analysis TOOLS button TOOLS.The wired analysis tools menu is displayed.

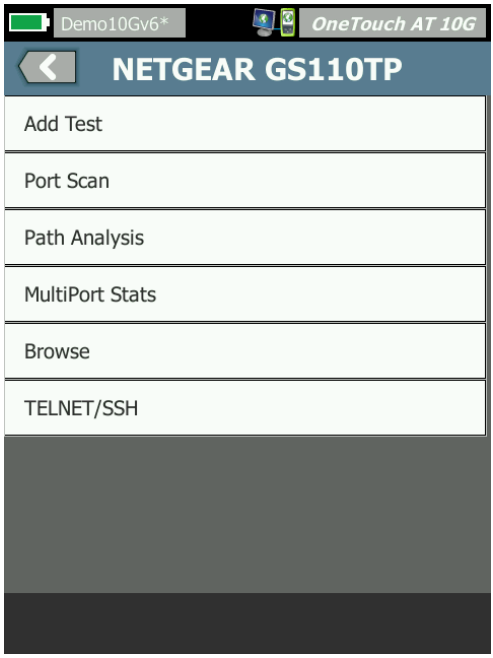


Figure 58. Wired Analysis Tools Menu

7 Tap the Path Analysis button.

The OneTouch AT 10G analyzer runs layer 2 and layer 3 path analysis to the target device and displays the results.

Each device along the path is shown on a button.

- The results screen is updated as each hop completes.
- The analyzer is the first device on the list.
- Each device's best name is shown at the top of the button and its IP address is shown below. Best name is described on page 165.
- Each queried device's response time is shown at the right side of the button.

- Each device is queried up to three times to elicit a response. If the queried device does not respond, dashes (--) are shown at the right side of the button.
- If an error is encountered a yellow warning triangle is displayed at the right side of the button. Tap the button to see the error type.
- The test concludes when the final hop to the target is resolved or if the test fails. The test will fail if link is lost during the test.

Figure 59. Path Analysis Results

The following information is shown at the bottom of the screen.

- A progress spinner, indicating the test is in progress, a green check mark, indicating the test passed, or a red X, indicating the test failed
- The number of hops it took to reach the destination
- The response time of the last hop displayed in the list
- The packet type used for path analysis
- The Packet Type button, which appears when path analysis completes or is stopped

  Tap the button to change the protocol used for path analysis. Available protocols are UDP, TCP, and ICMP. The default protocol is UDP. When using TCP, the default port is 80.

  The TCP protocol uses TCP SYN packets for path analysis, which often produces the best results.

8 Tap a device's button to see detailed information. Details such as utilization and errors are shown for SNMP-enabled devices.

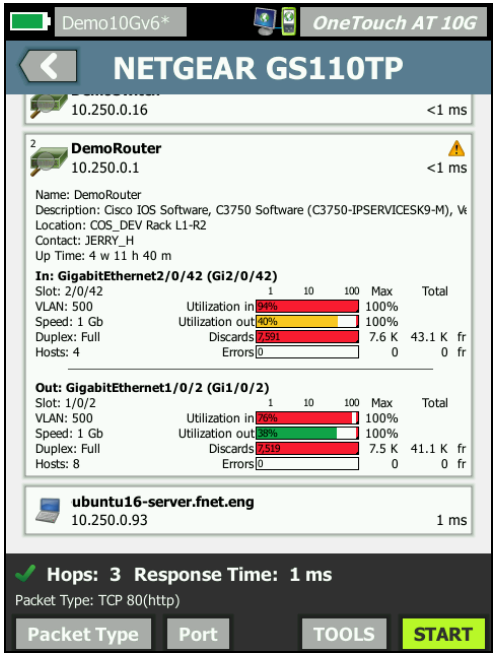


Figure 60. Path Analysis - Detailed Results

Tap the START button START to clear the results and run path analysis again.

MultiPort Statistics

The OneTouch AT 10G analyzer's MultiPort Statistics feature shows device health information including utilization, discards, and errors on each port.

Link Level Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP), Extreme Discovery Protocol (EDP), Foundry Discovery Protocol (FDP), and SNMP are used to gather information from the nearest switch. SNMP access is required to obtain information from all other devices. See "SNMP" on **page 158**.

Methods for Displaying MultiPort Statistics

Any of the following three methods can be used to view a device's port statistics.

MultiPort Statistics via WIRED ANALYSIS

Wired Analysis is described beginning on page 157.

1 Tap the Wired Analysis icon  on the HOME screen.

2 On the WIRED ANALYSIS screen, tap a device's button to expand it.

3 Tap the TOOLS  button.

If the analyzer is configured for SNMP access to the device and MultiPort Statistics are available, the **MultiPort Stats** button ap-

pears in the tools menu, as shown below.

Figure 61. MultiPort Statistics Button on Wired Analysis Tools Menu

4 Tap the **MultiPort Stats** button to display the device's port statistics.

MultiPort Statistics via the HOME Screen

1 On the HOME screen, tap the nearest switch icon or the gateway icon .

2 Tap the TOOLS button TOOLS to display the tools available to the device. If the **MultiPort Stats** button is shown, it means that SNMP is configured on the device and you will be able to view its MultiPort statistics.

3 Select the **MultiPort Stats** button.

MultiPort Statistics via Path Analysis

Path analysis is described beginning on page 169.

1 From the path analysis results screen, tap a device's button to expand it and view its details.

2 Tap the TOOLS button TOOLS, which is at the bottom of the screen. If MultiPort Statistics are available for the device the **MultiPort Stats** button is displayed.

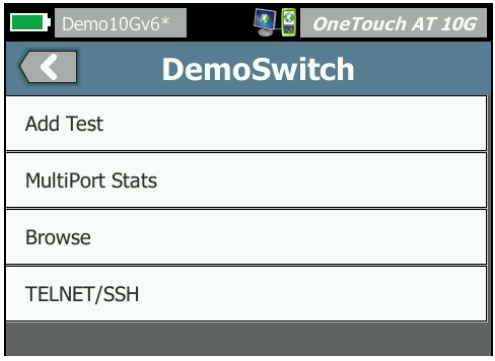


Figure 62. MultiPort Statistics Button on Path Analysis Tools Menu

3 Tap the **MultiPort Stats** button to display the device's port statistics.

If the **MultiPort Stats** button is shown, it means that SNMP is configured on the device and you will be able to view its multiport statistics.

MultiPort Statistics Summary Screen

- When you tap the MultiPort Stats button, the analyzer gathers information from the device and displays it on a summary screen.

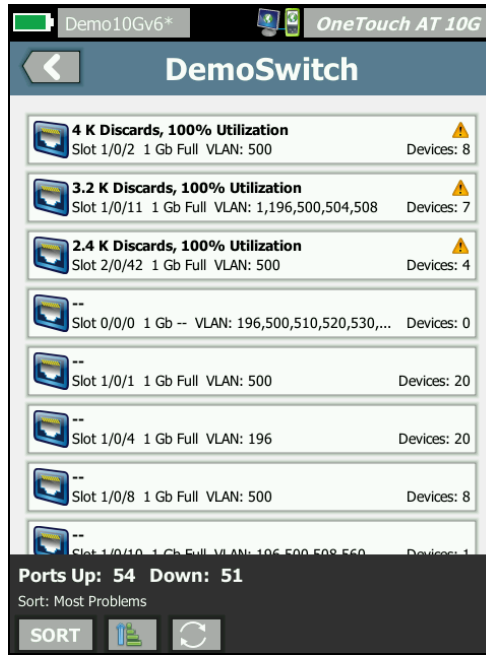


Figure 63. MultiPort Statistics Summary Screen

Only ports that are up (linked) are displayed. The list is updated realtime. By default, ports are sorted by maximum utilization.

The screen above shows the ports sorted by problem type. The most severe problem type is at the top of the list.

Use the SORT button to change the sort key. The top line on the device buttons changes based on the sort key.

Tap the SORT button to list ports by

- Slot number, port number
- Speed

- Duplex mode
- Problems (problem severity)
- Utilization In/Out
- Utilization In
- Utilization Out
- VLAN number
- Device Count (number of connected devices)

Use the Sort Order button to sort the results in ascending  or descending  order.

The **REFRESH** button  clears the results and restarts MultiPort analysis.

MultiPort Statistics Port Details Screen

Tap a port's button to expand it and view its details.

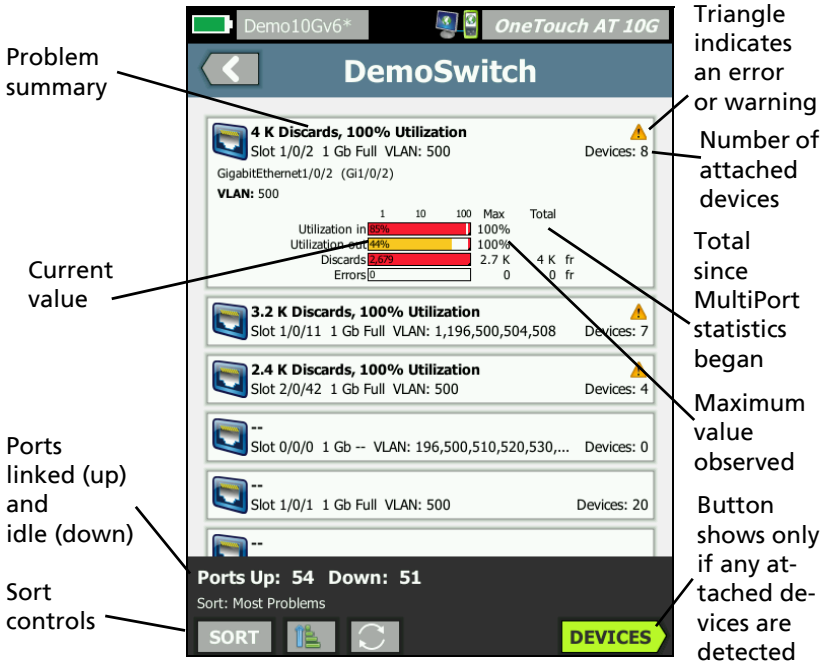


Figure 64. MultiPort Statistics Details Screen

Warning Triangle ⚠ - The warning triangle appears when (in or out) utilization is 70% or more, or when discards or errors occur.

Thresholds - The utilization bars and lines turn yellow at 40%; red at 70%. Discard error bars and lines are always shown in red.

Devices button - This button will only be shown if any attached devices are detected on the selected port. Selecting this button will show a listing of all the attached devices.

MultiPort Statistics Devices on Port Details Screen

Selecting the **Devices** button will show a listing of all attached devices on the current port. If you select a device that is SNMP

enabled, a TOOLS TOOLS button will be shown at the bottom left of the screen. Choosing the TOOLS button will present you with a listing of available tools.

Figure 65. MultiPort - Device on Port Details Screen

Web Browser

When you tap the **Browse** button, the browser is launched with the selected device as the target server. See “Browser” on page 196.

Telnet/SSH

When you tap the **Telnet/SSH** button, a Telnet/SSH session is started with the selected device as the target. See “Telnet/SSH” on **page 197.**

Chapter 8: Tools

Tap the TOOLS icon on the HOME screen to access the TOOLS screen.

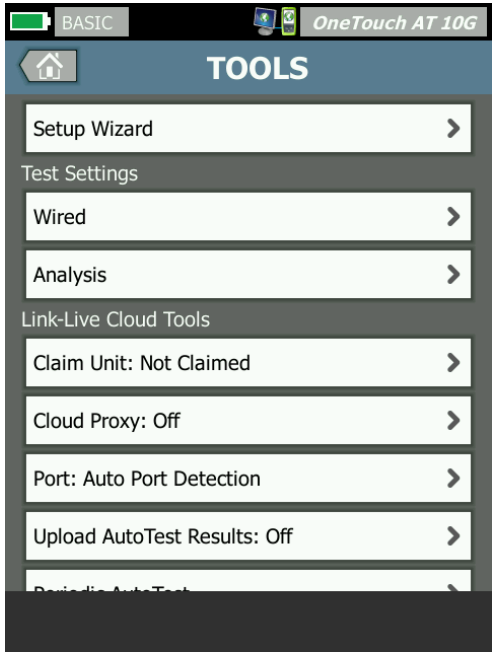


Figure 66. Tools Screen

Test Settings

The following test settings can be configured via the TOOLS screen. Refer to the following pages.

"Wired" on page 184

"SNMP" on page 158

"Slow Discovery" on page 159. Also included in this section:

"View or Change the analyzer's MAC Addresses" on page 186

Wired

On the HOME screen, tap **TOOLS**  , then tap the **Wired** button to access the wired settings.

Speed and Duplex

Choose a link speed and a duplex mode. Auto (Autonegotiation) is recommended in most circumstances. However, you can force Speed and Duplex settings if desired.

802.1X

Tap the **802.1X** button to open the SECURITY screen. Enable 802.1X authentication by setting **Enable** to **On**.

EAP - Select an EAP type that is appropriate for your authentication server.

If necessary for your selected EAP type, enter the **User** name (login name) and **Password**.

Alternate ID - The Alternate ID can be used with certain EAP methods to send an empty or anonymous identity in plain text while establishing a private connection. Once privacy is established, the analyzer sends the real identity (specified using the User and Password buttons) within the secure tunnel. Alternate ID is analogous to Microsoft Windows Identity Privacy.

The Alternate ID can also be used for routing to an authentication server in a different realm. In this case, the Alternate ID may take the form anonymous@MyCompany.com or /MyCompany/anonymous.

Certificate - TLS EAP types require a certificate for authentication. Certificates must be loaded in the **/internal/Certificates** directory on the OneTouch analyzer.

To import a user authentication certificate:

1 Insert an SD card or USB drive with the required certificate into the correct port on your OneTouch.

2 Tap the **Certificate:** button and then the MANAGE (Manage) button to open the MANAGE CERTIFICATES screen.

3 Tap IMPORT to open the IMPORT CERTIFICATE screen.

4 Select the storage location where the certificate is saved.

5 Select the certificate file, and then tap **OK**.

For more information on importing and exporting files, see "Managing Files" on page 229.

Address

The IPv6 option on the ADDRESS screen determines whether the IPv6 columns are shown on user test RESULTS screens. The wired IPv4 test results column is always displayed. IPv6 results are displayed if IPv6 is enabled as described below. The IPv4, IPv6, and MAC Address options listed below apply to the wired interface.

IPv4 - The analyzer's wired IPv4 address is always enabled. Tap the IPv4 address button to configure the analyzer with a static IP address, or to select DHCP. Choose the settings that are appropriate for your network.

IPv6 - When you enable the analyzer's IPv6 address, the analyzer links and obtains an IPv6 address when you run AutoTest, and IPv6 results are included in all user test RESULTS screens.

User MAC - If the network under test has an Access Control List (ACL) you can change the MAC address of the analyzer's network port to match an allowed MAC. Choose the MAC address of a device that currently is not on the network.

Enable IPv6 on the Wired Interface

To enable IPv6 address capability on the wired interface:

1 On the HOME screen, tap **TOOLS** .

2 In the Test Settings section, tap the **Wired** button.

3 Tap the **Address** button.

4 Tap the IPv6 **On** button.

View or Change the analyzer's MAC Addresses

If your network uses a MAC Access List, you will need to view the analyzer's MAC address and add it to the access list. The MAC is shown at the bottom of the ADDRESS screen.

To connect to the OneTouch AT 10G analyzer for remote viewing or remote file access you will need to know the IP address of the management port.

Ethernet MAC Address

To view or change the MAC address of the network under test port:

1 On the HOME screen, tap the **TOOLS** icon .

2 Tap the **Wired** button.

3 Tap the **Address** button.

4 Tap the **User MAC On** button.

5 Tap the **User MAC Address** button and enter the desired address.

Management Port MAC Address

The Management port MAC address can be viewed but it cannot be changed.

To view the Management Port MAC address:

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to Maintenance Tools section and tap the **Management Port** button.

Wi-Fi Adapter Management Port MAC Address

To view the Wi-Fi Adapter Management Port MAC address:

1 On the HOME Screen, tap **TOOLS** .

2 Scroll down to Maintenance Tools section and tap the **Management Port** button.

3 Toggle Active Port to Wi-Fi.

4 Insert the supported Wi-Fi Adapter. The MAC address will be shown in the status line of the screen.

VLAN

To make the analyzer a member of a VLAN:

1 On the HOME screen, tap **TOOLS** .

2 Tap the **Wired** button.

3 Tap the **VLAN** button.

4 Set **Tag** to **On**.

5 Tap the **ID** button and enter the VLAN ID.

6 Tap the **Priority** button and select a priority. This sets the priority field in the header of all packets sent by the analyzer. It has no effect on received packets.

Wait for Rx Frame

By default, when you connect the analyzer to a switch port, the analyzer attempts to ensure that the port is in the forwarding state before conducting tests. If you know that the switch port is in the forwarding state immediately upon link, set **Wait for Rx Frame** to **Off**.

To change the **Wait for Rx Frame** setting:

1 On the HOME screen, tap **TOOLS**  .

2 Tap the **Wired** button.

3 Tap the **Wait for Rx Frame** button.

4 Select **On** or **Off**.

Analysis

See “SNMP” on **page 158**, and “Slow Discovery” on **page 159**.

Link-Live Cloud Tools

The Link-Live Cloud tools are for interacting with the Link-Live Cloud Service.

Claim Unit:

You must *claim* your OneTouch AT analyzer before you can view its test results in the Link-Live Cloud. For additional information see "Claiming Your Unit," beginning on **page 246**.

Cloud Proxy:

By default this setting is off. If you choose to enable it, additional input options will be shown: Proxy Address, Proxy Type, and Proxy Port.

Port:

By default, the OneTouch automatically detects and uses an appropriate port. If needed, you can specify the Management

Port or the Wired Port to communicate with the Cloud Service and upload test results and reports.

Note

You must have an active connection to the Management Port when claiming your unit or uploading screenshots to the Link-Live Cloud Service. Test results and reports will upload via any available port.

Upload AutoTest Results:

Turn this setting off if you do not want your OneTouch to upload AutoTest results to Link-Live Cloud Service.

Periodic AutoTest

When the analyzer is in Periodic AutoTest mode, the OneTouch runs AutoTests at specified intervals and sends the results to Link-Live so that you can view the results over time. The OneTouch AT unit must be claimed before any Periodic AutoTesting can occur, and Periodic AutoTesting must be configured to allow the OneTouch AT's test results to be sent to the Link-Live Cloud.

To enable Periodic AutoTest:

1 Select **TOOLS**  from the HOME screen.

2 Under **Link-Live Cloud Tools**, select **Periodic AutoTest.**

3 Configure the following:

Duration - The length of time during which test results will be sent to the Link-Live Cloud. The duration can be set to Unlimited Duration, 2, 5, 10, and 30 minutes, or 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hrs, 8 hrs, and 12 hrs, or 1 day, 2 days, 3 days, 4 days, 5 days, or 1 week, or 2 weeks.

Interval - This is the amount of time between sent test results to the Link-Live Cloud over a selected time duration.

Comment - This entry will appear beneath the Periodic AutoTest results in Link-Live Cloud Service. Use this feature to anno-

tate your Periodic AutoTest session.

Backlight Timeout - This feature controls how long the OneTouch screen's backlight stays illuminated while Periodic AutoTesting is ongoing.

Cloud Remote:

Enable this option when you want to allow the claimed unit to be accessed remotely from the Link-Live Cloud. See page 250.

Unit Name:

You can give your OneTouch AT a descriptive name to make it easier to identify when working in the Link-Live Cloud. See page 250.

Testing Tools

The following testing tools are available on the TOOLS screen.

Capture

See "Packet Capture" on **page 221**.

iPerf Test

The iPerf Test is a standardized network performance tool used to measure UDP or TCP capacity and throughput. The OneTouch can perform iPerf testing using either a NETSCOUT Test Accessory endpoint or iPerf3 software installed on a PC or other device as the endpoint.

OneTouch can automatically discover, and use as endpoints, Test Accessories that are claimed to the same organization as your OneTouch unit on Link-Live Cloud Service. See "Link-Live Cloud Service" on **page 245** and your Test Accessory User Guide for more information.

To use an iPerf server installed on a PC or other device as the endpoint, iPerf version 3.0 or higher is required. You can download it at this URL: **https://iperf.fr**

To perform iPerf Performance Testing, your OneTouch 10G must be connected to an active wired network.

To Configure an iPerf Test

1 On the HOME screen, tap **TOOLS** .

2 In the **Testing Tools** section, tap the **iPerf Test** button.

The iPerf Test screen is displayed.

Figure 67. iPerf Test Setup Screen

3 Touch the **iPerf Server:** button to open the iPerf Server screen.

Figure 68. iPerf Server Screen

4 Your iPerf server can be either a Test Accessory or iPerf software installed on another device. Select the appropriate iPerf test endpoint using one of the following methods:

- Touch the **iPerf Server:** button on the IPERF SERVER screen to manually enter your iPerf server's IPv4 address or URL using the virtual keyboard. Touch DONE to save your entry.
- If it is claimed to Link-Live, OneTouch automatically queries Link-Live for any claimed Test Accessories in the same organization and displays them in the **Available iPerf Remotes** list. Touch the **QUERY IPERFS** button to re-query Link-Live for Test Accessories. Select a discovered Test Accessory from the list to use it as your iPerf Server.

Note

You must have a NETSCOUT Test Accessory claimed to the same organization as your OneTouch unit for your OneTouch to be able to discover the Test Accessory for iPerf testing.

Additionally, your OneTouch must be connected to a network via the Management Port to query Link-Live.

Once selected, the iPerf Server software's or Test Accessory's address displays in the top field on the iPerf Test screen.

5 If needed, tap **Port** to enter a port number other than the default 5201.

Note

If you change the default Port number on the OneTouch, you must also change the Port number in the iPerf server's settings to match.

6 Choose a **Protocol** to test, either **TCP** or **UDP**.

The test parameter options change depending on the selected Protocol. Figure 67 shows the TCP parameters and Figure 69 shows UDP test parameters.

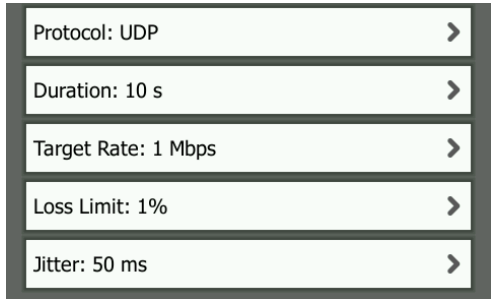


Figure 69. UDP Protocol Parameters

7 Adjust the iPerf test **Duration**, **Target Rate**, **Window Size**, **Loss Limit**, and/or **Jitter** as needed for your testing purposes.

To Run an iPerf Test

To begin the test, tap the **START** button at the bottom of the iPerf Test screen.The iPerf test begins, and the Wired results screen appears.

To View iPerf Test Results

The results screen header displays the IP address of the selected iPerf server.

Specific test results vary depending on the Protocol (TCP or UDP) being tested.

At the bottom-left corner of the screen, an icon indicates the test's status:

- A progress spinner indicates the test is in progress.
- A green check mark indicates the test passed.
- A red x indicates the test failed.

  An error message indicates the reason for test failure.

TCP Protocol Test Results

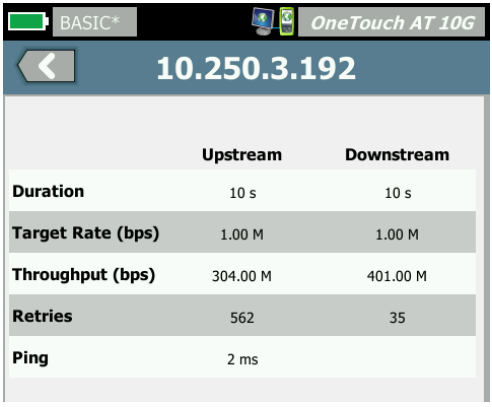


Figure 70. iPerf TCP Test Results

Duration is the length of time the test ran.

Target Rate (bps), for the TCP protocol, is the pass/fail threshold for the test, as set on the iPerf Test setup screen.

Throughput (bps) is the measured bit rate based on frames sent and the actual number of frames received.

Retries (TCP Protocol only) is the number of retransmitted TCP segments.

Ping shows the Ping response time from the iPerf server.

Note

If the Ping portion of the test fails, the entire iPerf test will fail.

Tap the **TEST AGAIN** button to re-run the test.

UDP Protocol Results

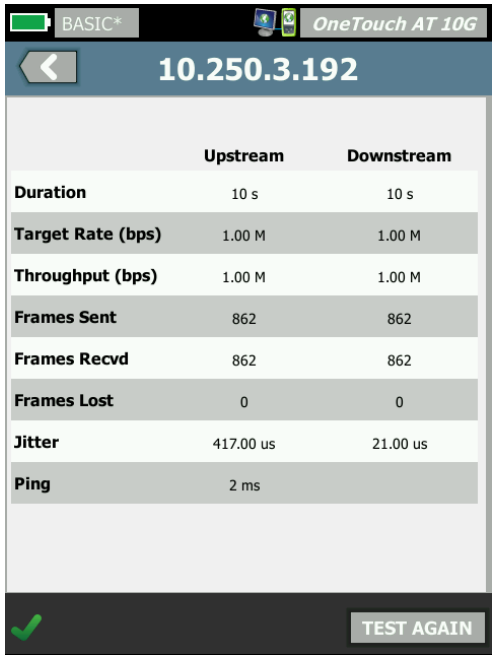


Figure 71. iPerf UDP Test Results

Duration is the length of time the test ran.

Target Rate (bps) is the requested bit rate from the iPerf Test setup screen.

Throughput (bps) is the measured bit rate based on frames sent and the actual number of frames received.

Frames Sent is the actual number of frames sent by the source.

Frames Recvd is the actual number of frames received at the destination.

Frames Lost is the number of frames sent less the number of frames received.

Jitter is the average frame delay variation.

Ping shows the Ping response time from the iPerf server.

Tap the **TEST AGAIN** button to re-run the test.

Performance Peer

This tool is used when running Wired Performance tests that require two devices - the source OneTouch AT 10G and either a peer or reflector. This tool is used when designating this device to be the peer.

See "1G Wired Performance Test (RFC 2544)" on **page 103** and "10G Wired Performance Test (Y.1564)" on **page 120** for more information.

Browser

The OneTouch AT 10G analyzer's web browser and SSH allow you to perform tasks such as verifying and changing switch provisioning, accessing technical information on the web, and closing trouble tickets in help desk portals. To access the web browser or the SSH client:

1 Establish a wired Ethernet connection to your network. You can use the network test ports (RJ-45 or Fiber) or the management ports.

2 On the HOME screen, tap **TOOLS**  .

3 In the **Testing Tools** section, tap **Browser**.

4 Use the **Web Server** button to specify the target server.

5 Select the port you want to use for the browser connection.

6 Set **Mobile** to **On** to advertise to the web server that you are on a mobile device. If available, you will receive content formatted for the smaller screens of mobile devices.

7 Use the **Proxy** button to specify a server through which the connection will be established.

8 Tap the **LAUNCH** button to launch the browser.

Swipe your finger across the display to pan across a web page.

Tap a text entry area to display the touchscreen keyboard.

Note

The browser does not support Flash or Java.

Browse to a Test Target from the HOME Screen

The browser can be launched from SETUP or RESULTS screens of the following tests: DNS, Ping, TCP, HTTP, FTP, RTSP, SMTP. This lets you test web connectivity to the configured servers.

1 Tap the test's icon on the HOME screen.

2 Tap the wired analysis TOOLS button 

.

3 Tap the **BROWSE** button at the bottom of the screen. This opens the BROWSER screen and populates the Web Server field.

4 Tap the **LAUNCH** button.

Telnet/SSH

1 Establish a wired Ethernet connection to your network. You can use the network test ports (RJ-45 or Fiber) or the management ports.

2 On the HOME screen, tap **TOOLS** .

3 In the **Testing Tools** section, tap **Telnet/SSH**.

4 Tap the **Telnet/SSH Server** button and specify the target.

5 Select the port you want to use for the telnet or SSH session.

6 On the Protocol button, select **Telnet** or **SSH**.

7 If you selected SSH, enter the user name and password.

8 Tap the **LAUNCH** button to start the session. The analyzer starts a telnet or SSH session.

Use the on-screen keyboard to type your commands.

To end the session, tap the back button .

Flash Port

Flash port is a tool for finding the port on a switch where a copper or fiber cable is connected. When activated, the analyzer repeatedly links and unlinks, causing the switch's link indicator to flash on and off.

1 On the HOME screen, tap **TOOLS** .

2 In the Testing Tools section, scroll down and tap **Flash Port**.

3 Tap the **Rate** button.

4 Select the rate you want the analyzer to link and unlink from the port.

5 Observe the link indicators on the switch. Find the one that is flashing on and off at the selected rate (one second, two seconds, or three seconds).

6 Tap the **STOP** button to end the test.

FiberInspector

The optional DI-1000 video probe connects to the USB-A port on the analyzer. The probe lets you see dirt, scratches, and other

defects on fiber connector endfaces that can cause unsatisfactory performance or failures in fiber optic networks.

1 Connect the FiberInspector to the analyzer's USB-A connector.

2 On the HOME screen, tap **TOOLS** .

3 In the **Testing Tools** section, scroll down and tap **FiberInspector/WebCam**. The image from the camera appears on the analyzer's screen.

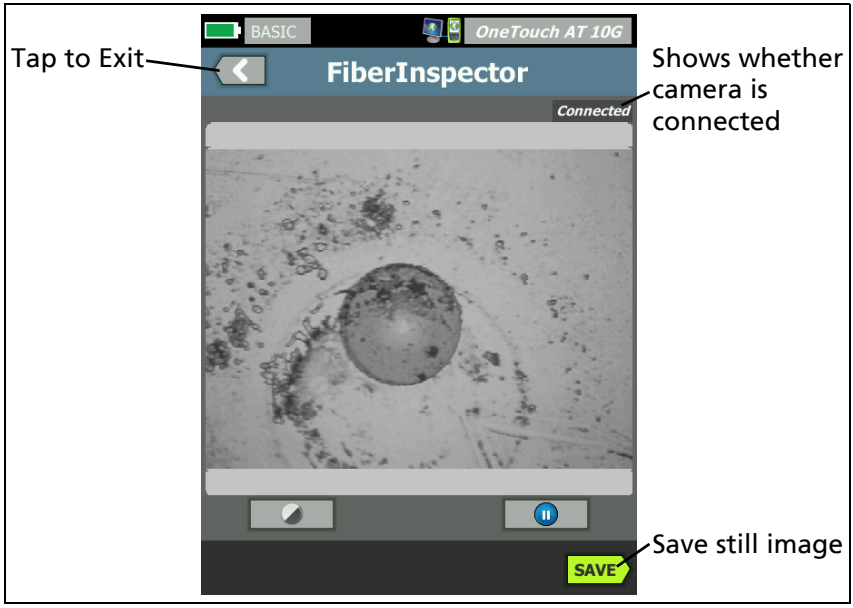


Figure 72. FiberInspector Image of an Endface

4 To adjust the focus, turn the knob on the probe clockwise or counterclockwise.

Note

The button on the DI-1000 probe has no function when you use the probe with the analyzer.

5 Tap the **Save** button to save the screen image. The image on the screen is paused (it becomes still). The image is saved in .PNG format to the /internal/screens directory.

Using the Scales

1 To show the scales, tap , then tap **SCALE ON**.

2 Drag the image of the core to the center of the screen.

3 To change the size of the measurement ring for the fiber core, tap **NEXT SCALE**.

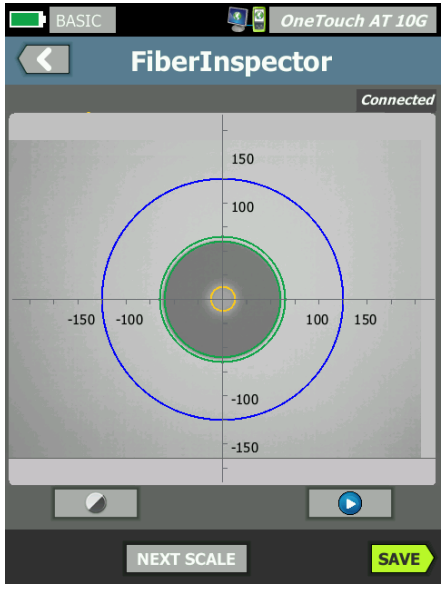


Figure 73. FiberInspector Image with Measurement Scales
(fiber with 50 μm core shown)

Note

To see the buttons for the measurement axes and core scales and to change the magnification of the screen, you must first tap to put the screen in still mode.

You can use the round, horizontal, and vertical scales to measure the size of the fiber core and cladding. You can also measure the size of particles, scratches, and other defects on the endface.

- Outer, blue ring: 250 μm cladding

- Middle, green rings: 120 μm and 130 μm
- Inner, yellow rings: 25 μm and 62.5 μm (to change the size, tap **NEXT SCALE**)

To adjust the brightness or contrast of the image, tap , then move the bars on the controls. To hide the controls, tap again.

Touchscreen Gestures

Use the pinch gesture to zoom out.

Use the reverse-pinch gesture to zoom in.

Drag the image in any direction to move it.

Use the double-tap gesture to center the image on the screen and reset the zoom to 100%.

WebCam and Remote View

A network technician can connect a WebCam to the analyzer and share its live image with a colleague.

A technician can share his live view of network components in a wiring closet while conversing with a remote colleague.

1 Connect the WebCam to the analyzer's USB-A connector.

2 On the HOME screen, tap **TOOLS**  .

3 In the Testing Tools section, scroll down and tap **FiberInspector/WebCam**. The image from the camera appears on the analyzer's screen.

4 Have the remote colleague establish a remote connection to the analyzer via a web browser (as described on page 234). The analyzer's browser control home screen appears in the colleague's browser.

5 Have the remote colleague select "Remote Control." The webcam image appears in the remote colleague's browser.

Link Validation

Use this tool to quickly determine the link speed available on the connected port.

To run, connect the OneTouch AT to your Switch Port via either the SFP or the RJ-45 port, tap the **Link Validation** button under **Testing Tools**, and simply wait for the results to display.

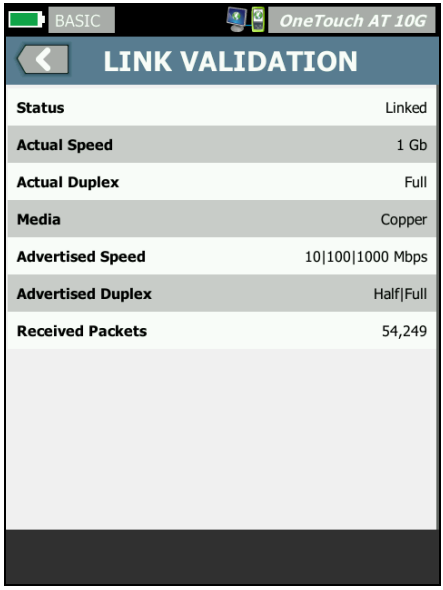


Figure 74. Link Validation Screen

Status indicates that the OneTouch is linked.

Actual Speed is the speed that was negotiated when the analyzer connected to the network.

Actual Duplex is the duplex that was negotiated when link was established.

Media is the type of cable in use on the link.

Advertised Speed indicates the speed(s) offered by the port where the analyzer is connected.

Advertised Duplex is the duplex capability of the port.

Received Packets is the number of packets received over the link by the OneTouch.

File Tools

The following file tools are available on the TOOLS screen.

Profiles

See Chapter 6: "Profiles," beginning on **page 151**.

Reports

The OneTouch analyzer can create a comprehensive report in PDF and/or XML format (for exporting to Excel). Specific report options are available when exporting to PDF: Tools Settings, AutoTest, and Wired Analysis. All available details are included when you save a report only in XML.

When you initially power on a OneTouch AT 10G analyzer, only two selectable report options are available, the Tools Settings and AutoTest. You must first run AutoTest to include AutoTest data in the saved report.

Note

*In addition to accessing the Reports options from the TOOLS screen, you can also tap the **OneTouch AT 10G** short-cut button on the top right corner of your OneTouch screen to access available report options.*

Obtaining Report Options

To obtain AutoTest and Wired Analysis data in your report, run AutoTest first.

Note

The OneTouch AT 10G analyzer must be connected to the wired network to display the Wired Analysis option in the SAVE report option list.

Figure 75. Available Report Options

Saving a Report

To save a OneTouch AT 10G analyzer report:

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the File Tools section, and tap **Reports**.

3 Tap the **SAVE** button.

Figure 76. Save Report Screen—Possible Report Options

4 Tap the **File:** button to change the file name if desired, and then tap the **Done** button.

5 Tap the **Format:** button to change the report output if desired. Reports can be exported as a PDF, XML for export to an Excel file, or both.

Note

The report content options are only available when saving in PDF format. XML reports will contain all available details.

6 Use the check boxes to select report options to be included in the report.

For **AutoTest** and **Wired Analysis**, you can determine which summaries and details you want the report to include.

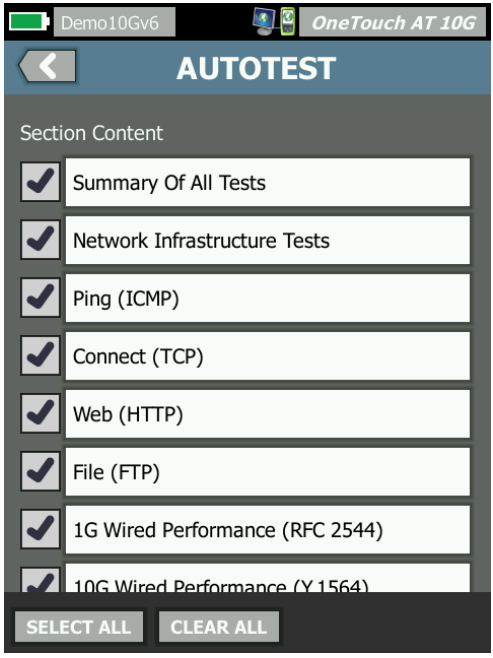


Figure 77. Report Content Options for AutoTest

7 Tap the back button to go back to the Save Report screen.

8 Tap the **Wired Analysis** button to select wired analysis content for your report.

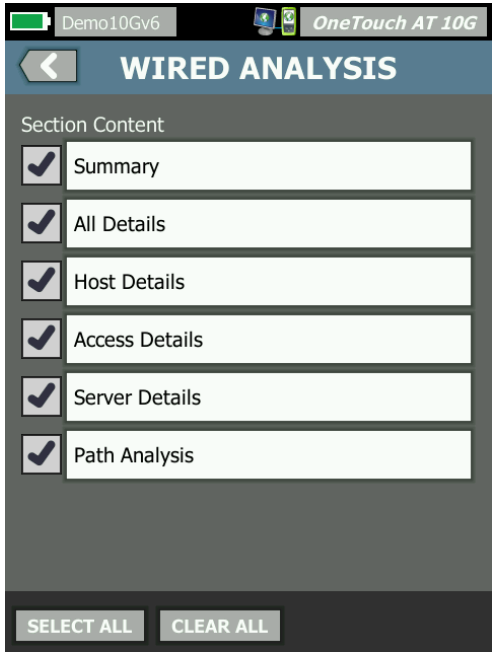


Figure 78. Report Content Options for Wired Analysis

To obtain Path Analysis data in your report, run Path Analysis using the Wired analysis screens. Then, tap the **Wired Analysis** button on the Save Report screen, select the **Path Analysis** check box, and save.

9 Tap the back button to go back to the Save Report screen.

10 Tap the **SAVE** button. The report is saved in your selected format(s) to the analyzer's /internal/Reports directory. You can access the saved file as described in Chapter 10: "Managing Files," beginning on page 229.

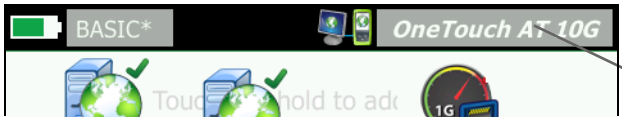
11 Tap **VIEW** to see the saved report on the OneTouch analyzer. See also: page 229.

Screens

Save a Screen Image

You can take a screen shot of the analyzer's display as follows:

1 Tap the text that says OneTouch AT 10G at the top-right corner of the screen.



2 Tap **Save Screen**. The SCREEN FILENAME screen appears.

3 A screen name that includes the date and time of the screen capture is populated in the name field. Optionally, you can edit the default name or type a new name using the on-screen keyboard.

4 When you are satisfied with the screen filename, tap the **DONE** button. The screen is saved.

Import, Export, Rename, or Delete a Screen Image

You can view previously saved screens using the SCREENS tool. You can manage (import, export, rename, or delete) previously saved screens using the MANAGE SCREENS tool.

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the File Tools section and tap **Screens**. The SCREENS tool appears.

3 Tap a screen file and tap the **VIEW** button to view it on the analyzer.

4 To import, export, delete, or rename a screen, tap the **MANAGE** button, then tap the screen file that you want to manage.

5 Tap a management button (**DELETE**, **RENAME**, **EXPORT**, or **IMPORT**) and complete the operation. When using EXPORT or IMPORT, you can tap to navigate the displayed directory structure.

Maintenance Tools

Version Information

To display software and hardware version information:

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section, and tap **Version Information**. The module and platform serial number, version number, and hardware revision are shown.

Management Port

The OneTouch AT 10G management port can be set to wired or Wi-Fi. The wired setting refers to the RJ-45 Ethernet port located on the left side of the analyzer. The Wi-Fi setting refers to the use of an optional Wi-Fi adapter that is connected to the analyzer's USB port on the right side of the device. The adapter can be ordered separately from NETSCOUT.

The wired management port is the default management port. It links automatically when connected to a network. It is not necessary to run AutoTest to make either of the management ports link. However, if you make any changes to the management port settings, you must tap the CONNECT button for those changes to take effect.

The Wi-Fi management port is disabled by default and needs to be configured on the Management Port configuration screen prior to use.

To configure the Wi-Fi management port:

1 Insert the Wi-Fi management port adapter into the OneTouch AT's USB port.

2 On the HOME screen, tap **TOOLS** .

3 Scroll down to the Maintenance Tools section and tap **Management Port**. The management port screen is displayed.

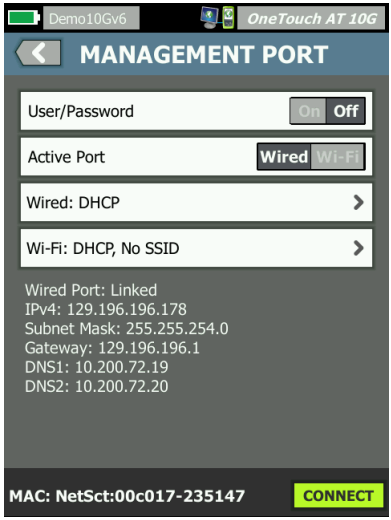


Figure 79. Management Port Screen Linked Wired

4 On the **Active Port** button**,** tap **Wi-Fi.**

5 Tap the **Wi-Fi** button.

6 Tap the **Address** button, then tap **DHCP** or **Static**.

Selecting **Static** will show additional selections: **IP**, **Subnet Mask**, **Gateway**, **DNS1**, and **DNS2**. You must provide a static IP address and a Subnet Mask.

7 Tap the **SSID** button.

8 Tap an **SSID** from the list of available SSIDs.

9 Tap the **Security** button. It will take you to the Security screen.

10 Tap the **Type** button if you want to change the current setting.

If you change the security type, additional selections will be-

come available. These additional selections will vary depending on the selected authentication type.

11 Tap each new selection that became available as a result of changing the authentication type and provide the requested information.

12 Tap the back button  to return to the initial Management Port screen.

13 Tap the **Connect** button 

for your new settings to take effect.

Management Port Selections

User/Password - This option is **Off** by default. When it is **On**, the **User** and **Password** buttons will be shown.

User - Assign a user name to the management port.

Password - Assign a password to the management port.

Active Port - Choose Wired or Wi-Fi. Wired is the default. When choosing Wired, a network cable must be connected to the RJ-45 management port. When choosing Wi-Fi, the optional Wi-Fi management port adapter must be connected to the OneTouch USB port.

Wired - Select DHCP or Static IP addressing.

Wi-Fi - Allows you to choose DHCP or Static IP addressing, select an SSID, and choose an authentication option. Connect the optional Wi-Fi management port adapter to the OneTouch's USB port.

Configure Login Credentials for Remote Access

To configure user name and password for remote access via management port:

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to Maintenance Tools and tap the **Management Port** button.

3 On the **User/Password** button tap **On**. This action will display the User and Password buttons on the screen.

4 Tap the **User** button and enter a user name.

5 Tap the **Password** button and enter a password.

6 Choose an Active Port: Wired or Wi-Fi. Ensure that if you choose the Wired Port, a cable is connected to the Wired management port, and if you choose Wi-Fi that the Wi-Fi management port adapter is connected to the USB port.

   If you select Wi-Fi, you may have to configure it. Follow the directions in the procedure above.

7 Tap the **Connect** button CONNECT for your new settings to take effect.

Address Control (DHCP or Static)

The Address control can be set to DHCP or Static. When set to DHCP, the analyzer gets its IP address, subnet mask, etc. from the DHCP server.

If the analyzer has obtained an IP address via DHCP, and you subsequently switch the Address control to Static, the currently configured IP address, subnet mask, etc. will be retained until you change it.

Setting a static IP address for the analyzer can simplify the process of connecting to it remotely, because the IP address will always be the same. This is convenient when you can't walk over to the analyzer and view the Management Port screen.

If a network administrator needs to reserve an IP address for the analyzer, you will need to provide the analyzer's MAC address to the administrator. See **"View or Change the analyzer's MAC Addresses" on page 186**.

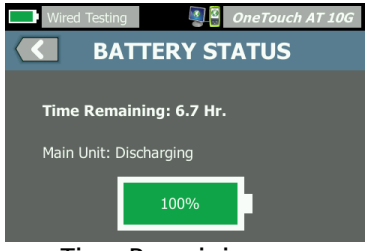
The analyzer's management ports can be used for:

- Remote viewing and control of the analyzer via web browser

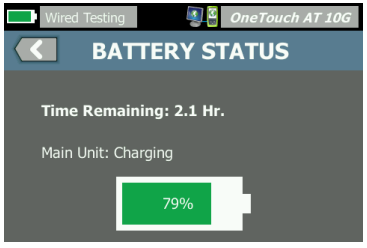
- Accessing the analyzer's user file system via web browser or FTP
- Verifying and changing switch provisioning using the built-in telnet and SSH tools
- Accessing technical information on the web using the built-in web browser

Battery Status

This screen shows the battery's status.



Time Remaining indicates estimated battery operating time if AC adapter is not connected



Time Remaining indicates estimated time to fully recharge if AC adapter is connected.

Figure 80. Battery Status Screen

Language

See "Set the Language" on **page 18**.

Date/Time

See "Date/Time" on **page 38.**

Number

See "Number Format" on **page 39.**

Length

See "Units for Length Measurements" on **page 39.**

Timeout Period

See “Timeout Periods (Power-Down and Backlight)” on **page 39.**

Audible Tone

You can enable or disable the sounds emitted upon system start, button presses, and system shutdown.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section.

3 In the **Audible Tone** panel, tap **On** or **Off**.

Display

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section, and tap **Display**.

3 Move the yellow bar to select the desired brightness.

4 Tap the **DONE** button.

Note

Increasing the display brightness draws more power, thereby decreasing run-time when operating the analyzer on battery power.

Update Software

Note

To prevent problems caused by losing power during a software update, supply power to the analyzer with the AC adapter.

Updating Software Using a USB Drive or SD card

To update software, download the new software image file from **www.enterprise.netscout.com.** You can install the new software image file from a USB flash drive or an SD card.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section and tap **Software Update**.

3 Navigate to the directory where you saved the new software image (**.img**) file and select the file.

4 Select the **OK** button.

5 Select **YES** to install the new file.

The new file will be installed and the analyzer will restart. The process will take several minutes.

Updating Software via Link-Live Cloud Service

Starting with OneTouch version 6.5.1, you can download updates from Link-Live if your OneTouch is claimed. (See also "Link-Live Cloud Service" on **page 245**.) To download major releases, you must have Gold Support.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section and tap **Software Update**.

3 On the Update Software screen, touch the **CHECK UPDATE** button. A pop-up dialog box informs you if an updated firmware version is available.

4 Touch **YES** to download the firmware.

5 Select a storage location for the update file by answering **YES** or **NO** when the options are shown. After you touch **YES**, the **.img** file will download to the selected location.

6 Navigate to the directory where you saved the new software image file, and select the file.

7 Select the **OK** button to install the new firmware.

8 Select **OK** again to confirm.

The new file will be installed and the analyzer will restart. The process will take several minutes.

Options

If you did not purchase your OneTouch AT 10G analyzer with all options enabled, you can purchase and activate options at a later time.

Enter an option's product key to activate the new option.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section.

3 Tap **Options**.

4 Enter the product key. You may be asked to restart the analyzer by cycling power to the analyzer.

To purchase options, contact NETSCOUT. See page 17 for contact information.

Export Logs

If you have reason to contact our Technical Assistance Center, you may be asked to send log files from the analyzer to the customer service representative.

1 On the HOME screen, tap **TOOLS**  .

2 Scroll down to the Maintenance Tools section.

3 Tap **Export Logs**.

4 Ensure that an SD card is inserted in the analyzer.

5 Tap **OK** to export the log files to the SD card.

Factory Defaults

Use this feature to restore factory settings and erase all user data.

You can select from two options: Quick or Full. Both options restore factory settings and erase user data with particular differences.

The Full option rewrites internal persistent memory to prevent recovery of data. Use this option when security is a concern and

you need to ensure that all user data is securely erased. The procedure may take as long as 30 minutes to complete.

The Quick option is less thorough and typically completes within two minutes.

Data stored on an SD card will not be erased by either option.

It is important that the restoration process is not interrupted while it is in progress.

User data items include

- Profiles
- Authentication credentials
- Test results
- Screen captures
- Reports

Factory default items include

- Number format
- Length units
- Backlight
- Power-down timeout periods

To restore factory settings:

1 Connect the AC adapter to your analyzer.

2 On the HOME screen, tap **TOOLS**  .

3 Scroll down to the Maintenance Tools section and tap **Factory Defaults**.

4 Tap the **Quick** or **Full** button.

Chapter 9: Packet Capture

Packet capture is the process of recording network traffic in the form of packets.

Packet capture and analysis can be used to:

- Analyze network problems
- Debug client/server communications
- Track applications and content
- Ensure that users are adhering to administration policies
- Verify network security

The OneTouch AT 10G analyzer can silently monitor and record network traffic. This is called Standalone Capture. The analyzer can also record all traffic to and from itself during AutoTest. This is called AutoTest Capture.

The analyzer saves captured packets to a .cap file on the SD card. Files are stored in pcap format.

The saved capture file can be analyzed with ClearSight Analyzer or other packet capture analysis software.

General Information

Using Packet Capture Filters

Capture filtering lets you capture and analyze only packets that are pertinent to the problem you are troubleshooting and solving.

For example:

- You can create a wired packet capture filter to capture only packets that are related to a specific application (based on IP address and port number).

- You can create a wired packet capture filter to capture only packets that are going to and from a particular server or client.

Filters Perform a Logical AND Operation

When you set more than one filter, a logical AND operation is performed using the filters that you select.

For example, if you enter an IP address filter of 10.250.0.70 and a port filter of 80, only packets that are going to and from port 80 and to or from 10.250.0.70 will be captured. See Figure 81.

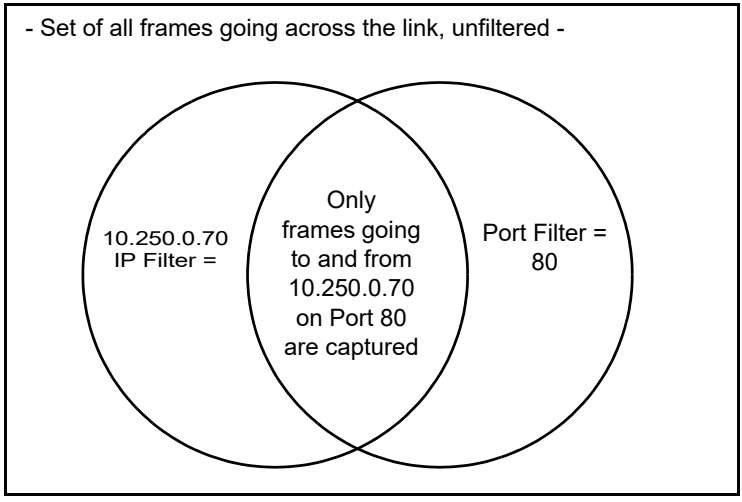


Figure 81. Capture Filters - Logical AND Operation

Packet Capture Speed and Dropped Frames

Note

The terms "packet" and "frame" are used interchangeably herein, though a frame is actually an encapsulated packet.

Capture performance is a function of frame size and the burst characteristics of the signal, coupled with SD card write speed.

You can use a Filter or the Slice Size control to reduce the likelihood of dropped packets.

SD Card

Use the supplied SD card for optimal performance. Use of other SD cards may result in slower write performance and increased possibility of dropped packets.

Connecting for Packet Capture

The OneTouch AT 10G is capable of single-ended packet capture, where the analyzer captures the traffic it detects at its test port. When performing single-ended packet capture, the analyzer is typically connected to a span port, mirror port, or tap.

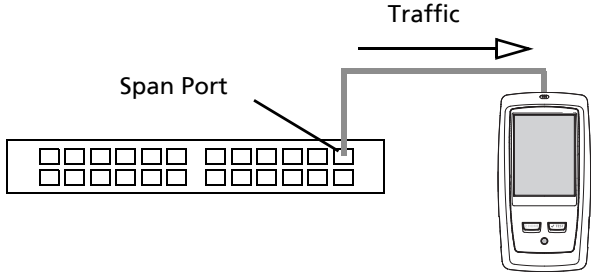


Figure 82. Single-Ended Packet Capture

Configuring and Running Packet Capture

1 On the HOME screen, tap **TOOLS** .

2 In the **Testing Tools** section, tap **Capture**.

The CAPTURE screen is displayed.

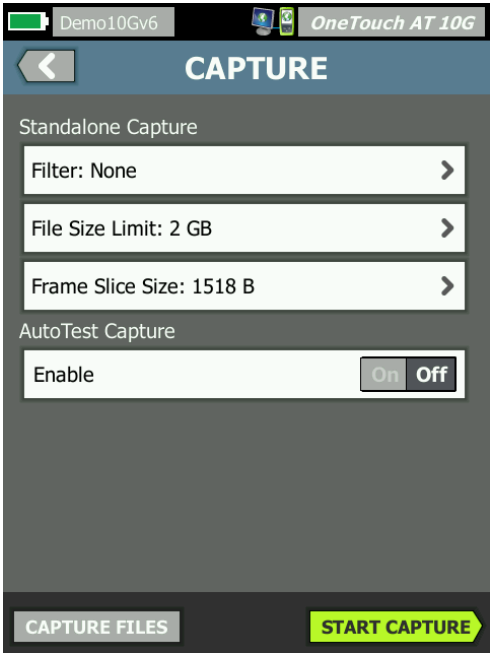


Figure 83. The Wired CAPTURE Screen

3 Tap **Filter** and set filter values. The following settings are available:

MAC - When you enter the MAC address of a host, only packets that contain the host's MAC address as the source or destination will be captured.

VLAN - When you enter a VLAN number, only traffic that is tagged for the specified VLAN will be captured.

IP - When you enter the IP address of a host, only traffic to and from the host will be captured. Only an IPv4 address can be specified.

Port - When you specify a port number, only traffic to and from the specified UDP or TCP port will be captured. For example, to

capture only HTTP traffic, specify port 80.

NOT - Tap **On** to invert your filter selections. If you have selected multiple filters, the NOT function will give the inverse of the aggregated filter results. For example, if you have set up a filter to capture traffic to and from 10.250.0.70 on port 80, and you select **NOT**, all traffic will be captured *except* traffic to and from 10.250.0.70 on port 80.

IPv6 - Tap **On** to filter on IPv6 traffic. Do not turn this parameter on if you have specified an IP address in the above **IP** address field.

4 Set the **File Size Limit** and the **Frame Slice Size** to limit / control the amount of data that will be captured.

File Size Limit - The analyzer can save up to 2 GB of traffic in each capture file. You can select a smaller file size if desired. The capture will stop before exceeding the selected file size.

Frame Slice Size - The Frame Slice Size control limits how much of each packet is captured. If you select 64 B, the first 64 bytes of each packet will be captured. This is useful when you are interested in the packet's header, but you don't need to see all the payload data. You can also use slice size to control the amount of data captured, and thereby reduce the possibility of dropped frames.

5 Enable **AutoTest Capture** to cause the analyzer to capture traffic automatically when AutoTest is run.

Start Packet Capture

To start packet capture:

1 On the CAPTURE screen, tap the **START CAPTURE** button. The CAPTURE FILENAME screen is displayed.

By default, the capture file name format is as follows:

- cap–<date><time>.pcap (wired capture files)

2 You can use the keyboard to change the capture file name if desired. The .cap extension cannot be changed.

3 Tap the **DONE** button. File capture begins.

As a wired packet capture progresses, unicasts, broadcasts, multicasts, error frames, total captured frame count, and the number of dropped packets are shown for connected test port.

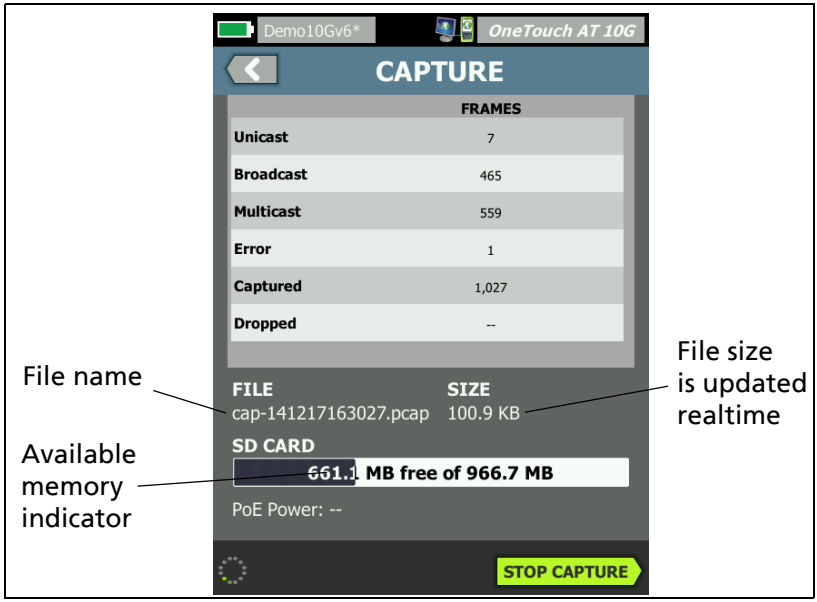


Figure 84. Wired Capture Results

The **SD CARD** indicator bar gives a quick visual indication of how much storage space is available on the SD memory card.

Stop Packet Capture

The capture is terminated in any of the following conditions.

- the maximum file size (set in Limits) is reached
- the memory card is full
- you tap the **STOP CAPTURE** button

Note

Do not remove the SD card from the OneTouch analyzer until the **START CAPTURE** *button re-appears. Failure to wait for the* **START CAPTURE** *button to re-appear may result in loss or corruption of SD card data.*

AutoTest Capture

The OneTouch AT 10G analyzer can capture traffic to and from the analyzer during AutoTest. The capture file can be examined to obtain detailed troubleshooting information.

When AutoTest Capture is enabled, each time you run AutoTest the analyzer captures wired traffic to and from the analyzer. If you don't save the capture, it is overwritten the next time you run AutoTest.

To Enable or Disable AutoTest Capture

1 Tap the TOOLS icon on the HOME screen.

2 Tap the **Capture** button.

3 In the AutoTest Capture section, set **Enable** to On.

The setting is stored in the Profile.

To Save an AutoTest Capture

1 Run AutoTest.

2 When AutoTest completes, tap the OneTouch AT 10G button OneTouch AT 10G at the upper right corner of the HOME screen.

3 Tap the **Save AutoTest Capture** button.

Note

This button only appears when AutoTest Capture is enabled and AutoTest has completed. The same button appears on the CAPTURE screen in the TOOLS menu.

The CAPTURE FILENAME screen is displayed.

By default, the capture file name format is pcap–<date><time>.pcap

You can use the keyboard to change the capture file name if desired. The .pcap extension cannot be changed.

4 Tap the **DONE** button. The AutoTest capture file is saved on the SD card.

The AutoTest capture file size is limited to 32 MB.

AutoTest capture may impact User Test performance if User Tests generate a high volume of network traffic.

AutoTest ends when the last user test completes, before wired analysis begins.

Managing Capture Files

Captures are stored as .cap files on the SD card. You can view the list of captured files as follows:

1 After stopping the capture, tap the back button  .

2 Tap the **CAPTURE FILES** button 

.

The list of capture files is displayed. You can use the buttons at the bottom of the screen to delete or rename capture files.

To move or copy capture files to a PC, eject the SD card and insert it in the PC. Or see “Managing Files” on page 229.

Analyzing Capture Files

You can use ClearSight Analyzer software or other protocol analysis software to analyze the captured packets on a PC.

Chapter 10: Managing Files

The following types of files can be managed:

- Profiles
- Reports
- Screens
- Certificates
- Packet captures

Profiles, Reports, and Screens can be managed using the built-in file manager. File management operations include loading, viewing, importing, exporting, renaming, or deleting files.

Certificates can be loaded using the Wired 802.1X settings dialog. See page 184.

Packet captures can be managed using the Capture tool. See page 228.

Using the Built-in File Manager

To manage files using the built-in file manager:

1 On the HOME screen, tap **TOOLS** .

2 Scroll down to the File Tools section.

3 Tap **Profiles, Reports, or Screens**, depending on the type of file you want to manage. The corresponding file manager screen appears. The figure below shows each of the four types of file manager screens.

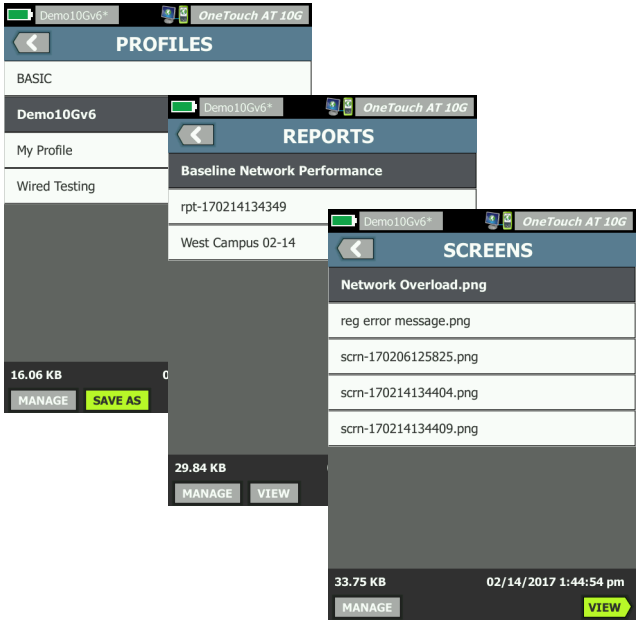


Figure 85. The Three File Manager Screens

The following section describes buttons that are available on one or more of the file manager screens.

SAVE

The **SAVE** button saves the current profile or report.

When you tap the **SAVE** button, the SAVE AS screen is displayed.

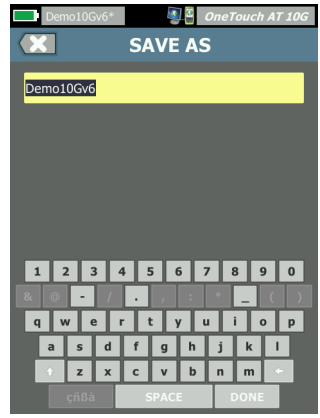


Figure 86. SAVE AS Screen

You can tap the **DONE** button to save the file with the suggested file name, or you can use the keyboard to change the name.

VIEW

The **VIEW** button is available in the REPORTS file manager and the SCREENS file manager.

LOAD

The **LOAD** button is available in the PROFILES file manager.

When you tap the **LOAD** button, the current profile is replaced by the one you load. Consider saving the current profile before you tap the **LOAD** button.

The **LOAD** button puts the highlighted profile into use. A loaded profile can be modified and re-saved using the same name or a different name. When a profile has been modified, an asterisk appears after its name in the shortcut bar. See “Shortcut Bar” and “Profile Name” on page 30.

MANAGE

Profiles, reports, and screens each have their own directory in analyzer's internal memory. Tap the **MANAGE** button to manage files in the Profiles, Reports, or Screens directory. Then tap the file that you want to manage.

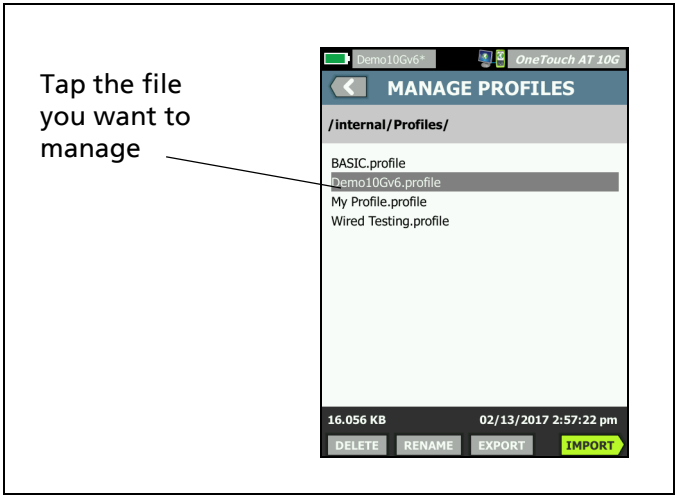


Figure 87. Manage Profiles Screen

DELETE

DELETE permanently removes the file from the list and from memory. You must tap the **MANAGE** button and select a file in the list to make the **DELETE** button available.

RENAME

RENAME lets you change the name of a profile, report, or screen. You must tap the **MANAGE** button and select a file in the list to make the **RENAME** button available.

The file's extension cannot be changed using the built-in file manager. A file named LabNetwork.profile will retain the .profile extension even if you change its name. The file's extension should not be changed using any file management tool.

EXPORT

EXPORT lets you save a copy of the file to internal memory, an SD card, or a USB flash drive. Tap the **EXPORT** button to show the navigable file tree.

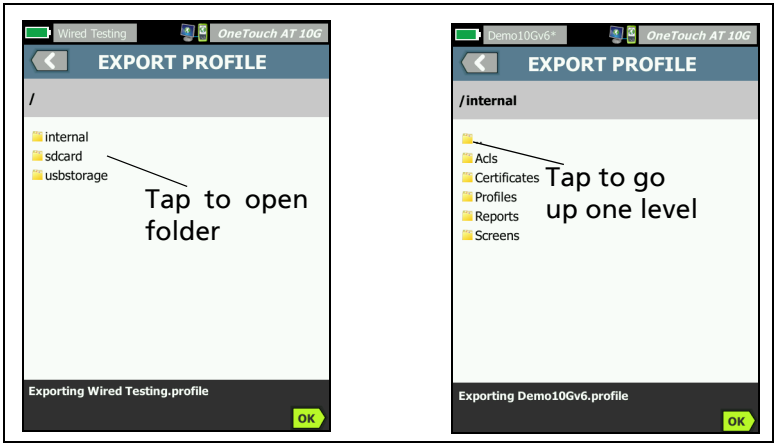


Figure 88. File Manager - Export File Tree

Navigate to the desired location and tap the **OK** button to save a copy of the file.

IMPORT

To import a profile, report, or screen:

1 Put the file to be imported on an SD card or USB flash drives.

2 Insert the SD card or connect the flash drive to the analyzer.

3 In the file manager, tap the **MANAGE** button.

4 Tap the **IMPORT** button.

5 Navigate to the file to be imported and tap it.

6 Tap the **OK** button.

The file is imported.

Note that the file will not appear in the file manager's file list if it does not have the correct extension.
Profiles must have the .profile extension,
reports must have the .pdf extension, and
screens must have the .png extension to be displayed in the file list. You can import other file types but they will not be displayed in the file manager's list.

Remote User Interface and File Access

You can access the analyzer remotely when you connect to its management port.

Remote control of the OneTouch analyzer's user interface is possible via a VNC client connection and in the **"Link-Live Cloud Service"**.

Note

For more information on accessing and remote controlling your OneTouch in Link-Live, see Chapter 12: "Link-Live Cloud Service, " beginning on **page 245***.*

To remotely access the file system, connect via Link-Live, FTP, a web browser, or a mapped network drive (WebDAV).

You can set up remote access security by configuring the OneTouch analyzer's management port.

User Interface Remote Control

Remote Control Using a VNC Client

To connect to the analyzer using a VNC Client:

1. Obtain the IP address of the management port as described on page 211.
2. Provide the analyzer's management port IP address to your VNC client.
3. Connect using your VNC client.

4 If required, enter the analyzer's remote access **user** name and **password**. See "Configure Login Credentials for Remote Access" on **page 213.**

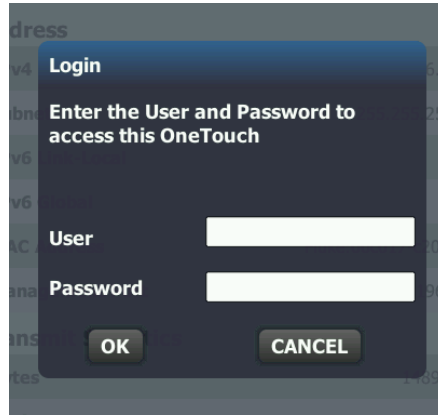


Figure 89. Browser Remote Access Login Credentials

5 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.

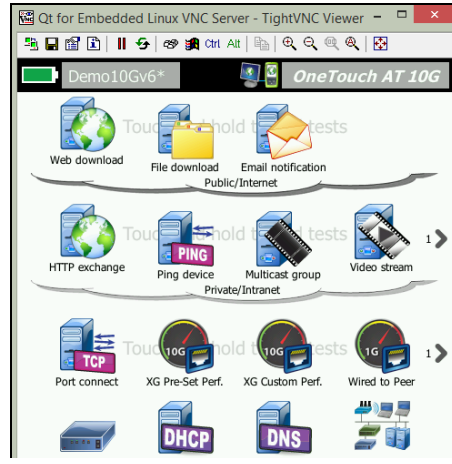


Figure 90. Remote Access OneTouch Home Screen

Remote Control Using the Link-Live Cloud Service

See "Remote Access from the Cloud" on **page 250**.

Remote File Access

You can remotely access files on the analyzer using an FTP, Link-Live, a web browser, or a network drive mapped with WebDAV.

Remote File Access Using a Web Browser

To access the OneTouch analyzer's user file system using a web browser:

1. Obtain the IP address of the management port as described on page 211.
2. Open a web browser.
3. Enter the OneTouch analyzer's Management Port IP address in the web browser's field.
4. If required, enter the OneTouch analyzer's remote access **user** name and **password**. See also: "Configure Login Credentials for Remote Access" on **page 213**.

Figure 91. OneTouch Web Server Home

5. Select the **Files** button.

6 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.

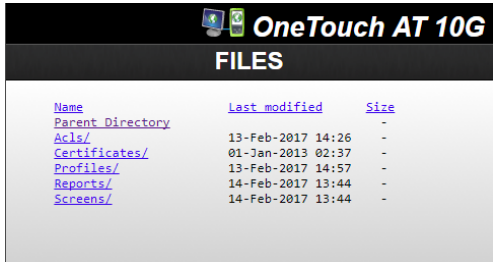


Figure 92. OneTouch Remote File Access

7 To download an item, right click its name, and select "**Save [target/link/image] as...**".

Note

You cannot delete, rename, move, or upload files using a Web Browser.

Remote File Access Using an FTP Client

To connect to the analyzer's user file system with an FTP Client:

1 Obtain the IP address of the management port as described on page 211.

2 Provide the analyzer's management port IP address to the FTP client.

3 Always use Anonymous as the user name, even if you have User/Password security enabled.

4 If you have User/Password security enabled, then use the password entered there. Otherwise, leave the password empty.

5 Once connected, your FTP client will be able to browse the analyzer's files.

Remote File Access Using a Mapped Network Drive (WebDAV)

The OneTouch AT 10G supports integration of its user file system into Windows Explorer as a network drive.

The following instructions explain how to map to the analyzer's user file system from a Windows computer.

1. Obtain the IP address of the management port as described on page 211.
2. Select the Windows **Start** button, or open **File Explorer.**
3. Right-click **Computer** or **This PC**.
4. Select **Map network drive...**.
5. In the Map Network Drive dialog, select an available drive letter.
6. Enter the path to your analyzer. For example: http://10.250.50.4/files. Be sure to add /files after the address.
7. You may be asked for a **user** name and **password** if the user and password credentials are enabled on the analyzer's management port. See also: "Configure Login Credentials for Remote Access," beginning on **page 213**.

You may experience delays when using the network drive if there is no proxy server between the computer and the analyzer. Microsoft has documented this issue and the solution at: **http://support.microsoft.com/kb/2445570**

Other Remote Access Information

Disconnect a Remote User

Remote control users connected to the analyzer through a web browser or a VNC client can be disconnected through the selection of the Remote Access icon  .

1 Tap the Remote Access icon on the analyzer.

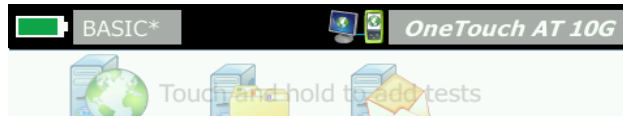


Figure 93. Remote Access icon located in Shortcut Bar

2 Select the **Disconnect** button.

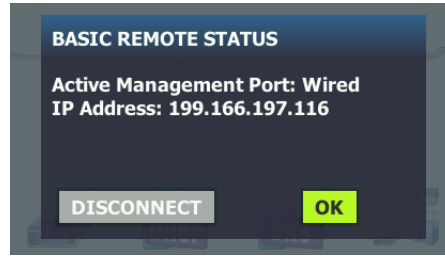


Figure 94. Management Port Status dialog - Remote Control Disconnect

3 A remote user's IP address is shown on the same dialog box as the Disconnect button.

Notes about Remote Controlling the OneTouch AT 10G

- Use the Up/Down arrows or the PgUp and PgDn keys to scroll vertically.
- Use your pointing device (mouse, touch screen, etc.) to select items.
- If another user connects to the analyzer while you are connected, your remote session will be terminated. The analyzer does not support concurrent remote user sessions.

SD Card

To manage files using an SD card, insert it into the analyzer. See "SD card slot" on page 25. The analyzer supports FAT and FAT32 file systems on external media.

USB Flash Drive

To manage files using a USB flash drive, connect it to the analyzer. See “USB-A Connector” on page 24. The analyzer supports FAT and FAT32 file systems on external media.

Chapter 11: Maintenance

Maintenance

⚠Warning⚠

To prevent possible fire, electric shock, personal injury, or damage to the analyzer:

- **The battery is the only user serviceable component. Do not open the case except to replace the battery.**
- **Use only replacement parts that are approved by NETSCOUT.**
- **Use only service centers that are approved by NETSCOUT.**

Clean the Analyzer

To clean the touchscreen, turn off the analyzer, then use a soft, lint-free cloth that is damp with alcohol or a mild detergent solution.

To clean the case, use a soft cloth that is damp with water or a mild detergent solution.

⚠Caution

To prevent damage to the touchscreen do not use abrasive materials.

To prevent damage to the case, do not use solvents or abrasive materials.

Extend the Life of the Battery

To extend the amount of time the battery will provide satisfactory operation before it needs to be replaced:

- Recharge the battery frequently. Do not let the battery discharge completely.
- Do not keep the battery in hot areas.
- Before you put a battery into storage, charge it to approximately 50% of full charge.

Store the Analyzer

- Before you store an analyzer or an extra battery for a long period, charge the battery to approximately 50% of full charge. The discharge rate of the battery is 5% to 10% each month. Check the battery every 4 months and charge it if necessary.
- Keep a battery attached to the analyzer during storage. If you remove the battery for more than approximately 24 hours, the analyzer will not keep the correct time and date.
- See "Environmental and Regulatory Specifications" on **page 253** for storage temperatures.

Remove and Install the Battery

1 Turn off the analyzer.

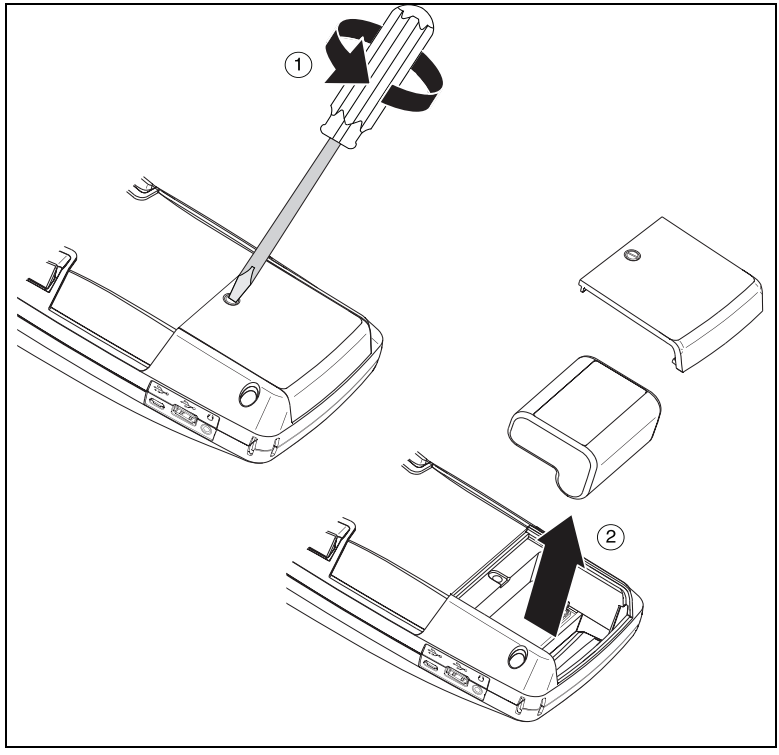
2 Disconnect the AC adapter.

3 Replace the battery as shown in Figure 95.

Use only NETSCOUT battery model 1T-BATTERY.

Note

If you remove the battery and do not connect the AC adapter, the clock keeps the current date and time for a minimum of 24 hours.



GVO003.EPS

Figure 95. Remove and Install the Battery

Chapter 12: Link-Live Cloud Service

Overview

The OneTouch AT 10G allows you to send test results to your Link-Live.com Cloud Service account, where those results can be viewed, organized, and managed from a web-enabled device.

In addition to viewing and analyzing results, you may remotely access your OneTouch AT 10G analyzer through the cloud service, as well as configure your OneTouch to automatically upload reports of your test results to Link-Live for storage and retrieval.

Link-Live Cloud Service Support Page

For detailed information on using the Link-Live Cloud Service to manage your OneTouch AT 10G test results and reports, go to **https://app.link-live.com/support**, or from Link-Live.com, click **Support** > **Questions**.

Infrastructure and User Tests in the Cloud

Test result trends from the following tests can be managed from the cloud:

Infrastructure Tests

- Nearest Switch
- Gateway
- DHCP
- DNS

User Tests

- Ping (ICMP)
- Connect (TCP)
- Web (HTTP)

- File (FTP)
- 1G Wired Performance (RFC 2544)
- Video (RTSP)
- Email (SMTP)

Setting Up and Accessing the Cloud Service

The following steps will help you set up and get started using your Link-Live Cloud Service.

1 Create or sign in to your **Link-Live.com** account.

2 **Claim** your unit.

3 Enable **Upload AutoTest** to send results to Link-Live.

4 Create a unique name for your OneTouch analyzer.

5 Go to Link-Live.com to manage your test results.

To begin setup from the OneTouch HOME screen, tap **TOOLS** and scroll down to **Link-Live Cloud Tools**.

Creating a Link-Live.com Account

To create a Link-Live.com account:

1 Go to **https://app.link-live.com/signup**.

2 Enter the appropriate information on the web page, and click CREATE ACCOUNT.

Claiming Your Unit

The process to claim your analyzer includes both the unit and the Link-Live Cloud website. You must have a user account to claim your unit.

Note

A claimed unit is associated with the currently active Organization. See the Link-Live.com Support page for more information about Organizations.

1 In **Link-Live.com**, navigate to the **Units** page from the left sidebar.

2 Click the **Claim Unit** button at the lower right of the page.

3 Select your device (OneTouch), and follow the prompts on the Link-Live website.

Once your OneTouch analyzer is successfully claimed, you should see a successful claim message on Link-Live.com, and the claim status on the unit should update to **Claimed**.

Setting up Periodic AutoTest

When the analyzer is in Periodic AutoTest mode, the OneTouch analyzer runs AutoTests at specified intervals and sends the results to Link-Live so that you can view the results over time. Periodic AutoTest is helpful when baselining network performance or troubleshooting intermittent problems.

Periodic AutoTesting can be set up only after a unit has been claimed. Your unit must be connected to a network for this process to work. Your results can be sent through either of the network test ports or the management port.

To enable Periodic AutoTest:

1 Select **TOOLS** from the HOME screen.

2 Under **Link-Live Cloud Tools**, select **Periodic AutoTest.**

Note

A shortcut to the Periodic AutoTest screen is to touch and hold the Test button on a unit's HOME screen.

3 Configure the following:

Duration - The length of time during which test results will be sent to the Link-Live Cloud. The duration can be set to Unlimited Duration, 2, 5, 10, and 30 minutes, or 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hrs, 8 hrs, and 12 hrs, or 1 day, 2 days, 3 days, 4 days, 5 days, or 1 week, or 2 weeks.

Interval - This is the amount of time between sent test results

to the Link-Live Cloud over a selected time duration.

Comment - This entry will appear beneath the Periodic AutoTest results in Link-Live Cloud Service. Use this feature to annotate your Periodic AutoTest session.

Backlight Timeout - This feature controls how long the OneTouch screen's backlight stays illuminated while Periodic AutoTesting is ongoing.

This option is disabled by default. You can set the backlight to turn off automatically after 5, 10, or 15 minutes, extending the life of the screen. When the backlight turns off, you can tap the screen to turn it back on.

4 Tap the **Launch** button.

Periodic AutoTest setup is successful when a translucent PERIODIC AUTOTEST STATUS screen is displayed on the unit's HOME screen and shows an IP address.

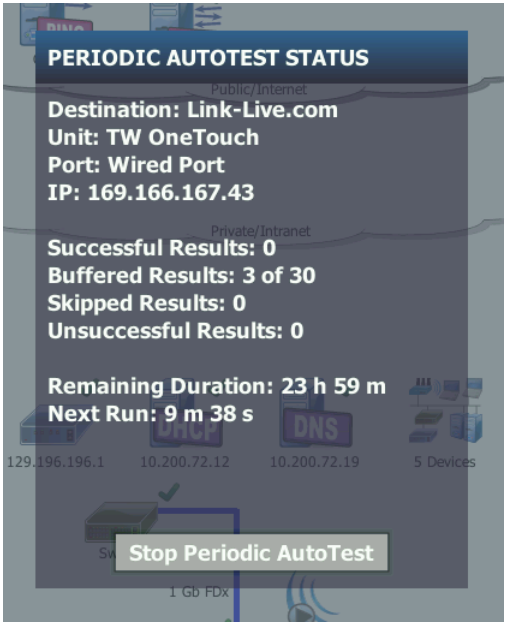


Figure 96. Periodic AutoTest Status Screen

Periodic AutoTest Status Screen

The Periodic AutoTest Status screen (Figure 96) shows the following information:

Destination: shows the web location of where the AutoTest results are sent.

Unit: shows the unit name.

Port: the port that the Periodic AutoTest process will use to send results to the cloud. It can be the network test ports, the RJ-45 management port, or the optional Wi-Fi management port.

IP: the IP address of the Periodic AutoTest port currently in use.

Successful Results: the number of successful runs to Link-Live.com after the completion of an AutoTest, regardless if the AutoTest passed or failed.

Skipped Results: If an AutoTest run did not complete during the time assigned for the interval, that run will be skipped. For example, if the assigned interval was 1 minute long and the AutoTest is taking 3 minutes to complete (for various reasons: test retries, port issues, etc), the assigned interval time will be too short and the run will be skipped.

Unsuccessful Results: The number of unsuccessful runs to Link-Live.com after the completion of an AutoTest, regardless if the AutoTest passed or failed.

Remaining Duration: The amount of time left in a specified Periodic AutoTest duration. Refers to the Duration time assigned on the OneTouch AT 10G in **Tools > Link-Live Cloud Tools > Periodic AutoTest**.

Next Run: The amount of time until the next AutoTest run begins. Refers to the interval time assigned on the unit in **Tools > Periodic AutoTest**.

Naming your OneTouch AT 10G

By default, the analyzer's name is its serial number. We recommend that you rename your OneTouch AT 10G to a familiar or descriptive name.

Note

When you claim a OneTouch AT 10G unit to Link-Live Cloud Service, the name entered on Link-Live is reassigned to the OneTouch.

To rename your analyzer on the unit:

1 On the analyzer HOME screen, tap **TOOLS** .

2 In the **Link-Live Cloud Tools** section, tap **Unit Name.**

3 Enter a descriptive name for your OneTouch AT 10G.

4 Tap **DONE** when finished.

Remote Access from the Cloud

You can connect remotely to a claimed OneTouch AT 10G analyzer and choose to control the analyzer or view its user files on Link-Live.com.

The claimed unit must be part of your organization or belong to an organization of which you are a member.

Preparing Your Unit for Remote Access

Before your analyzer can be accessed from the Link-Live Cloud, the **Cloud Remote** option needs to be enabled on the unit.

Note

If the unit is not enabled for remote cloud access, it can still be accessed from a browser (outside of the cloud account) via the management port address.

To enable remote cloud access:

1 On the analyzer's HOME screen, tap **TOOLS** .

2 In the **Cloud Tools** section, touch the **Cloud Remote** button to open the CLOUD REMOTE screen.

3 Enable remote access to the OneTouch by switching the toggle to **On**.

A **Cloud Remote icon**  will be shown on the unit at the top of the screen.

Chapter 13: Specifications

Environmental and Regulatory Specifications

Operating temperature[1]	32°F to 122°F (0°C to 50°C)
Storage temperature[2]	-40°F to 160°F (-40°C to 71°C)
Operating relative humidity (% RH without condensation)	5% to 45% at 32°F to 122°F (0°C to 50°C) 5% to 75% at 32°F to 104°F (0°C to 40°C) 5% to 95% at 32°F to 86°F (0°C to 30°C)
Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	CAN/CSA-C22.2 No. 61010-1-04 IEC 61010-1:CAT none, pollution degree 2
Operating altitude	13,123 ft (4,000 m) 10,500 ft (3,200 m) with AC adapter
Storage altitude	39,370 ft (12,000 m)
Pollution degree	2
EMC	EN 61326-1:portable

1 The battery will not charge if its temperature is outside the range of 32°F to 104°F (0°C to 40°C).

2 Do not keep the battery at temperatures below -4°F (-20°C) or above 122°F (50°C) for periods longer than one week. If you do, the battery capacity can decrease.

Cables

Cable types	100 Ω Unshielded Twisted Pair (UTP) LAN cables. 100 Ω Shielded or Screened Twisted Pair (SeTP) LAN cables. TIA Category 3, 4, 5, 5e, and 6. ISO Class C, D, E and F.
Cable length measurement	Measurable cable lengths are from 3 feet (1 meter) to 656 feet (200 meters). Accuracy: ± 10m (~30 ft). Length measurement is based on Nominal Velocity of Propagation (NVP) for CAT 5e cable.

Network Ports

Network analysis ports	One RJ-45 100/1000/10GBASE-T Ethernet One SFP / SFP+ Fiber (Ethernet) that supports 1000Base-X (SFP) and 10GBase-SR/LR (SFP+)
Not for connection to telephone networks	The OneTouch AT 10G analyzer is NOT designed for connection to a telephone network. The OneTouch AT 10G analyzer is NOT designed for connection to an ISDN line. Do not connect to a telephone network or ISDN line except through a regulatory agency compliant computer network modem device.

Supported Network Standards

IEEE 100BASE-T **IEEE 1000BASE-T** **IEEE 100BASE-FX** **IEEE 1000BASE-X** **IEEE 10GBASE-T** **IEEE 10GBASE-LR** **IEEE 10GBASE-SR**	RFCs and standard MIBs used: 1213, 1231, 1239, 1285, 1493, 1512, 1513, 1643, 1757, 1759, 2021, 2108, 2115, 2127, 2233, 2495, 2515, 2558, 2618, 2737, 2790, 2819, 3592, 3895, 3896, 4188, 4502.

SFP+ Adapters

The OneTouch AT 10G analyzer supports 1000Base-X (SFP) and 10GBase-SR/LR (SFP+)

Power

AC adapter	Input: 100-240 Vac, 50-60 Hz, 1.0 A Output: +15 Vdc, 2.0 A
Battery type	Lithium ion battery pack, 7.2 V
Battery life	Approximately 3-4 hours. Life varies depending on type of usage.
Charge time	4 hours to charge from 10% capacity to 90% capacity with the analyzer powered-off.

Certifications and Compliance

CE	Conformite Europeene. Conforms to the requirements of the European Union and the European Free Trade Association (EFTA).
C SP US	Listed by the Canadian Standards Association.
	The Product complies with Australian standards.
	Conforms to relevant South Korean EMC Standards

Electromagnetic Compatibility. Applies to use in Korea only. Class A Equipment (Industrial Broadcasting & Communications Equipment)	This product meets requirements for industrial (Class A) electromagnetic wave equipment and the seller or user should take notice of it. This equipment is intended for use in business environments and is not to be used in homes.

Memory

Internal memory	The OneTouch AT 10G analyzer has 2 GB of internal memory that is shared between system and user files. The built-in file managers can be used to import and export files.
SD card	The packet capture feature functions optimally when the supplied SD card is used. Use of other types of SD cards may result in reduced performance. FAT and FAT32 file systems are supported.
USB 2.0 port	The OneTouch AT 10G analyzer has a USB 2.0 type A port, for use with USB mass storage devices, such as USB flash drives. FAT and FAT32 file systems are supported.

Headset Jack

3.5 mm, 4-conductor jack

Dimensions

With module and battery installed:

10.3 in x 5.3 in x 2.9 in (26.2 cm x 13.5 cm x 7.3 cm)

Weight

With module and battery installed: 3.5 lb (1.6 kg)

Display

5.7 inch (14.5 cm), 480 x 640 pixel LCD display with a projected capacitance touchscreen.

Regulatory Information

This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A

digital device pursuant to Part 15, Subpart J of the FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of the equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Korea Statements

<table>
<tr><td colspan="2">당해 무선설비는 전파혼신 가능성이 있으므로
인명안전과 관련된 서비스는 할수 없음</td></tr>
<tr><td colspan="2">(This device shall not be used for life-safety related service
due to the possibility of radio interference.)</td></tr>
<tr><td>A급 기기
(업무용 방송통신기자재)</td><td>이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.</td></tr>
<tr><td>(Class A Equipment
(Industrial Broadcasting
& Communication
Equipment))</td><td>This product meets requirements for industrial (Class A) electromagnetic wave equipment and the seller or user should take notice of it. This equipment is intended for use in business environments and is not to be used in homes.</td></tr>
</table>

— Notes —

— Notes —