FLUKE networks®

OneTouch™ AT

Network Assistant

Users Manual

Released 5/2012. Rev. 2, 05/2013

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Each Fluke Networks product is warranted to be free from defects in material and workmanship under normal use and service. The warranty period for the mainframe is one year and begins on the date of purchase. Parts, accessories, product repairs and services are warranted for 90 days, unless otherwise stated. Ni-Cad, Ni-MH and Li-Ion batteries, cables or other peripherals are all considered parts or accessories. The warranty extends only to the original buyer or end user customer of a Fluke Networks authorized reseller, and does not apply to any product which, in Fluke Networks' opinion, has been misused, abused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke Networks warrants that software will operate substantially in accordance with its functional specifications for 90 days and that it has been properly recorded on non-defective media. Fluke Networks does not warrant that software will be error free or operate without interruption.

Fluke Networks authorized resellers shall extend this warranty on new and unused products to end-user customers only but have no authority to extend a greater or different warranty on behalf of Fluke Networks. Warranty support is available only if product is purchased through a Fluke Networks authorized sales outlet or Buyer has paid the applicable international price. Fluke Networks reserves the right to invoice Buyer for importation costs of repair/replacement parts when product purchased in one country is submitted for repair in another country.

Fluke Networks warranty obligation is limited, at Fluke Networks option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke Networks authorized service center within the warranty period.

To obtain warranty service, contact your nearest Fluke Networks authorized service center to obtain return authorization information, then send the product to that service center, with a description of the difficulty, postage and insurance prepaid (FOB destination). Fluke Networks assumes no risk for damage in transit. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB destination). If Fluke Networks determines that failure was caused by neglect, misuse, contamination, alteration, accident or abnormal condition of operation or handling, or normal wear and tear of mechanical components, Fluke Networks will provide an estimate of repair costs and obtain authorization before commencing the work. Following repair, the product will be returned to the Buyer transportation prepaid and the Buyer will be billed for the repair and return transportation charges (FOB Shipping point).

THIS WARRANTY IS BUYER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY.

Since some countries or states do not allow limitation of the term of an implied warranty, or exclusion or limitation of incidental or consequential damages, the limitations and exclusions of this warranty may not apply to every buyer. If any provision of this Warranty is held invalid or unenforceable by a court or other decision-maker of competent jurisdiction, such holding will not affect the validity or enforceability of any other provision.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Contents

Chapter 1: Get Acquainted

Chapter 2: Get Started

Chapter 3: Network Infrastructure Tests

Chapter 4: User Tests

Chapter 5: Profiles

Chapter 6: Wired Analysis

Chapter 7: Wi-Fi Analysis

Chapter 8: Tools

Chapter 9: Packet Capture

Chapter 10: Managing Files

Chapter 11: Maintenance

Chapter 12: Specifications

List of Figures

Chapter 1: Get Acquainted

Overview of Features

The OneTouch™ AT 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

The OneTouch analyzer answers questions such as:

- Can I connect to the wired and Wi-Fi networks?
- Are basic services such as DHCP and DNS operational?
- Can I access the Internet from the network?
- Are my email and FTP servers working?
- Can I receive multicast video?
- What is the performance of my wired/Wi-Fi network infrastructure?

The analyzer features:

- User-configurable tests
- User-configurable Profiles
- Complete L1/L2 measurements of any media type
    - Two copper/RJ45 and two Fiber/SFP Ethernet ports
    - One 802.11a/b/g/n Wi-Fi interface
- Network services measurements

- USB Type A port
- Wired Performance test using a Peer or Reflector
- Wi-Fi Performance test with the option of using a Peer or Reflector
- Built-in 10/100 Mbps management port
- Ethernet packet capture and Wi-Fi packet capture

Safety Information

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

Table 1. International Electrical Symbols

⚠	Warning or Caution: Risk of damage or destruction to equipment or software. See explanations in the manuals.
⚠	Warning: Class 1 laser when an SFP module is installed. Risk of eye damage from hazardous radiation.
⏻	This key turns on the OneTouch analyzer.
🗑	Do not put products containing circuit boards into the garbage. Dispose of circuit boards in accordance with local regulations.

⚠Warning: With an SFP fiber adapter installed, the product contains a Class 1 laser.⚠

To prevent possible eye damage caused by hazardous radiation and to prevent possible fire, electric shock, or personal injury:

- **Carefully read all instructions and safety information before using the product.**
- **Do not look directly into optical connectors. Some optical equipment emits invisible radiation that can cause permanent damage your eyes.**
- **Do not run any tests that activate the SFP's optical output unless a fiber is attached to the output.**
- **The battery is the only user servicable component. Do not open the case except to replace the battery.**
- **Do not modify the OneTouch (the analyzer).**
- **If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment can possibly be impaired.**

- **Do not use the analyzer if it is damaged. Inspect the analyzer before use.**
- **Do not operate the product around explosive gas, vapor or in damp or wet environments.**
- **Do not short-circuit or disassemble the battery pack.**
- **Do not put the battery pack in a fire or an environment with temperatures more than 158 °F (70 °C).**
- **Batteries must be recycled or disposed of properly.**
- **Use only ac adapters approved by Fluke Networks for use with the OneTouch analyzer to supply power to the analyzer and charge the battery.**
- **To prevent unreliable test results, connect the ac adapter or replace the battery as soon as the battery icon turns red.**
- **Do not remove the USB flash drive while the LED on the drive flashes. Doing so can corrupt the data on the USB flash drive.**
- **Use the correct cables and connectors when connecting the product to a network.**
- **Do not connect the analyzer to a telephone line or an ISDN line.**
- **Do not block or restrict the analyzer’s air intake or exhaust ports.**
- **Turn the analyzer off before removing or installing a module.**

Register Your Product

Registering your product with Fluke Networks gives you access to valuable information about product updates, troubleshooting tips, and other support services. To register, fill out the online registration form on the Fluke Networks website at **www.flukenetworks.com**.

Contact Fluke Networks

ℹ **www.flukenetworks.com**

✉ **support@flukenetworks.com**

✉ Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA
1-800-283-5853

☎ +1-425-446-4519

- Australia: 61 (2) 8850-3333 or 61 (3) 9329 0244
- Beijing: 86 (10) 6512-3435
- Brazil: 11 3759 7600
- Canada: 1-800-363-5853
- Europe: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japan: 03-6714-3117
- Korea: 82 2 539-6311
- Singapore: +65-6799-5566
- Taiwan: (886) 2-227-83199
- United States: 1-800-283-5853

Additional Resources

For OneTouch analyzer product information and accessories, see **www.flukenetworks.com**.

The Fluke Networks Knowledge Base answers common questions about Fluke Networks products and provides articles on network troubleshooting and more.

To access the Knowledge Base, log on to **www.flukenetworks.com**, then click **Support** > **Knowledge Base**.

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 page 25) 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 Period" on page 276.

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.

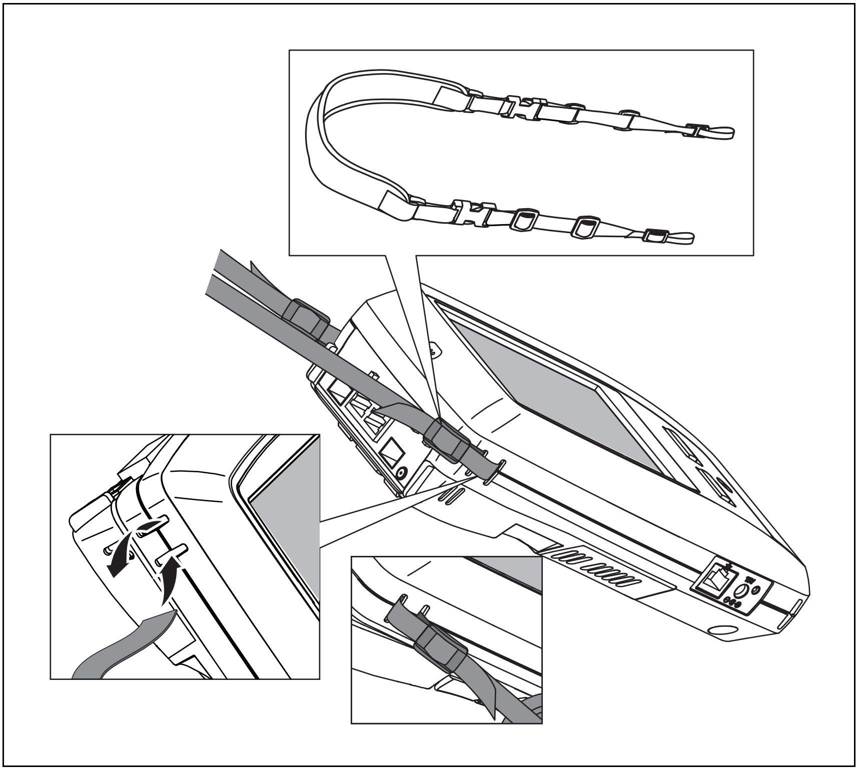


Figure 1. Install and Use the Hand Strap

Test Frame System

The Test Frame System (TFS) is a handheld computer and display platform that accepts modules like the OneTouch AT module. The OneTouch AT module attaches to the TFS as shown below.

Remove and Install a Module

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

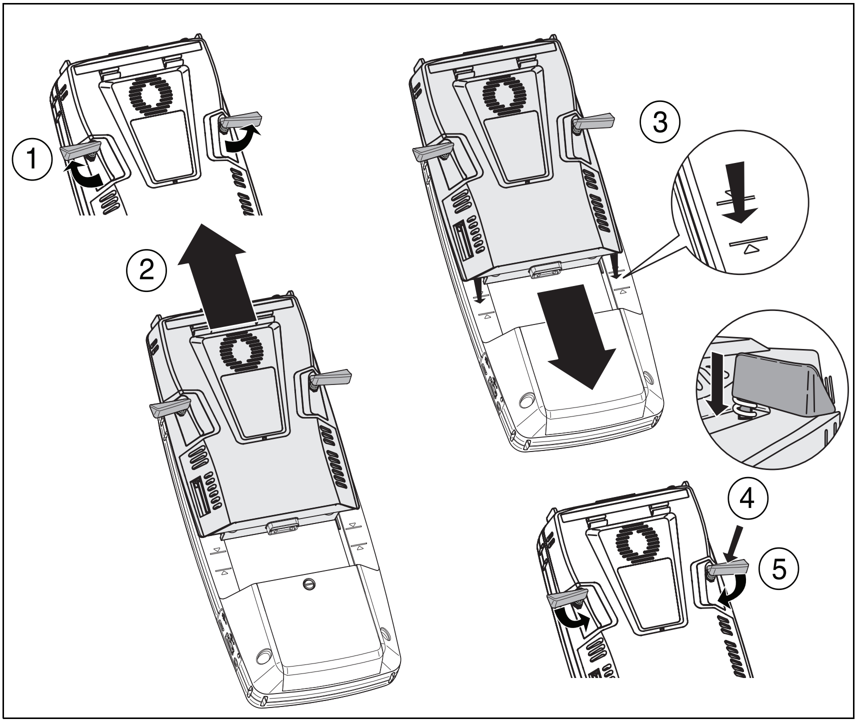
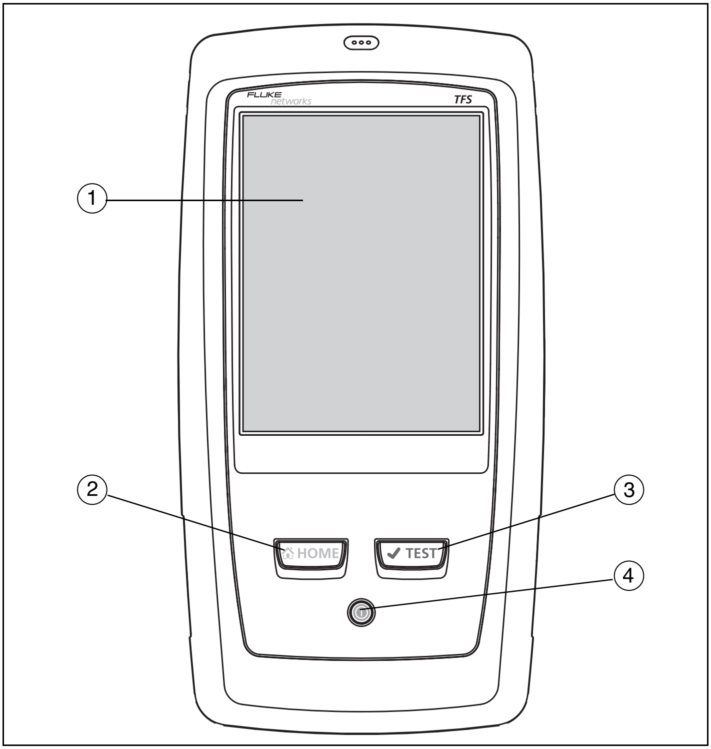


Figure 2. Remove and Install a Module

Connectors, Keys, and LEDs



GVO005.EPS

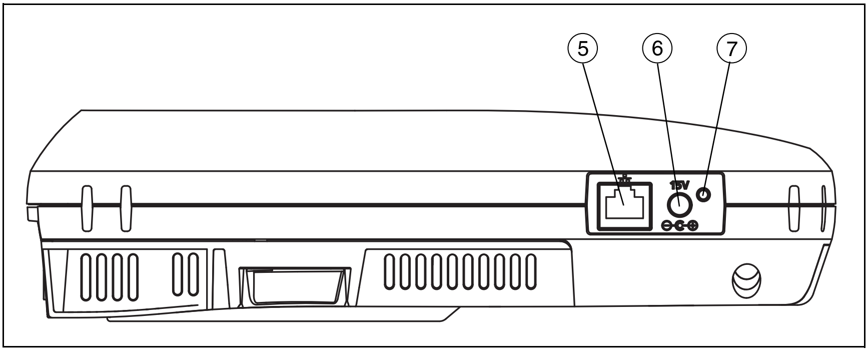
Figure 3. Features of the Main Unit

① **LCD display with touch-screen** - To change the brightness, tap **Tools→Display**. See also: “Touchscreen” on page 31.

② HOME - Press this key to go to the Home screen. See “The HOME Screen” on page 32.

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 19.



GVO006.EPS

Figure 4. Left Side View

⑤ **Management Port** - Connect to the analyzer via this 10 Mbps/ 100 Mbps 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 19.

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

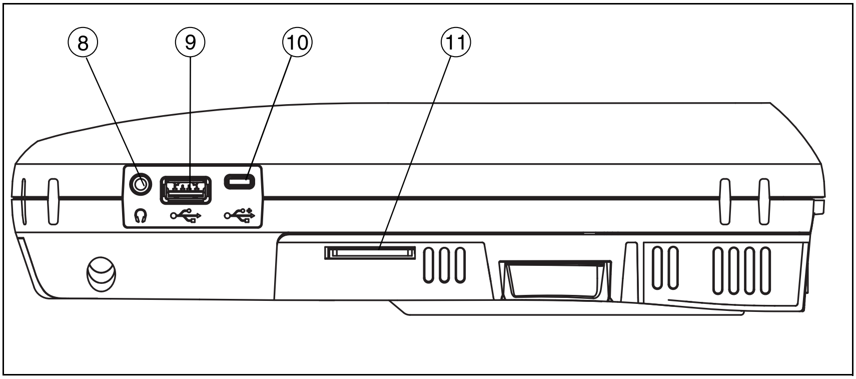


Figure 5. Right Side View

⑧ **Headphone Jack -** You can connect headphones to avoid interrupting nearby people while you’re using the Wi-Fi locate feature.

⑨ **USB-A Connector -** This connector is for managing files on a USB storage devices such as a flash drive. See Chapter 10: "Managing Files," beginning on page 303.

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 303.

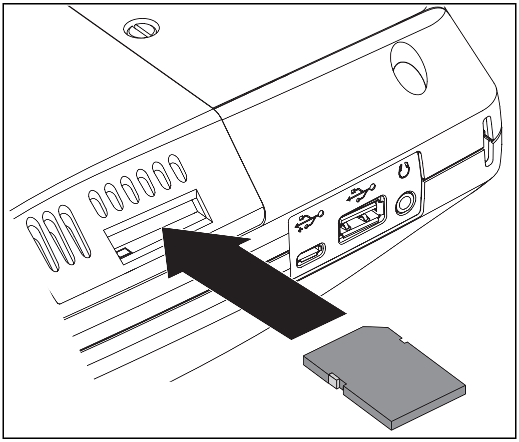


Figure 6. Insert the SD Card

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.

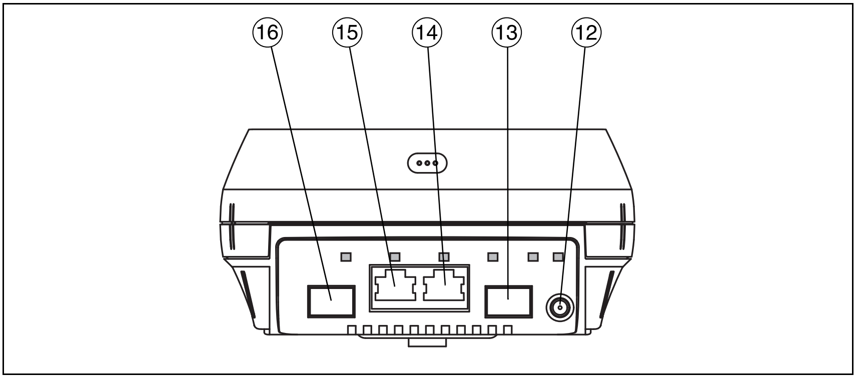


Figure 7. Top End View - Connectors

- ⑫ **External Antenna Connector** (see “Locate Tool” on page 243)
- ⑬ **Fiber Port A** (SFP receptacle)
- ⑭ **Wired Ethernet Port A** (RJ45 connector)
- ⑮ **Wired Ethernet Port B** (RJ45 connector)
- ⑯ **Fiber Port B** (SFP receptacle)

Port A and Port B Connectors

Port A and Port B each have two connectors:

- 10/100/1000 Mbps RJ45 Ethernet connector (for copper connection)
- 100/1000 Mbps standard SFP socket (for fiber connection)

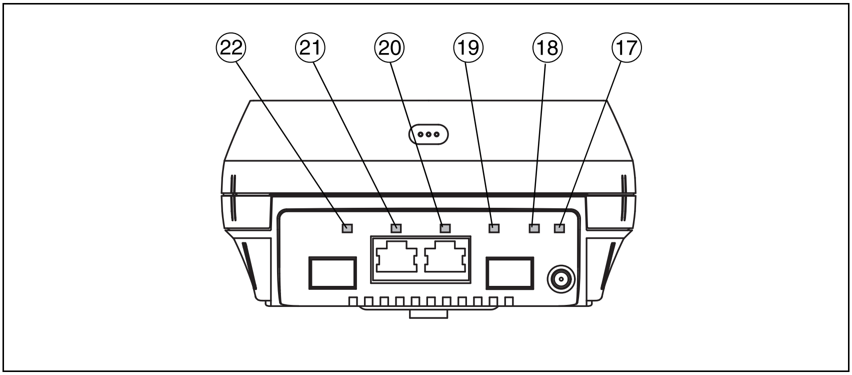
To connect to a network using a copper cable, make a connection to the Port A RJ45 jack. Appropriate cable and fiber types are listed in Chapter 12: "Specifications," beginning on page 323.

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

Port B is used for copper or fiber inline packet capture, packet capture on ports A and B, and for copper cable test.

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

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



GVO008.EPS

Figure 8. Top End View - LEDs

⑰ **Wi-Fi Link/Scanning/Monitoring LED**

⑱ **Wi-Fi Activity LED**

⑲ **Port A Link LED**

⑳ **Port A Activity LED**

㉑ **Port B Link LED**

㉒ **Port B Activity LED**

Receive (Rx)/Link and Transmit (Tx) LEDs

The Management Port and each Ethernet port (Port A, Port B, and Wi-Fi) have two LEDs: “Link” and “Activity.”

Table 2. Link LED

LED State	Meaning
Off	The port is not linked.
Green	Link is established on the port.
Yellow	Wi-Fi scanning or monitoring mode (Wi-Fi port only).

Table 3. Activity LED

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

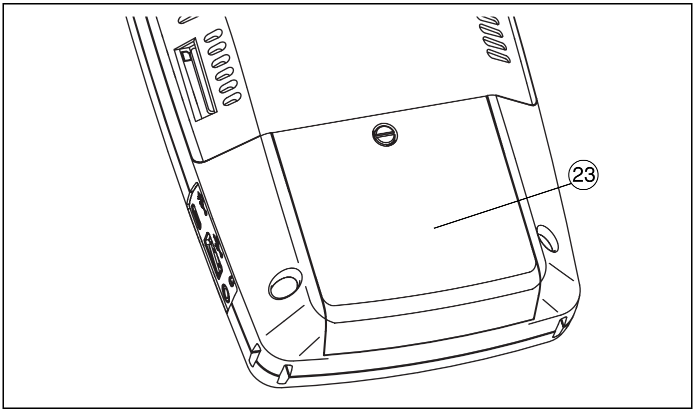


Figure 9. Battery Compartment

㉓ Battery Compartment - The battery pack can be replaced. See “Remove and Install the Battery” on page 321.

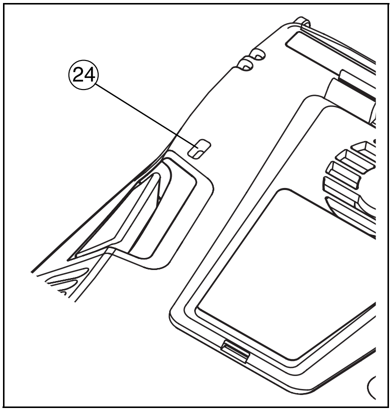


Figure 10. Kensington Security Slot

㉔ 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.

㉕ The stand can be removed as shown on page 244.

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.

The HOME Screen

Press the HOME key to display the Home screen.

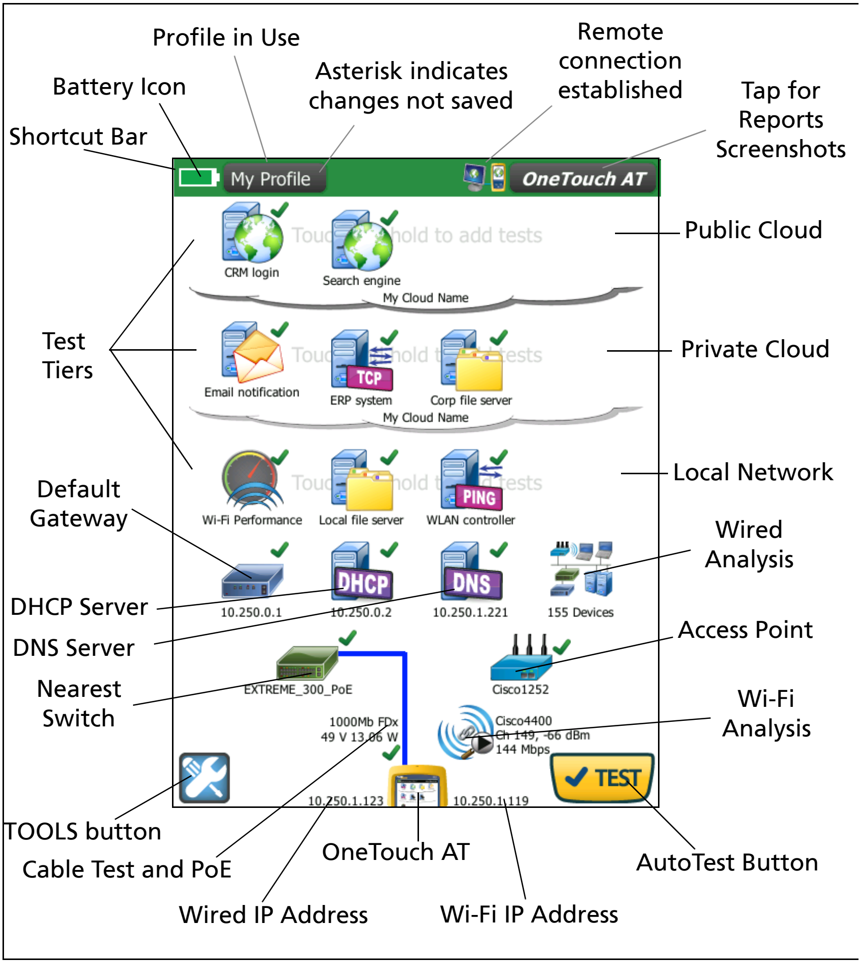
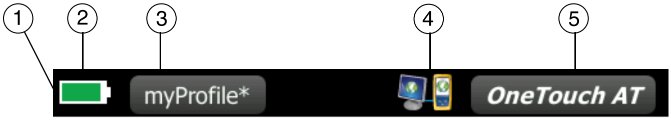


Figure 11. The OneTouch AT Home Screen

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.

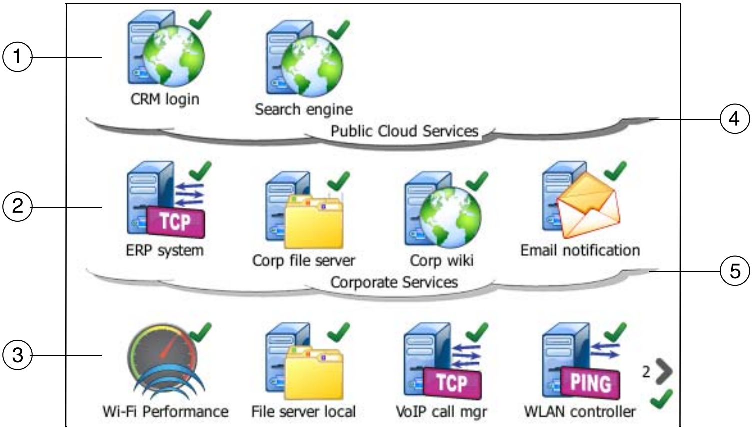
To see more information about the battery status, tap the Tools icon 🔧, then scroll down and tap the Battery Status button. See also: "AC Adapter and Battery" on page 19.

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. For more information see "Profiles" on page 165.

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

⑤ **OneTouch AT Button:** Tap the OneTouch AT 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 272, "Reports" on page 270, and "AutoTest Capture" on page 301.

Test Tiers



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

① **Public Cloud Tier:** This tier is generally used for tests of servers that are in the public cloud (the internet).

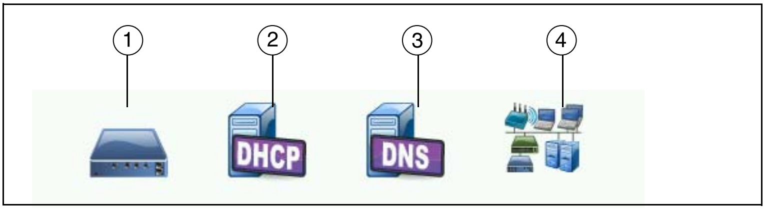
② **Private Cloud Tier:** This tier is generally used for tests of servers that are in the private cloud (the corporate intranet).

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

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

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

Network Services Tier



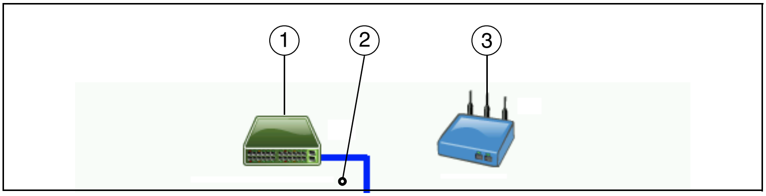
① **Default Gateway:** This shows the default gateway for the wired and/or Wi-Fi connection. Tap the icon for details of this router. If a problem is detected, a red X appears on the icon. See page 95.

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 99.

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 102.

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 104.

Network Access Tier

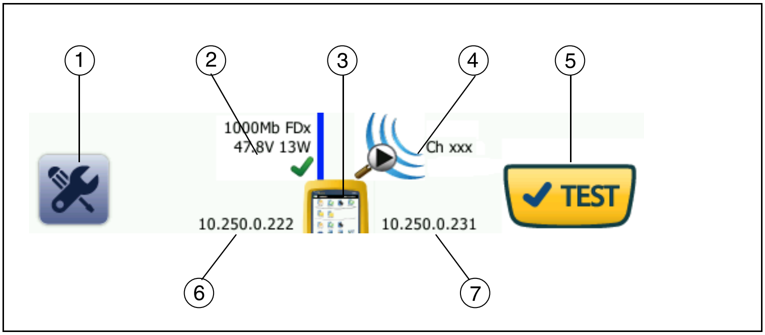


① **Nearest Switch:** Tap the icon to show details of the nearest switch. If a problem is detected, a red X appears on the icon. See page 86.

② **Cable:** Tap the link icon to view cable and PoE statistics. See "Cable Test" on page 71 and "PoE Test" on page 79 for more information.

③ **Wi-Fi Access Point:** Tap the icon for AP test results and connection log. For more information see “Wi-Fi Network Connect Test” on page 89.

Instrument Tier



① **TOOLS button:** Tap this button to enter the TOOLS menu. See Chapter 8: "Tools," beginning on page 247.

② **Cable:** Tap the icon to view cable, link, and PoE test results. See “Cable Test” on page 71 and “PoE Test” on page 79 for more information.

③ **OneTouch Icon:** Tap the icon to view a detailed list of wired and Wi-Fi transmit and receive statistics, along with address information. Note that the analyzer’s wired and Wi-Fi IP addresses are shown to the left and right of the icon. See page 66.

④ **Wi-Fi Analysis:** Tap the icon to open the Wi-Fi Analysis screen. See Chapter 7: "Wi-Fi Analysis," beginning on page 197.

⑤ **AutoTest Button:** Tap the button to run all configured tests. The analyzer does not link (on the wired or Wi-Fi ports) and does not perform any infrastructure tests or user tests until you tap the AutoTest button (or press the AutoTest key ✓TEST).

⑥ **Wired IP Address:** This is the IP address of the Ethernet NUT (Network Under Test) port.

⑦ **Wi-Fi IP Address:** This is the IP address of the Wi-Fi adapter.

Entering Text

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

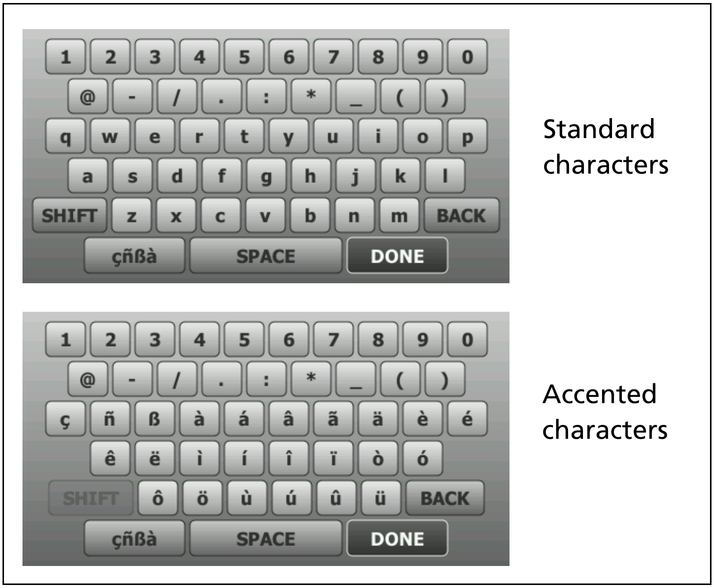
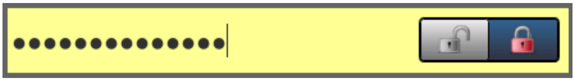


Figure 12. Keyboards for Text Entry

Entering Passwords and Other Hidden Text

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



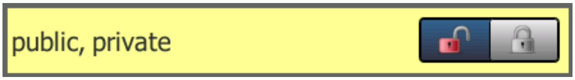
••••••••••••••

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



public, private

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.

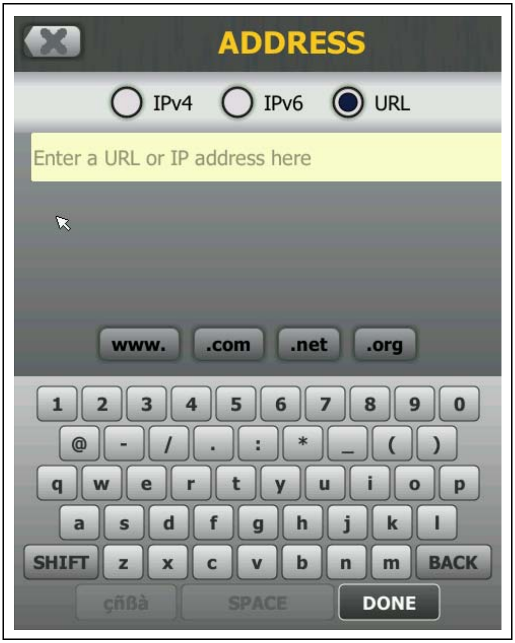


Figure 13. Keyboard for URL Entry

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.

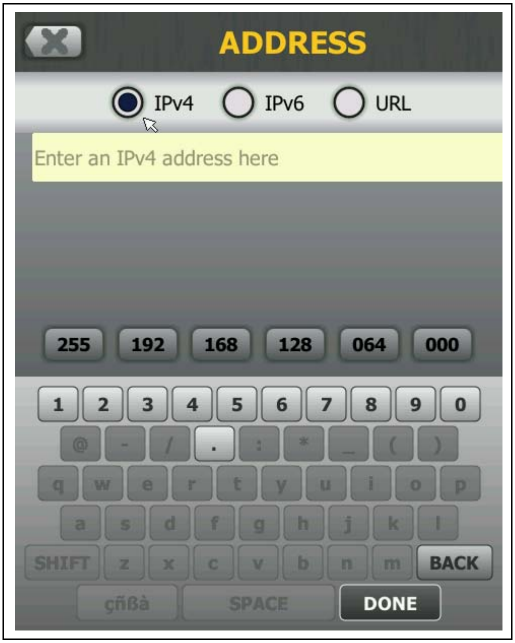


Figure 14. Keyboard for IPv4 Address Entry

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

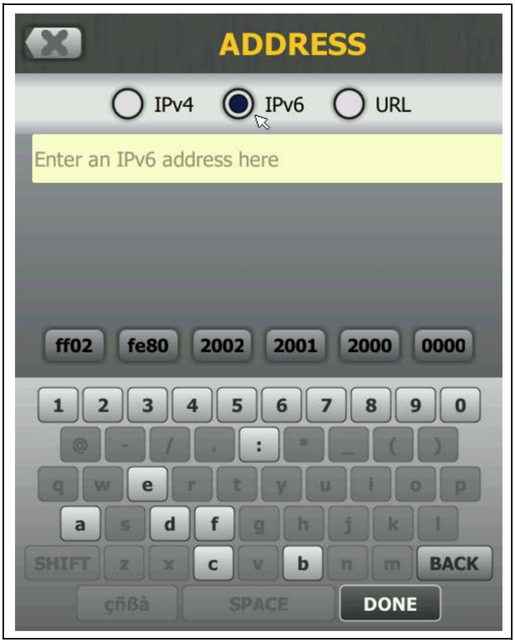


Figure 15. Keyboard for IPv6 Address Entry

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 19.

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 42.
- 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**.

Power Line Frequency

Set the power line frequency to the power frequency in the area where you will use the analyzer. This setting helps prevent external ac noise from affecting wiremap and resistance measurements.

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

2 Scroll down to the Maintenance Tools section, and tap **Power Line Frequency.**

3 Tap **50 Hz** or **60 Hz**, according to your ac power frequency.

Chapter 2: Got Started

⚠ 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.

Objectives

Follow the steps in this chapter to:

- Add a Connect (TCP) user test to the HOME screen
- Connect the OneTouch analyzer to a network
- Run AutoTest
- View the results

Add a User Test

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 182.

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.

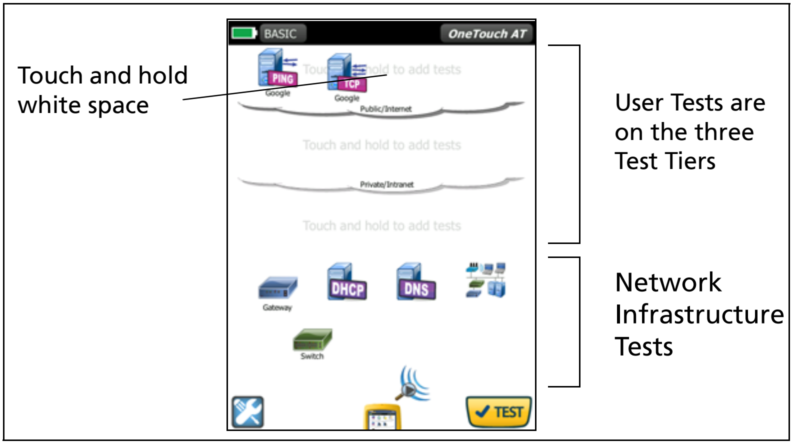
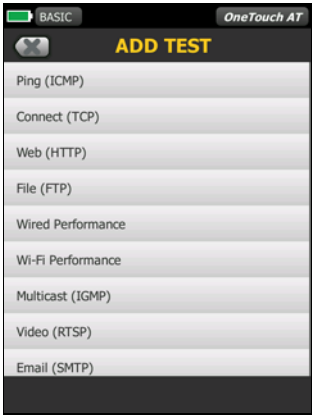

Touch and hold white space
BASIC
OneTouch AT
PING
Google
TCP
Google
Touch and hold to add tests
Public/Internet
Touch and hold to add tests
Private/Intranet
Touch and hold to add tests
Gateway
DHCP
DNS
Switch
TEST
User Tests are on the three Test Tiers
Network Infrastructure Tests

Figure 16. The Home Screen

The ADD TEST screen is displayed.



BASIC

OneTouch AT

ADD TEST

Ping (ICMP)

Connect (TCP)

Web (HTTP)

File (FTP)

Wired Performance

Wi-Fi Performance

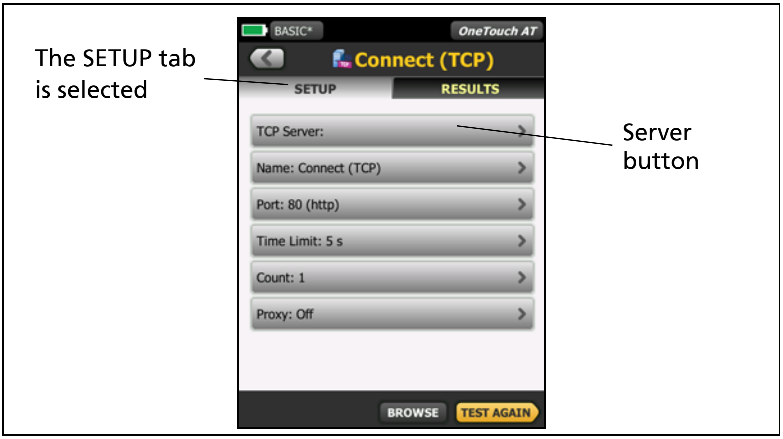
Multicast (IGMP)

Video (RTSP)

Email (SMTP)

Figure 17. ADD TEST Screen

2 Tap **Connect (TCP)**. The test's screen opens with the SETUP tab selected. Note that the active tab's color matches the screen's background.



The SETUP tab is selected

Server button

BASIC*

OneTouch AT

Connect (TCP)

SETUP

RESULTS

TCP Server:

Name: Connect (TCP)

Port: 80 (http)

Time Limit: 5 s

Count: 1

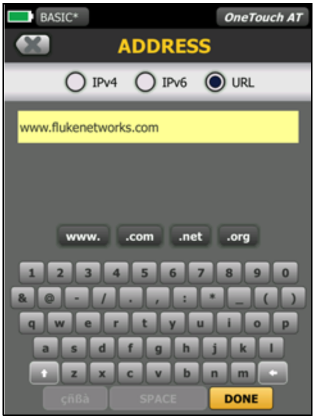
Proxy: Off

BROWSE

TEST AGAIN

Figure 18. Connect (TCP) Test Setup Screen

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



○ IPv4 ○ IPv6 ● URL

www.flukenetworks.com

Figure 19. 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 **flukenetworks** 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 5: "Profiles," beginning on page 165.

Connect to a Network

You can connect the OneTouch analyzer to a network via network Port A, or via the optional built-in Wi-Fi adapter. To purchase options, contact Fluke Networks. See page 17 for contact information.

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

Network Port B is used for VoIP analysis and the optional packet capture feature.

Establish a Wired (Copper) Connection

Connect an appropriate cable from the OneTouch analyzer's network Port A 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 248.

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 SFP Port A. To remove, gently pull the SFP's bail. If the SFP has retention tabs, press and hold the tabs on the sides of the adapter and pull it from the fiber port.

The OneTouch analyzer supports 100BASE-FX and 1000BASE-X SFP adapters.

Establish a Wi-Fi Connection

This section applies to OneTouch analyzers with the optional Wi-Fi feature.

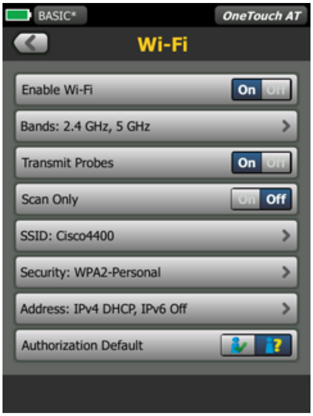
By default, the OneTouch analyzer operates in scan-only mode. It will not connect to a network unless it is configured to do so.

To connect to a Wi-Fi network:

1 Press the ⌂HOME key on the front panel.

2 Tap the **TOOLS** icon 🛠.

3 Tap the **Wi-Fi** button.



Enable Wi-Fi On Off
Bands: 2.4 GHz, 5 GHz
Transmit Probes On Off
Scan Only On Off
SSID: Cisco4400
Security: WPA2-Personal
Address: IPv4 DHCP, IPv6 Off
Authorization Default

Figure 20. Wi-Fi Test Settings Screen

4 Ensure that **Enable Wi-Fi** is **On**.

5 Using the **Band** button, select operation in the 2.4 GHz band, the 5 GHz band, or both.

6 The **Transmit Probes** setting is on by default. If you want the analyzer to be silent on Wi-Fi, set **Transmit Probes** to off. For details, see “Wi-Fi Analysis” on page 201.

7 Set **Scan Only** to **Off**. When Scan Only is set to **On**, the OneTouch analyzer will perform Wi-Fi analysis (as described on page 197), but it will not connect to a Wi-Fi network.

8 Tap the **SSID** button and select an SSID from the list. Or, if you want to connect to a network that is hidden (not broadcasting its SSID), tap the **ADD SSID** button.

9 Tap the back button <.

10 Tap the **Security** button and enter the credentials that are appropriate for your network.

11 Tap the **Address** button if you want to enter a static IP address, enable IPv6, or change the analyzer's MAC. These options are described on page 249. The options are the same for the analyzer's Wi-Fi and wired test ports.

12 You do not need to tap the **Authorization Default** button at this time. This feature is described in "Authorization Status Tool and Default Setting" on page 235.

13 Press the ⌂HOME key on the front panel.

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 ✓TEST (located at the lower-right corner of the HOME screen) or press the AutoTest key ✓TEST (located on the front panel). The OneTouch analyzer will:

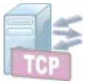
- Link on active ports (wired and/or Wi-Fi ports)
- Obtain IP addresses
- Run Network Infrastructure Tests (listed on page 71)
- Run User Tests (including the Connect (TCP) user test that you just created)
- When multiple user tests are present, they are run consecutively, starting with the lower-left 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 301.

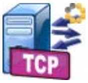
Icons Indicate Test Status

When AutoTest begins, the AutoTest button ✓TEST 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 ✓TEST.

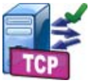
As AutoTest runs, each user test icon changes to indicate its status.



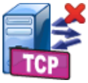
The test has not started. The icon is faded.



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 ✗.

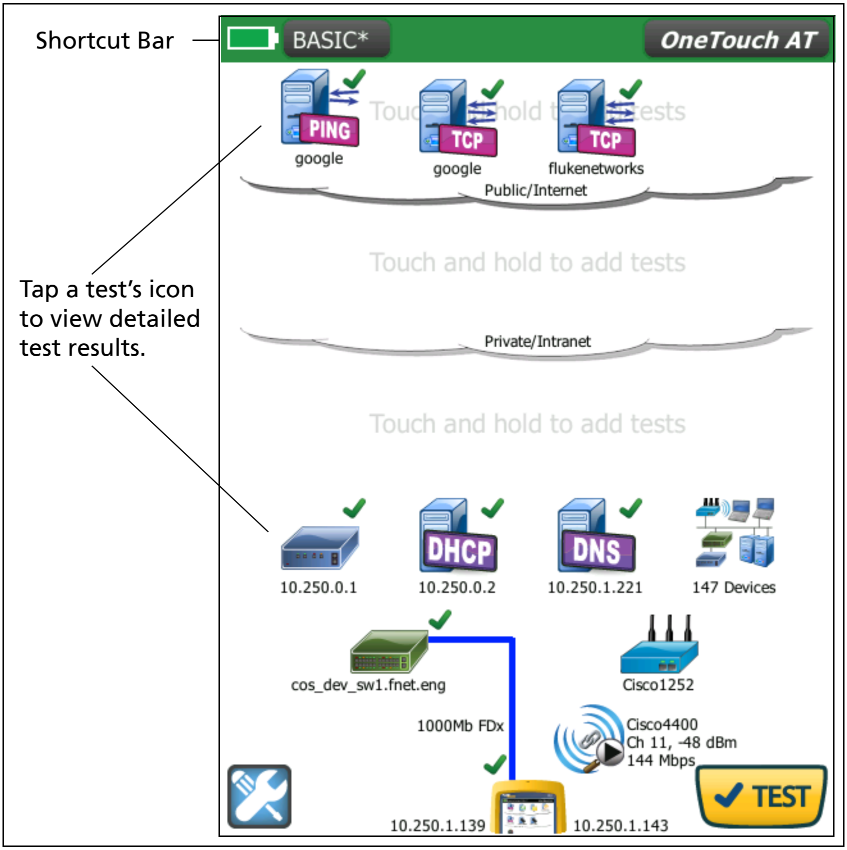
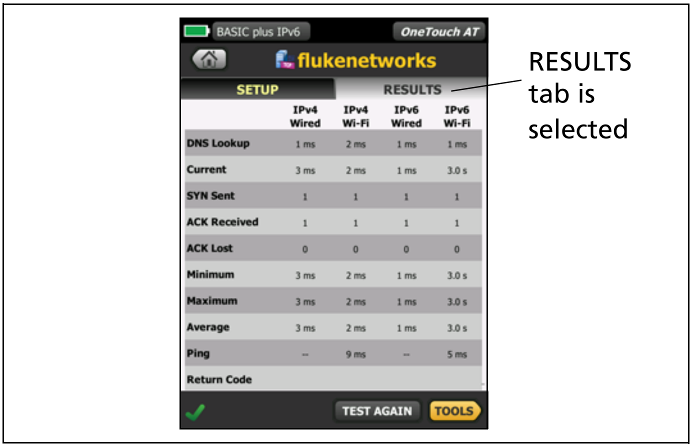


Figure 21. HOME Screen After Running AutoTest

View Detailed Test Results

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



	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	1 ms	2 ms	1 ms	1 ms
Current	3 ms	2 ms	1 ms	3.0 s
SYN Sent	1	1	1	1
ACK Received	1	1	1	1
ACK Lost	0	0	0	0
Minimum	3 ms	2 ms	1 ms	3.0 s
Maximum	3 ms	2 ms	1 ms	3.0 s
Average	3 ms	2 ms	1 ms	3.0 s
Ping	--	9 ms	--	5 ms
Return Code				

RESULTS tab is selected

Figure 22. Connect (TCP) Test Results Tab

Note

Results are shown with IPv6 enabled. To enable IPv6 testing see "Wired" on page 248.

- A red X ✗ indicates a failure.
- A pair of dashes -- indicate that results for a test were not received.

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 OneTouch analyzer.

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

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 servers' IP and MAC addresses are displayed. If you specified a target server's URL, the IP 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 TOOLS button TOOLS run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server. Tap the **TEST AGAIN** button TEST AGAIN to re-run the test.

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 46.

You can also add user tests from a Wired Analysis screen as described in "Wired Analysis Tools" on page 182.

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

• **Ping (ICMP) Test**	**(page 106)**
• **Connect (TCP) Test**	**(page 111)**
• **Web (HTTP) Test**	**(page 116)**
• **File (FTP) Test**	**(page 121)**
• **Wired Performance Test**	**(page 126)**
• **Wi-Fi Performance Test**	**(page 139)**
• **Multicast (IGMP) Test**	**(page 152)**
• **Video (RTSP) Test**	**(page 155)**
• **Email (SMTP) Test**	**(page 159)**

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/

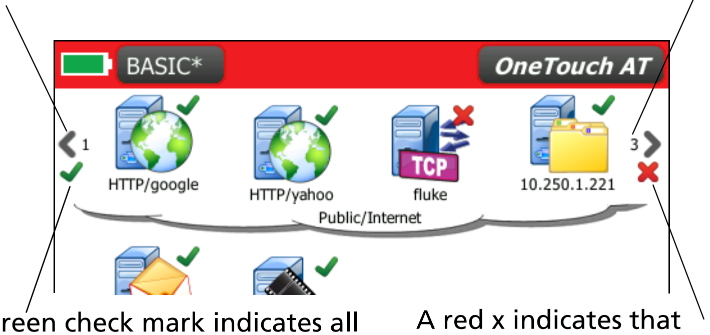
Intranet. Tap a cloud to open the cloud's SETUP and RESULTS screen. The SETUP tab lets you rename the cloud. The RESULTS tab provides a summary of the number of tests on the tier above and the number of tests that failed when AutoTest was run.

See Off-Screen Tests

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

Tap the chevron to scroll to the tests that are currently off-screen.

The number of off-screen tests is shown.



A green check mark indicates all off-screen tests passed.

A red x indicates that one or more off-screen tests failed.

Figure 23. 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

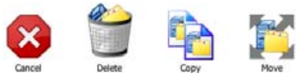
To edit a test, tap its icon. Tap the test's SETUP tab to edit the test parameters.

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 5: "Profiles," beginning on page 165.

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 analyzer.

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

- Network Infrastructure Tests are described on page 65.
- User Tests are described on page 105.

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 OneTouch analyzer retains its wired and Wi-Fi connections (link and IP address), and wired analysis begins.

If "Enable Wi-Fi" is set to "Off," the OneTouch analyzer will not connect to an AP, and when AutoTest completes Wi-Fi analysis (scanning) will begin.

When you run AutoTest again, the following actions occur.

- The wired and Wi-Fi links are dropped.
- Infrastructure test results, user test results, and wired discovery results are cleared.
- The wired link is re-established.
- If the OneTouch analyzer is configured to connect to a Wi-Fi network, the Wi-Fi link is re-established.
- Wired and Wi-Fi 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 183

"Browse to a Test Target from the HOME Screen" on page 263

"Telnet/SSH" on page 263

Configure the OneTouch Analyzer to Use SNMP

Add SNMP Community Strings/Credentials to allow display of SNMP-enabled switch and gateway statistics, and enable crosslinking between wired and Wi-Fi device details via the Discovery Button. See “SNMP” on page 174. See also: page 177 and page 216 for an explanation of the Discovery Button.

Store Your Test Setup in a Profile

You can save OneTouch analyzer test configurations in Profiles. See “Profiles” on page 165.

See Wi-Fi Analysis

To see Wi-Fi analysis, tap the Wi-Fi analysis icon. See Chapter 7, "Wi-Fi Analysis."

See IPv6 Results

To see IPv6 test results, enable IPv6 operation and run AutoTest again. See “Address” on page 249.

Generate a Report

See “Reports” on page 270.

Set Up Remote Control of the Analyzer

See “Remote User Interface and File Access” on page 308.

Chapter 3: 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 105.

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

- **OneTouch Instrument, page 66**
- **Cable Test, page 71**
- **Link Test, page 77**
- **PoE Test, page 79**
- **Wi-Fi Analysis, page 85**
- **Nearest Switch Test, page 86**
- **Wi-Fi Network Connect Test, page 89**
- **Gateway Test, page 95**
- **DHCP Server Test, page 99**
- **DNS Server Test, page 102**
- **Wired Analysis, page 104**

OneTouch Instrument

Description

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

Configuration

Connect the OneTouch analyzer to a wired network, a Wi-Fi network, or both (see “Connect to a Network” on page 50) and tap the AutoTest button ✓TEST.

How it Works

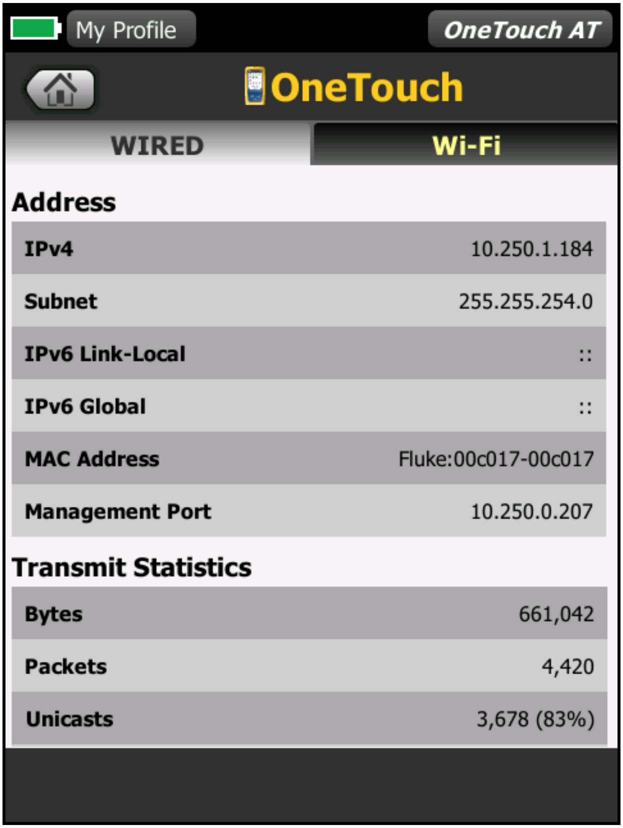
The OneTouch analyzer collects and displays connection parameters such as IP addresses, and monitors and reports on transmitted and received frames. Received frames with errors are categorized based on the type of error, and error counts are shown. If an SFP is installed, its manufacturer, model, type,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

Results

On the HOME screen, the wired IP address is shown to the left of the OneTouch instrument icon 10.250.1.152 10.250.0.152 and the Wi-Fi IP address is shown on the right.

Tap the OneTouch instrument icon to view test results and statistics gathered from the wired and Wi-Fi connections. The ONETOUCH results screen has two tabs: one for the wired connection and another for the Wi-Fi connection.

WIRED Results Tab



Address

IPv4	10.250.1.184
Subnet	255.255.254.0
IPv6 Link-Local	::
IPv6 Global	::
MAC Address	Fluke:00c017-00c017
Management Port	10.250.0.207

Transmit Statistics

Bytes	661,042
Packets	4,420
Unicasts	3,678 (83%)

Figure 24. Wired OneTouch 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, total packets, unicast packets, multicast packets, and broadcast packets transmitted by the OneTouch analyzer are shown.

Receive Statistics - The following information is displayed:

Bytes - The total number of bytes received

Packets - The total number of packets received

Unicasts - The total number of unicast packets received

Multicasts - The total number of multicast packets received

Broadcasts - The total number of broadcast packets received

The warning icon ⚠ appears next to the instrument icon if any of the following errors are seen.

FCS Errors - This counter increments for each frame received that has an integral length (8-bit multiple) of 64-1518 bytes and contains a frame check sequence error.

Undersize Frames - This counter increments each time a frame is received that is less than 64 bytes in length, contains a valid FCS, and was otherwise well formed. This count does not include range or length errors.

Undersize frames may be caused by a faulty or corrupt LAN driver.

Oversize Frames - This counter increments each time a frame is received that exceeds 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN), contains a valid FCS, and was otherwise well formed.

In general you should not see oversize frames, though their presence is not a guarantee that the network is failing. Oversize frames may be caused by a faulty or corrupt LAN driver.

Fragments - This counter increments for each frame received that contains an invalid FCS and is less than 64 bytes in length. This includes integral and non-integral lengths.

Jabbers - This counter increments for each frame that exceeds 1518 bytes in length (non-VLAN) or 1522 bytes (on a VLAN) and contains an invalid FCS. This includes alignment errors.

Possible causes include a bad NIC or transceiver, faulty or corrupt NIC driver, bad cabling, grounding problems, and nodes jamming the network due to above normal collision rates.

A possible solution would be to identify the node(s) that are sending out excessive errors and replace the defective hardware.

Dropped Frames - This counter increments for each frame that is received but is later dropped due to a lack of system resources.

Control Frames - This counter increments for each MAC control frame received (PAUSE and unsupported) from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, with a valid CRC.

PAUSE Frames - This counter increments each time a PAUSE MAC control frame is received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, with a valid CRC.

Unknown OP codes - This counter increments each time a MAC control frame is received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, and contains an opcode other than PAUSE, but the frame has a valid CRC.

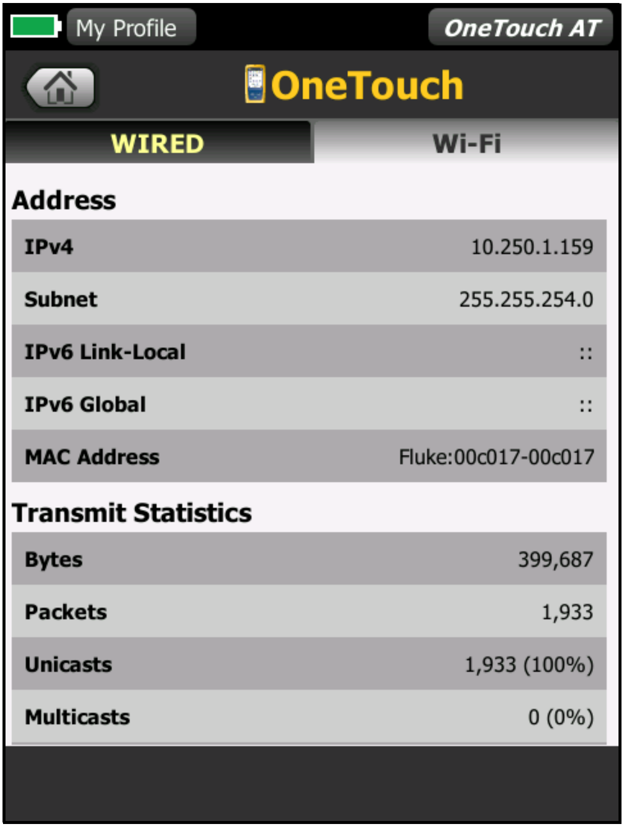
Alignment Errors - This counter increments for each frame received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, contains an invalid FCS, and is not an integral number of bytes.

Alignment errors may manifest as an inability to connect to the network or as intermittent connectivity.

Frame Length Errors - This counter increments for each frame received in which the 802.3 length field did not match the number of data bytes actually received (46-1500 bytes). The counter does not increment if the length field is not a valid 802.3 length, such as an Ethertype value.

Code Errors - This counter increments each time a valid carrier is present and at least one invalid data symbol is detected.

Carrier Sense Errors - This counter shows the number of times that the carrier sense condition was lost or was not asserted when attempting to transmit frames. The count increments at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.



Address

IPv4	10.250.1.159
Subnet	255.255.254.0
IPv6 Link-Local	::
IPv6 Global	::
MAC Address	Fluke:00c017-00c017

Transmit Statistics

Bytes	399,687
Packets	1,933
Unicasts	1,933 (100%)
Multicasts	0 (0%)

Figure 25. Wi-Fi OneTouch Results

Figure 25 shows OneTouch instrument results on the Wi-Fi tab. Details of the analyzer's address are shown along with transmit and receive statistics.

Cable Test

10.5ft ✓

Description

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

When you tap the AutoTest button ✓ TEST, the OneTouch analyzer attempts to establish link. If the OneTouch analyzer cannot establish link, it performs cable test instead.

Copper Cable Test

Configuration and Capabilities

Connect an Ethernet cable to network Port A. The other end of the cable can be:

- Connected to a Fluke WireView™ WireMapper

  This provides the most robust cable test. The OneTouch analyzer:

  - Determines length
  - Finds shorts and opens
  - Tests shield continuity
  - Finds splits (impedance mismatch, cross-pair short, mis-wrapping (conductor wrapped to wrong pair))
  - Identifies a crossover cable

- Unterminated (not connected to anything)

  The OneTouch:

  - Determines length
  - Finds shorts
  - Finds opens if they are more than 2 m from the far end

  - Finds splits

- Connected to the OneTouch analyzer's network Port B

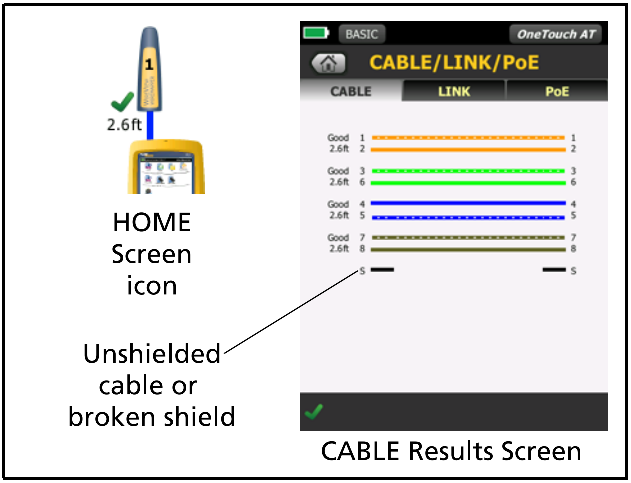
  The OneTouch analyzer:

  - Finds shorts and opens
  - Finds splits
  - Identifies crossover cables
  - Attempts to link at 1 Gbps. If it can't link at 1 Gbps it attempts to link at 100 Mbps, then at 10 Mbps. Results are reported on the CABLE Results screen.
  - Identifies normal or negative pair-wise polarity (e.g. pins 1,2 connected to pins 2,1.)

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.



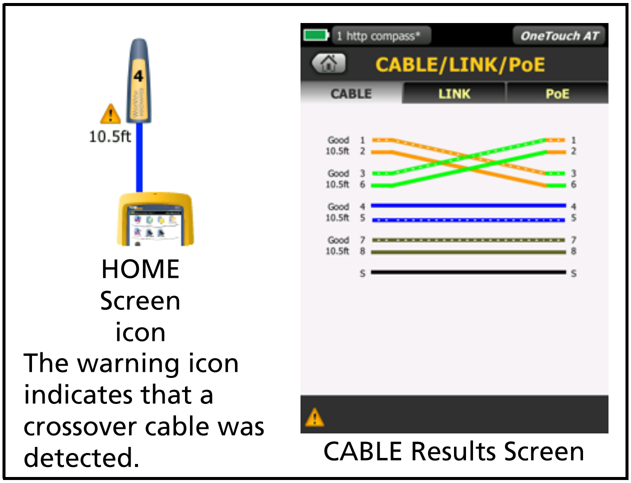
HOME Screen icon

Unshielded cable or broken shield

CABLE Results Screen

Figure 26. Cable Connected to WireMapper #1

This shows a cable connected to Fluke WireView WireMapper #1. The broken “S” wire indicates an unshielded cable or a cable that has a broken shield. The shield’s status does not affect the test’s pass/fail result.



HOME Screen icon

The warning icon indicates that a crossover cable was detected.

CABLE Results Screen

Figure 27. Shielded Crossover Cable Connected to WireMapper #4

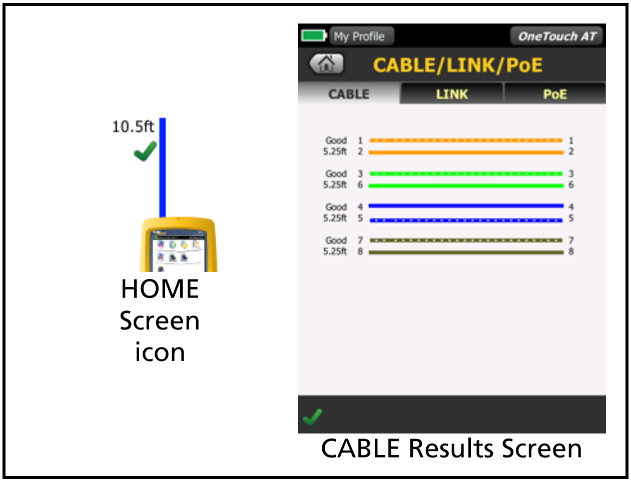
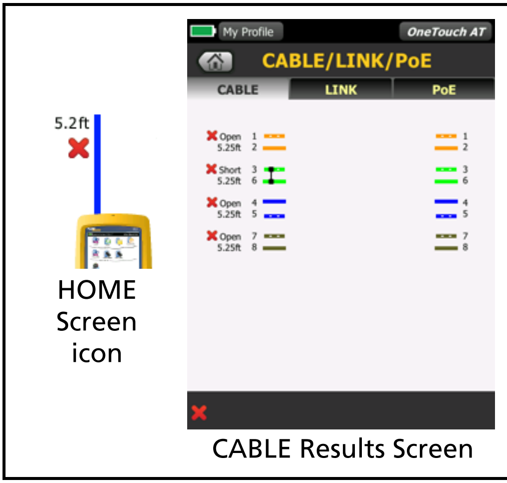


Figure 28. Unterminated Cable Connected to Port A



The results screen shows which wires are open or shorted and the distance from the OneTouch analyzer to the cable fault.

Figure 29. Unterminated Cable with Shorts and Opens

This shows an unterminated cable with shorts and opens connected to Port A.

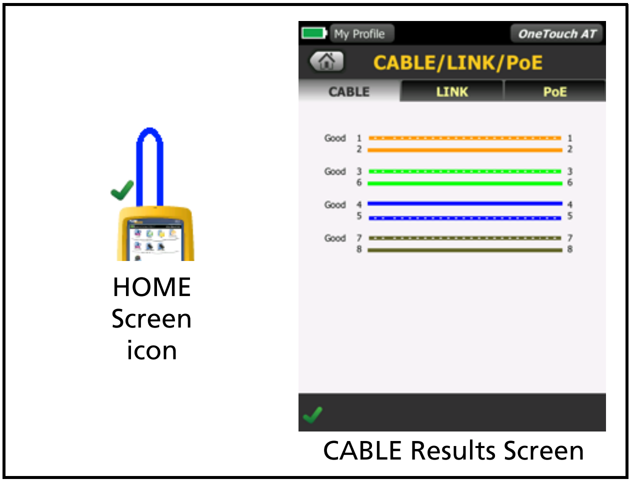
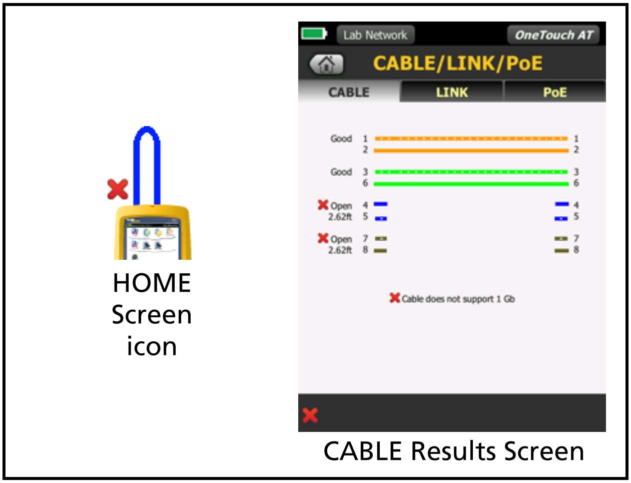


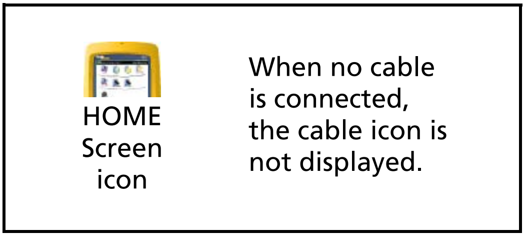
Figure 30. Cable Connected from Port A to Port B



Cable does not support 1 Gb

Figure 31. Cable With Only Two Pairs of Conductors

This shows a cable with only two pairs of conductors connected from Port A to Port B.



When no cable is connected, the cable icon is not displayed.

Figure 32. No Cable Connected

Fiber Cable Diagnostics

The OneTouch analyzer works with fiber cables when connected via a 100BASE-FX or 1000BASE-X SFP adapter. The fiber cable is shown in orange on the HOME screen.

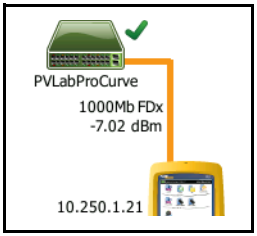


Figure 33. Fiber Cable Shown on HOME Screen

When a DDM (Digital Diagnostics Monitoring) capable SFP is installed in the OneTouch 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 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/PoE 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.

Rx Pair is the wire pair on which link negotiation was offered by the port.

Level indicates whether the voltage level of the link negotiation signal was normal or low. Communication might not be reliable if the level is low. If the link level is low, the warning icon ⚠ appears next to the cable icon on the HOME screen.

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

PoE Test

Description

Power over Ethernet (PoE) is a system for supplying electrical power, along with data, over Ethernet cabling. When connected to PoE Power Sourcing Equipment (PSE), the OneTouch analyzer can emulate a Powered Device (PD). The OneTouch analyzer negotiates and reports the advertised class, unloaded and loaded voltage, loaded power, and the pairs used to deliver power.

Configuration

To configure the PoE test:

1. Connect Port A of the OneTouch AT analyzer to the network.
2. Ensure that a PoE device is *not* connected to Port B.
3. On the HOME screen, tap **TOOLS**.
4. Tap the **Wired** button.
5. Tap the **Power over Ethernet** button.

- **Enable PoE** - This button is used to enable or disable PoE measurements.
- **Enable TruePower™** - This button enables or disables the loaded voltage and power measurements.
- **Class**: The OneTouch analyzer will attempt to negotiate to the selected class.
  - When you select class 4 an option is available for enabling LLDP Negotiation. Most PSE requires LLDP negotiation for class 4.

How it Works

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

The OneTouch analyzer requests the selected class (0-4) from the PSE. Negotiation is performed for the selected class. A PSE's power output can be measured up to the limit specified by the negotiated class using the OneTouch analyzer's TruePower feature.

Results

If the voltage is below the PSE type's minimum, or the delivered power is below the class's specified maximum deliverable power, the test will fail. If the port meets the class's voltage and power requirements, the test will pass.

When you set TruePower to **On**, the loaded voltage and available power (up to the class's maximum) will be displayed. If TruePower is off, only the unloaded voltage is displayed.

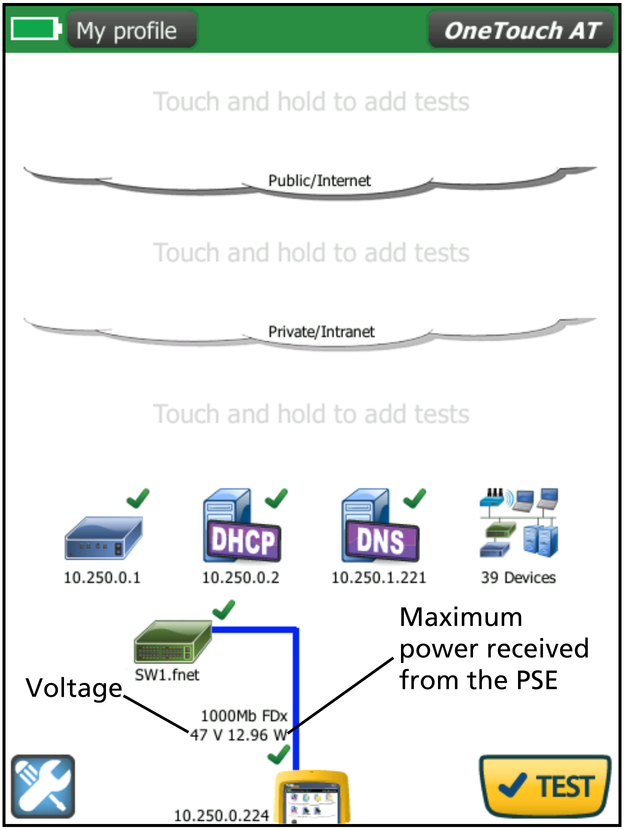
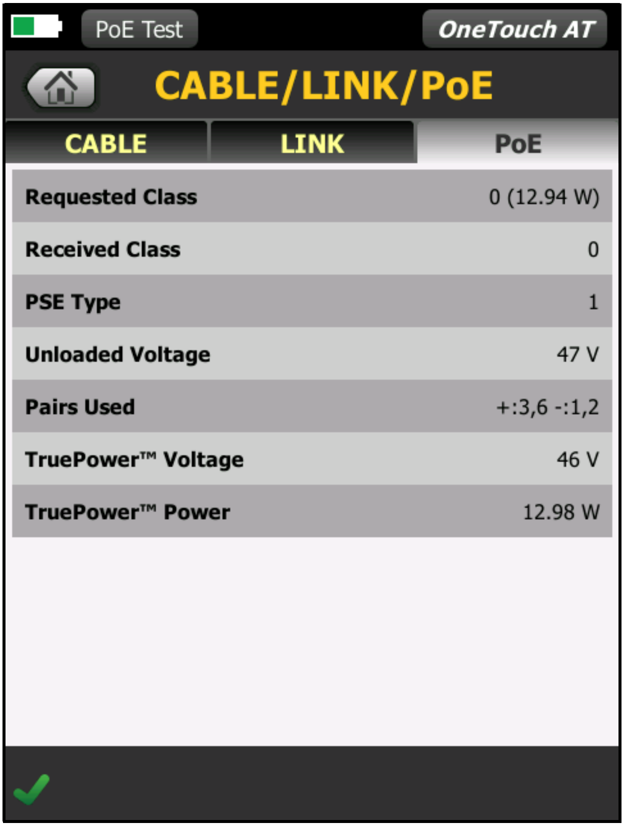


Figure 34. HOME Screen - PoE Test Passed

Figure 34 shows the HOME screen after testing to Class 3 on a switch port capable of supplying the specified power.

Tap the PoE test results on the HOME screen, then tap the PoE tab to show detailed results.



Requested Class	0 (12.94 W)
Received Class	0
PSE Type	1
Unloaded Voltage	47 V
Pairs Used	+:3,6 -:1,2
TruePower™ Voltage	46 V
TruePower™ Power	12.98 W

Figure 35. Detailed PoE Test Results - Test Passed

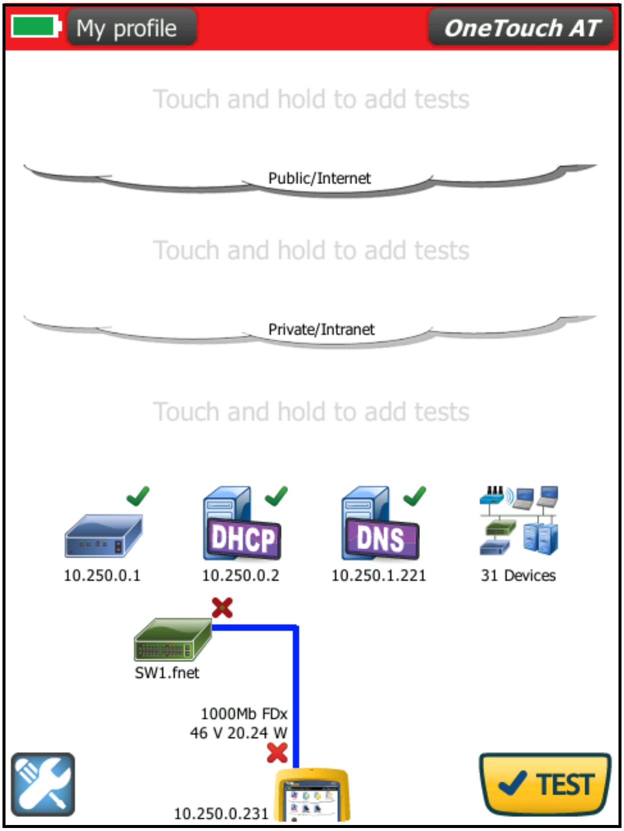
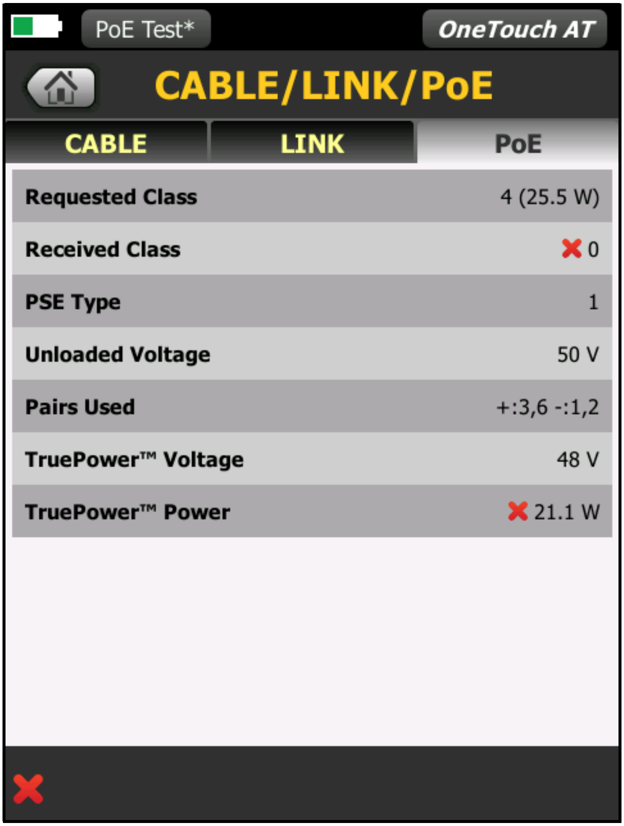


Figure 36. HOME Screen - PoE Test Failed

Figure 36 shows the HOME screen after setting the OneTouch analyzer to request Class 4 from a Type 1 switch port. A Type 1 switch cannot supply the power specified by Class 4.

Figure 37 shows the CABLE/LINK/PoE results screen after setting the OneTouch analyzer to request Class 4 from a Type 1 switch port. A Type 1 switch cannot supply the power specified by Class 4.



Requested Class	4 (25.5 W)
Received Class	✗ 0
PSE Type	1
Unloaded Voltage	50 V
Pairs Used	+:3,6 -:1,2
TruePower™ Voltage	48 V
TruePower™ Power	✗ 21.1 W

✗

Figure 37. Detailed PoE Test Results - Test Failed

Wi-Fi Analysis

Tap the Wi-Fi Analysis icon to analyze 802.11 networks, access points, clients, and channels. The analyzer can be used for troubleshooting client connectivity and locating devices.

See Chapter 7: "Wi-Fi Analysis," beginning on page 197 for details.

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 OneTouch analyzer for SNMP. See “SNMP” on page 174.

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 OneTouch analyzer uses SNMP to acquire system group information and packet statistics for the port where the OneTouch analyzer is connected.

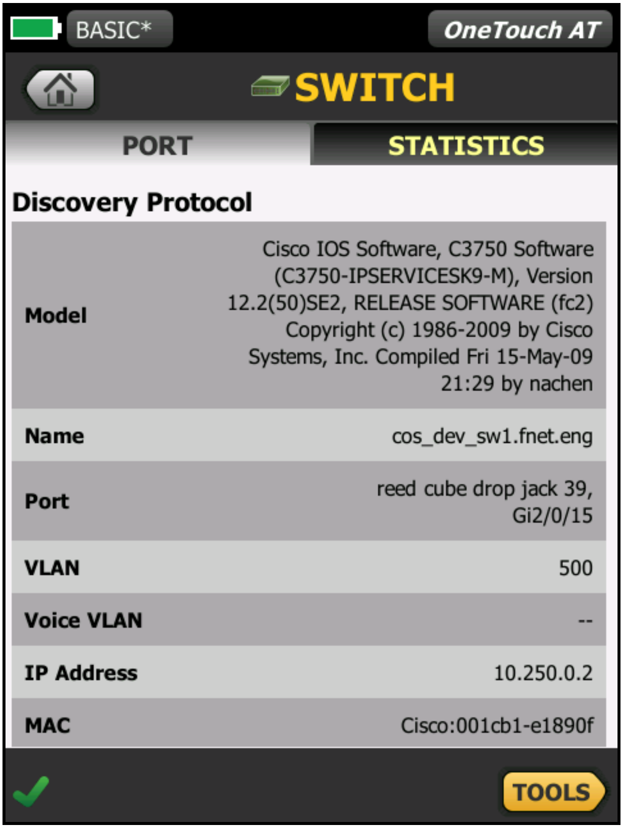
Results

> 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 OneTouch 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.

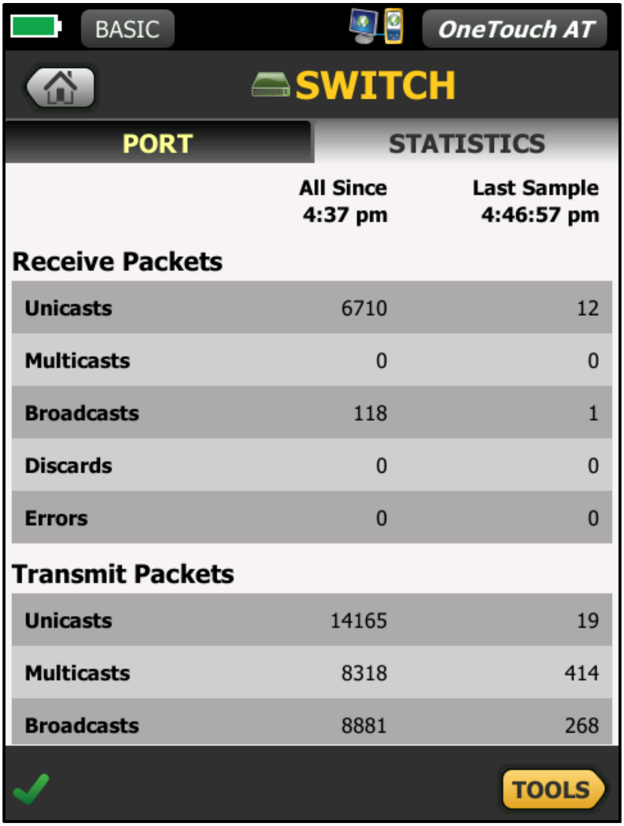
Run AutoTest, then tap the Nearest Switch icon to show the results. There are two tabs: PORT and STATISTICS.



Discovery Protocol

Model	Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(50)SE2, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Fri 15-May-09 21:29 by nachen
Name	cos_dev_sw1.fnet.eng
Port	reed cube drop jack 39, Gi2/0/15
VLAN	500
Voice VLAN	--
IP Address	10.250.0.2
MAC	Cisco:001cb1-e1890f

Figure 38. Nearest Switch - PORT Tab



	All Since 4:37 pm	Last Sample 4:46:57 pm
Receive Packets		
Unicasts	6710	12
Multicasts	0	0
Broadcasts	118	1
Discards	0	0
Errors	0	0
Transmit Packets		
Unicasts	14165	19
Multicasts	8318	414
Broadcasts	8881	268

Figure 39. Nearest Switch - STATISTICS Tab

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.

Wi-Fi Network Connect Test

Description

The Wi-Fi Network Connect test performs link to the configured Wi-Fi network to test user connectivity and the general health of the local network environment. The test verifies the authentication and association process and as well the state of layer one and layer two Wi-Fi infrastructure. The target SSID and its security credentials must be included in the loaded profile. Wi-Fi linking targets the “best” access point and channel—generally the access point with the strongest signal level. The test passes if a successful connection is made.

The results include the following key health metrics.

Tx Rate is a performance metric indicating the speed of packets transmitted (Tx rate) as compared to the capability of the link.

Retries indicates the percentage of packets resent. A higher percentage is an indication of network congestion and interference.

Signal and Noise - The signal quality is a combination of signal strength of the connected AP and noise level in the connected channel; high quality is represented by strong signal and low noise levels.

Channel Utilization - the percentage of bandwidth usage on the connected channel. High utilization values may indicate network congestion and interference. The results include both 802.11 and non-802.11 utilization. These values are reported upon completion of AutoTest.

Channel APs - the number of access points that are configured to use the connected channel. Too many access points may interfere with each other and impact the connectivity or performance. Too few APs may impact a user's ability to stay connected or roam.

Configuration

1. On the HOME screen, tap **TOOLS** 🛠.
2. Tap the **Wi-Fi** button.
3. Ensure **Enable Wi-Fi** is **On**.
4. Ensure **Scan Only** is **Off**.
5. Tap the **SSID** button and select the network for the connection test.
6. Tap the **Security** button. Configure the authentication type and credentials.
7. Return to the HOME screen.
8. Tap the AutoTest button ✓TEST.

How it Works

When you run AutoTest, the OneTouch analyzer attempts to connect to the configured Wi-Fi network. The OneTouch analyzer logs the steps in the connection or connection attempt. This can be a valuable troubleshooting aid.

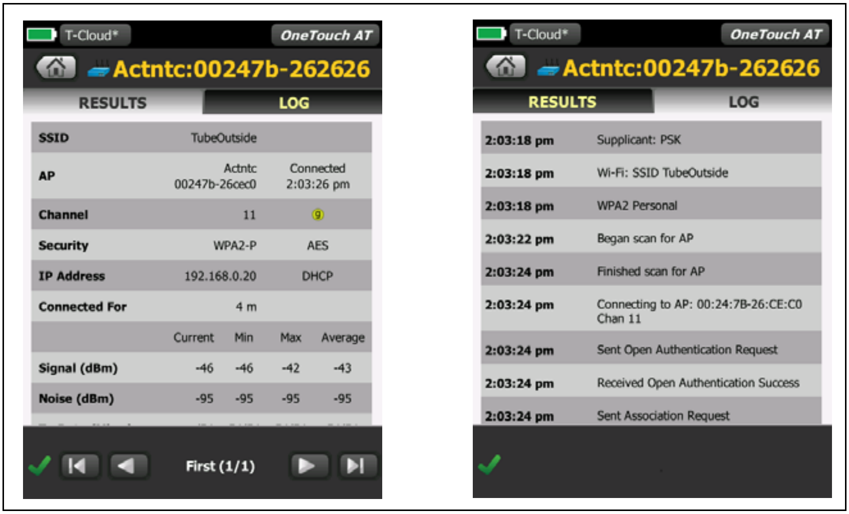
When AutoTest completes, the analyzer stays connected to the Wi-Fi network. You can roam from one AP to another.

The OneTouch analyzer collects and displays information about the currently connected AP, including the manufacturer, BSSID, channel number, etc. Transmit and receive statistics, utilization, and amount of time connected are updated continuously. Results are reported on the RESULTS tab.

Navigation controls at the bottom of the RESULTS screen let you see connection results of previously roamed APs.

Results

If the connection is made the test passes and a green check mark ✓ is shown next to the AP icon on the HOME screen. If the connection attempt fails a red x ✗ is shown next to the AP icon. The warning icon ⚠ is displayed if a warning condition occurred (see page 92) but the test otherwise passed. Tap the AP icon for detailed results.



SSID	TubeOutside			
AP	Actntc 00247b-26cec0	Connected 2:03:26 pm		
Channel	11	9		
Security	WPA2-P	AES		
IP Address	192.168.0.20	DHCP		
Connected For	4 m			
	Current	Min	Max	Average
Signal (dBm)	-46	-46	-42	-43
Noise (dBm)	-95	-95	-95	-95

```
2:03:18 pm    Supplicant: PSK
2:03:18 pm    Wi-Fi: SSID TubeOutside
2:03:18 pm    WPA2 Personal
2:03:22 pm    Began scan for AP
2:03:24 pm    Finished scan for AP
2:03:24 pm    Connecting to AP: 00:24:7B-26:CE:C0
              Chan 11
2:03:24 pm    Sent Open Authentication Request
2:03:24 pm    Received Open Authentication Success
2:03:24 pm    Sent Association Request
```

Figure 40. Wi-Fi Network Connect Test Results

RESULTS Tab

Measurements are shown in rows as follows:

SSID - The name of the network on which the Wi-Fi connection was established during AutoTest.

AP - This row shows the AP manufacturer, BSSID and the time when the OneTouch analyzer connected to the network. When you roam, this will indicate the time when the OneTouch analyzer connected to the current access point.

Channel - The channel number is shown, along with an icon representing the Wi-Fi media type (a, b, g, ac, n, n40+, n40-).

Security - This row shows the security parameters that are set in the profile. See "Establish a Wi-Fi Connection" on page 51.

IP Address - This row shows the Wi-Fi IP address and indicates whether addressing is via DHCP or static.

Connected For - This shows the elapsed connection time. If roamed, it shows the time since the last roam.

The following measurements include current, minimum, maximum, and average (arithmetic mean) values. If a value is not within normal limits, a warning icon ⚠ is shown next to the AP on the HOME screen and next to the value on the RESULTS tab.

Tx Rate - The transmission rate is shown in Mbps or Kbps, then a slash (/), then the maximum theoretical Tx rate. Minimum, maximum, and average (arithmetic mean) values are also shown. When the average rate is less than 30% of the maximum rate, a warning icon ⚠ is displayed.

Retries - A warning icon ⚠ is displayed when the average retry rate exceeds 40% of total packets.

Signal - Signal strength statistics are displayed. A warning icon ⚠ is displayed when the average or maximum signal strength is equal to or below -75 dBm.

Noise - Noise statistics are displayed. A warning icon ⚠ is displayed when the average or minimum noise level on the channel is equal to or above -80 dBm.

Channel Utilization - A warning icon ⚠ is displayed when 802.11 utilization is greater than 40% of the channel's bandwidth, or when non-802.11 utilization is greater than 20% of the channel's bandwidth.

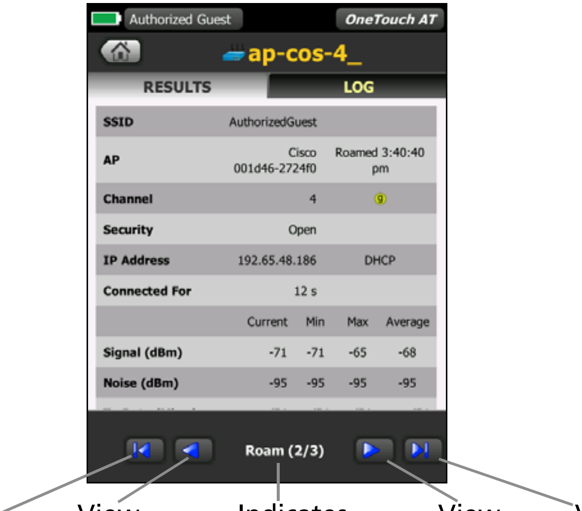
Channel APs - This shows the number of APs on the channel. A warning icon ⚠ is displayed when more than three APs overlap on the channel.

Roaming Results Navigation Controls

To roam with the OneTouch analyzer:

1. Configure the OneTouch analyzer to connect to a Wi-Fi network.
2. Run AutoTest.
3. Tap the AP icon on the HOME screen.
4. Walk from one AP coverage zone to another. The OneTouch analyzer records the details of each roam.

You can use the roaming results navigation controls to view the details of each associated AP.



SSID	AuthorizedGuest	
AP	Cisco 001d46-2724f0	Roamed 3:40:40 pm
Channel	4	9
Security	Open	
IP Address	192.65.48.186	DHCP
Connected For	12 s	

	Current	Min	Max	Average
Signal (dBm)	-71	-71	-65	-68
Noise (dBm)	-95	-95	-95	-95

View first AP's details

View previous AP's details

Indicates which roam's data you are viewing

View next AP's details

View last AP's details

Figure 41. Roaming Navigation Controls

See also: "Connect Tool" on page 239.

LOG Tab

The LOG tab shows the Wi-Fi connection log, including driver activity, supplicant, and DHCP process.

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 OneTouch analyzer for SNMP. See “SNMP” on page 174.

How it Works

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

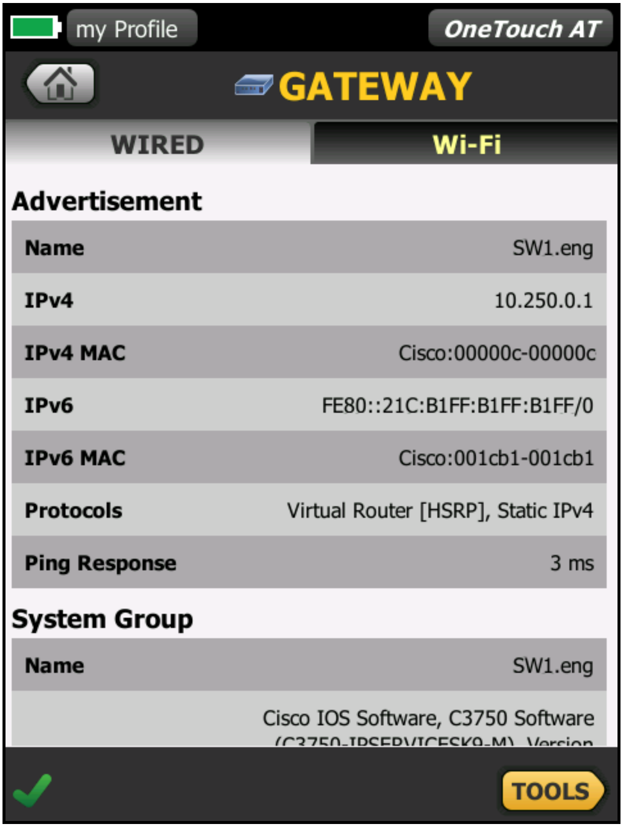
The OneTouch analyzer uses SNMP to acquire system group information and statistics for the port that services the analyzer’s subnet.

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 wired and Wi-Fi gateway information, including wired gateway statistics.



Advertisement

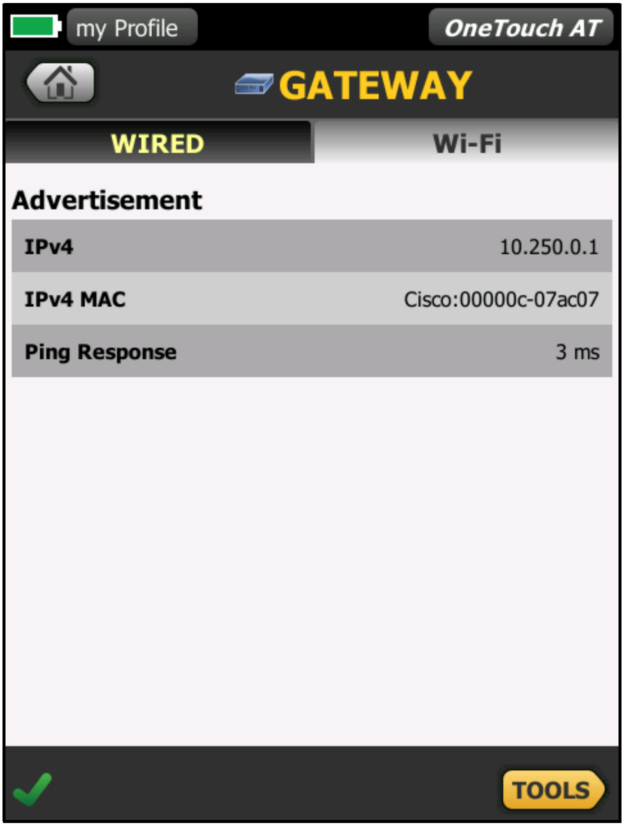
Name	SW1.eng
IPv4	10.250.0.1
IPv4 MAC	Cisco:00000c-00000c
IPv6	FE80::21C:B1FF:B1FF:B1FF/0
IPv6 MAC	Cisco:001cb1-001cb1
Protocols	Virtual Router [HSRP], Static IPv4
Ping Response	3 ms

System Group

Name	SW1.eng
	Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version

Figure 42. Gateway WIRED Tab

Wired gateway statistics are updated every 15 seconds.



Advertisement

IPv4	10.250.0.1
IPv4 MAC	Cisco:00000c-07ac07
Ping Response	3 ms

Figure 43. Gateway Wi-Fi Tab

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 and Wi-Fi connections. The identity of the DHCP server, offer and acceptance timing, and lease information are provided. The OneTouch analyzer also detects and reports the presence of more than one DCHP server on the network.

Configuration

If the OneTouch 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 OneTouch analyzer is configured for DHCP, this test will run. To enable or disable DHCP, see page 249.

The **Time Limit** determines how much time can elapse before the OneTouch 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 DHCP.

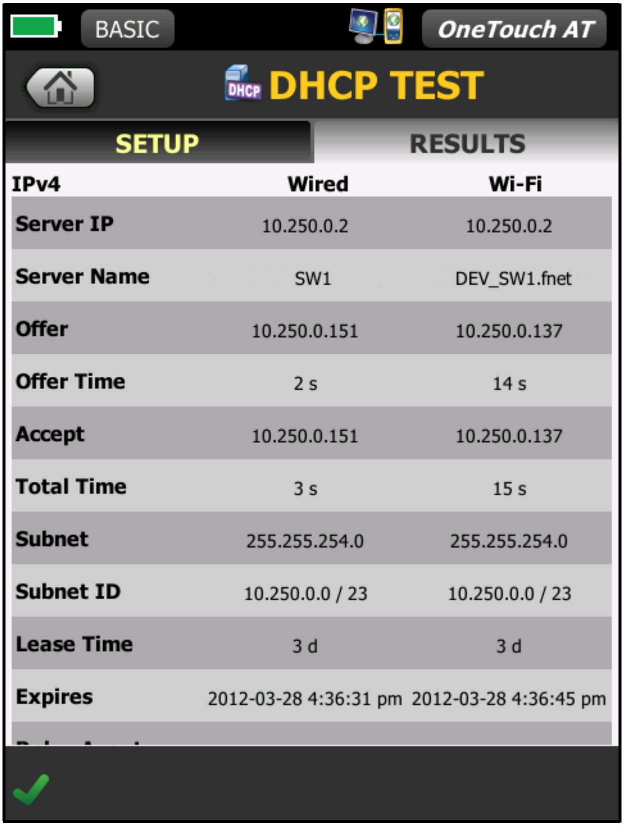
2 Tap the **SETUP** tab.

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

How it Works

The OneTouch 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



IPv4	Wired	Wi-Fi
Server IP	10.250.0.2	10.250.0.2
Server Name	SW1	DEV_SW1.fnet
Offer	10.250.0.151	10.250.0.137
Offer Time	2 s	14 s
Accept	10.250.0.151	10.250.0.137
Total Time	3 s	15 s
Subnet	255.255.254.0	255.255.254.0
Subnet ID	10.250.0.0 / 23	10.250.0.0 / 23
Lease Time	3 d	3 d
Expires	2012-03-28 4:36:31 pm	2012-03-28 4:36:45 pm

Figure 44. DHCP Test Results

Server IP is the IP address of the DHCP server.

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

IPv6 Wi-Fi Prefix - This is 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.)

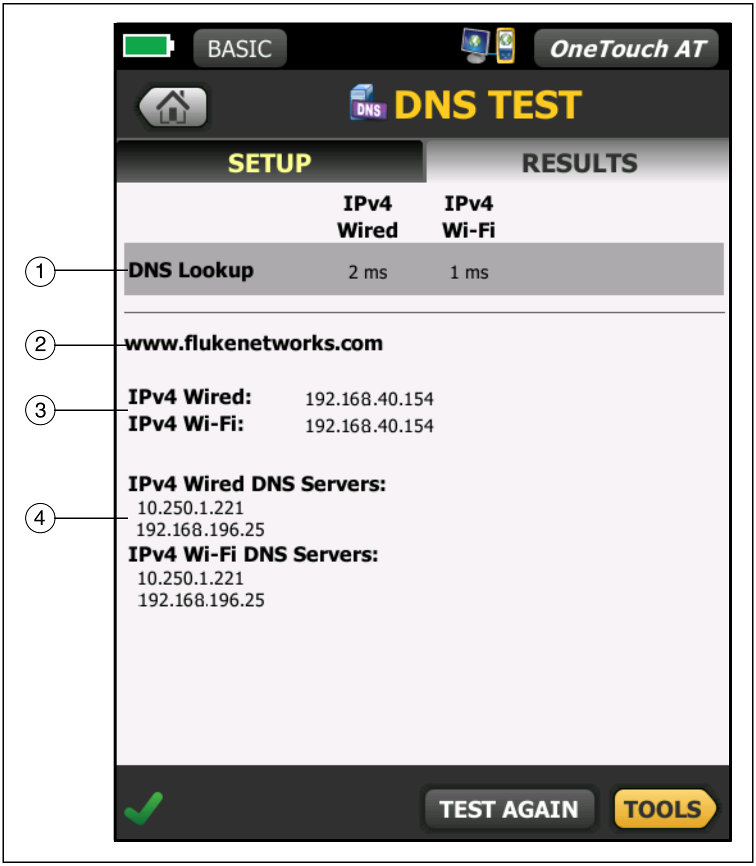
1. On the HOME screen, tap the DNS server icon DNS.
2. Tap the **SETUP** tab.
3. Tap the **Name** tab and enter the domain name to look up.
4. Tap the Time **Limit button** and choose the amount of time you want to allow for the test to complete.

How it Works

The address of the DNS server is obtained through DHCP or by static configuration, via the wired connection, the Wi-Fi connection, or both if available. The OneTouch 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 OneTouch analyzer can perform a DNS lookup for the configured URL via the wired or the Wi-Fi connection, the test will pass.



	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	2 ms	1 ms

www.flukenetworks.com

IPv4 Wired: 192.168.40.154
IPv4 Wi-Fi: 192.168.40.154

IPv4 Wired DNS Servers:
10.250.1.221
192.168.196.25
IPv4 Wi-Fi DNS Servers:
10.250.1.221
192.168.196.25

Figure 45. 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 wired hosts, access devices, and servers.

See Chapter 6: "Wired Analysis," beginning on page 171 for details.

Chapter 4: 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 analyzer settings, in a Profile. See “Profiles” on page 165.

Icons for user tests are located in the Test Tiers. The Test Tiers occupy the top half of the OneTouch analyzer’s display. See “Test Tiers” on page 34.

For instructions on adding user tests, see “Add a User Test” on page 45.

See also: “Finding User Test Target Servers in Wired Analysis” on page 181.

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

- **Ping (ICMP) Test, page 106**
- **Connect (TCP) Test, page 111**
- **Web (HTTP) Test, page 116**
- **File (FTP) Test, page 121**
- **Wired Performance Test, page 126**
- **Wi-Fi Performance Test, page 139**
- **Multicast (IGMP) Test, page 152**
- **Video (RTSP) Test, page 155**
- **Email (SMTP) Test, page 159**

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 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.

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.

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 OneTouch analyzer will send packets over the wired connection if available. If the wired connection is not available, the OneTouch analyzer will use the Wi-Fi connection. The OneTouch analyzer will not operate in Continuous mode over both wired and Wi-Fi connections.

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 OneTouch analyzer will send pings over all enabled interfaces. Wired IPv4 and wired IPv6 pings run simultaneously, then Wi-Fi IPv4 and Wi-Fi IPv6 pings run simultaneously.

Don't Fragment - When this option is **On**, the OneTouch 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

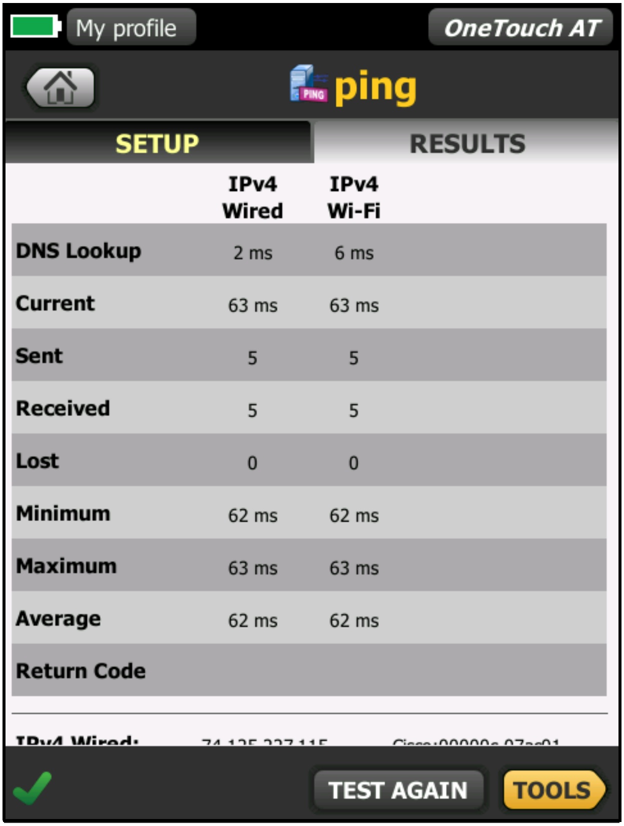
The ping test sends echo request packets to a host and awaits replies. Ping responses that don't return within the selected time limit are considered lost.

The OneTouch analyzer sends ICMP echo request packets to the target host (the server) and waits for a response. The OneTouch analyzer records the response time and reports whether packet loss occurs. The OneTouch 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.



	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	2 ms	6 ms
Current	63 ms	63 ms
Sent	5	5
Received	5	5
Lost	0	0
Minimum	62 ms	62 ms
Maximum	63 ms	63 ms
Average	62 ms	62 ms
Return Code		

IPv4 Wired: 74.125.227.115 Cisco:00000c-07ac01

Figure 46. Ping Test Results

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

Current - 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 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.

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 106.

Name - The Name button allows you to assign a custom name to the test. See also: “Name” on page 106.

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

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

The wired IPv4 and wired IPv6 tests run simultaneously. Then the Wi-Fi IPv4 and Wi-Fi IPv6 tests run simultaneously. So if you set a time limit of 10 seconds, a total of 20 seconds will be allowed: 10 seconds for wired tests and 10 seconds for Wi-Fi tests.

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 OneTouch analyzer will establish the TCP connection over the wired Ethernet connection if available. If the wired Ethernet connection is not available, the OneTouch analyzer will use the Wi-Fi connection. The OneTouch analyzer will not operate in Continuous mode over both wired and Wi-Fi connections.

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

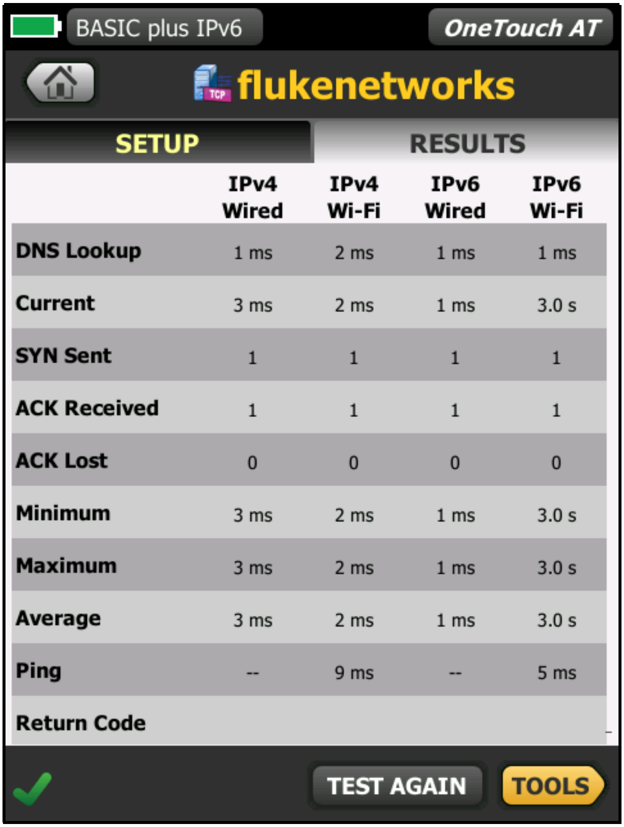
The TCP test performs a DNS lookup on the specified URL. If you specify an IP address, the DNS lookup is not performed.

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, Wi-Fi, IPv4, IPv6) within the time limit, the test will fail.



	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	1 ms	2 ms	1 ms	1 ms
Current	3 ms	2 ms	1 ms	3.0 s
SYN Sent	1	1	1	1
ACK Received	1	1	1	1
ACK Lost	0	0	0	0
Minimum	3 ms	2 ms	1 ms	3.0 s
Maximum	3 ms	2 ms	1 ms	3.0 s
Average	3 ms	2 ms	1 ms	3.0 s
Ping	--	9 ms	--	5 ms
Return Code				

Figure 47. 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 OneTouch analyzer.

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

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 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.

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 106.

Name - The Name button allows you to assign a custom name to the test. See also: "Name" on page 106.

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.

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.

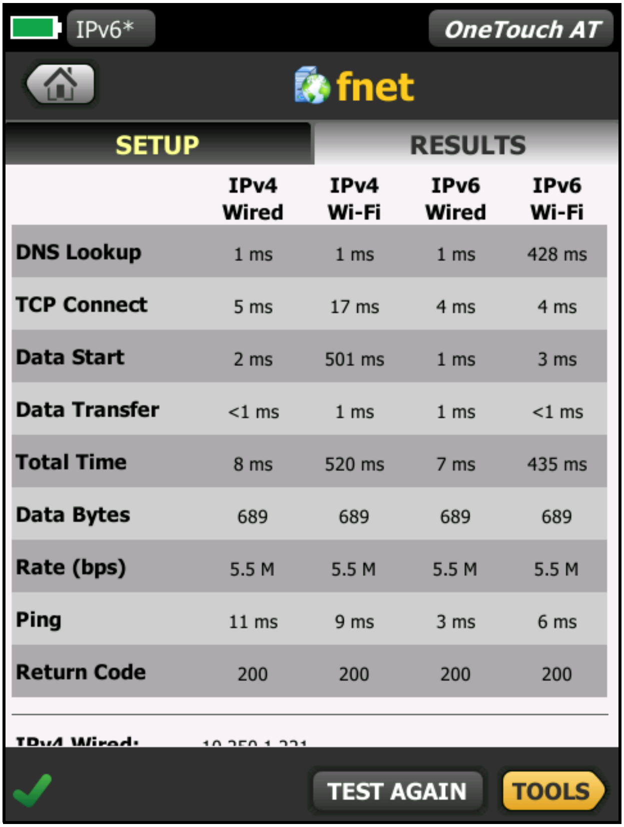
How it Works

When you execute an HTTP test, the OneTouch 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.

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.



	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	1 ms	1 ms	1 ms	428 ms
TCP Connect	5 ms	17 ms	4 ms	4 ms
Data Start	2 ms	501 ms	1 ms	3 ms
Data Transfer	<1 ms	1 ms	1 ms	<1 ms
Total Time	8 ms	520 ms	7 ms	435 ms
Data Bytes	689	689	689	689
Rate (bps)	5.5 M	5.5 M	5.5 M	5.5 M
Ping	11 ms	9 ms	3 ms	6 ms
Return Code	200	200	200	200

IPv4 Wired: 10.250.1.221

Figure 48. 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 addresses 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 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.

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.

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.

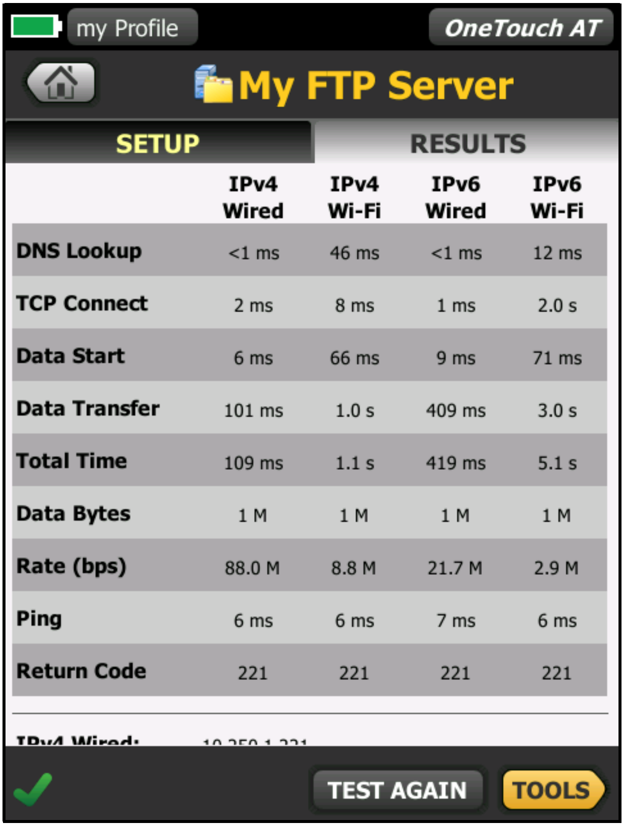
> If **Direction** is set to **Get**, File specifies the name of the file to be downloaded from the server. The file will be retrieved and the size and data rate will be calculated. Data is discarded as soon as it is downloaded. It is not written to a file and it is not retained on the OneTouch analyzer.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

How it Works

The OneTouch 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.



	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	<1 ms	46 ms	<1 ms	12 ms
TCP Connect	2 ms	8 ms	1 ms	2.0 s
Data Start	6 ms	66 ms	9 ms	71 ms
Data Transfer	101 ms	1.0 s	409 ms	3.0 s
Total Time	109 ms	1.1 s	419 ms	5.1 s
Data Bytes	1 M	1 M	1 M	1 M
Rate (bps)	88.0 M	8.8 M	21.7 M	2.9 M
Ping	6 ms	6 ms	7 ms	6 ms
Return Code	221	221	221	221

IPv4 Wired: 10.250.1.221

Figure 49. 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 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.

Wired Performance Test

Purpose

The OneTouch AT analyzer's Wired Performance 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 OneTouch AT 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

Connecting the Source and the Endpoint

1. Connect the controlling OneTouch AT analyzer to a point in the network (the source).
2. Connect a peer or reflector to another point in the network (the endpoint). Network performance is measured between the two points.

Configuration

Configuration includes setting up an endpoint, and setting up the source OneTouch AT analyzer. Traffic is exchanged and measured between the source and the endpoint

- The source is the OneTouch AT 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: peer and reflector.

Peer - A peer is another 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 round-trip traffic.

Reflector - A reflector is a LinkRunner AT 2000, LinkRunner Duo, or LinkRunner Pro. Frames are sent from the OneTouch AT analyzer and returned from the LinkRunner to the OneTouch AT analyzer. When using a reflector, the analyzer uses round trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

To Configure a OneTouch AT analyzer as a Peer

Follow these steps to configure a peer (OneTouch AT analyzer) endpoint.

1. Connect ac power to the OneTouch AT 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. The **Port** button appears.
4. If the default port is blocked, in use by another application, or otherwise unavailable, tap the **Port** button and select a different port. Note that you must select the same port in the source OneTouch AT Wired Performance Test configuration.

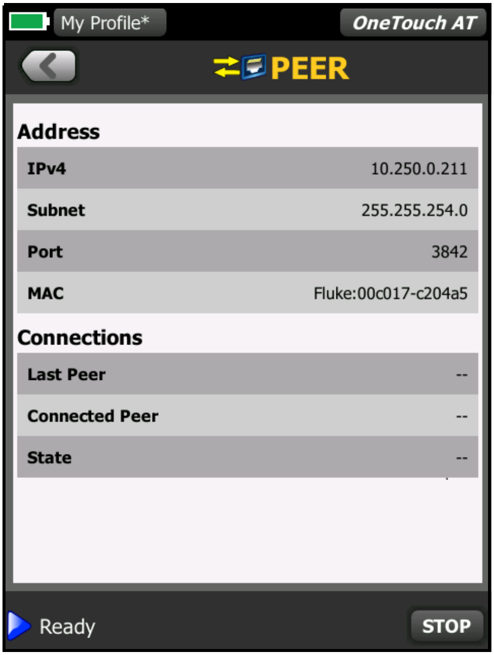
5 Tap the **START** button START. The PEER screen appears. Link will automatically be established if you have not yet run AutoTest (which establishes link). It may take up to a minute to establish link.

- The Address section of the screen shows information about the peer.
- The peer's IP address, subnet mask, and the control traffic port are shown.

Note

You need to supply the peer's IP address to the source OneTouch AT analyzer in a later step.

- The peer's MAC address is displayed.



Address

IPv4	10.250.0.211
Subnet	255.255.254.0
Port	3842
MAC	Fluke:00c017-c204a5

Connections

Last Peer	--
Connected Peer	--
State	--

Figure 50. Wired Performance Test - Peer Screen

The Connections section provides information about the connection to the source OneTouch AT analyzer. This section is populated with information when the source OneTouch AT analyzer initiates the test and the connections are made.

- The IP address of the last source OneTouch AT analyzer to which the peer was connected is shown.
- The IP address of the currently connected source is shown.
- The test state is shown: Ready, Running, or Finishing.

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.

To Configure a LinkRunner AT 2000 as a Reflector

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**.

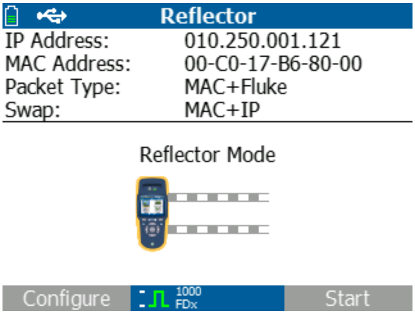
3 Select **General Configuration**.

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 tester will acquire an IP address. Note the IP address. You will enter this address when setting up the source OneTouch AT analyzer.

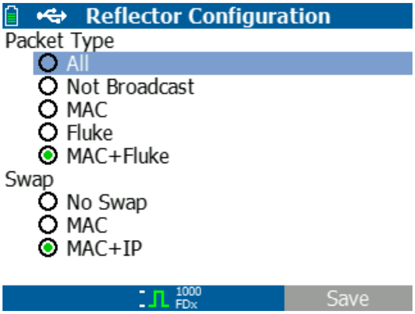
If the tester does not acquire an IP address, go to the Tools > IP Configuration screen and verify that DHCP has been selected or a static IP address has been entered.



Reflector

IP Address:	010.250.001.121
MAC Address:	00-C0-17-B6-80-00
Packet Type:	MAC+Fluke
Swap:	MAC+IP

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



Reflector Configuration

Packet Type
○ All
○ Not Broadcast
○ MAC
○ Fluke
● MAC+Fluke

Swap
○ No Swap
○ MAC
● MAC+IP

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

To Configure a LinkRunner Duo or LinkRunner Pro as a Reflector

Note

Reflector is a LinkRunner Duo and LinkRunner Pro option that needs to be purchased separately. Refer to the LinkRunner documentation to enable this option.

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

2 Power on the LinkRunner.

3 Scroll-down and select the Configuration icon.

4 Select the User Preferences icon.

5 Select the Power Options icon ⏻.

6 Use the up or down key to select the infinity symbol ∞.

7 Press the Select key to set the option. This will prevent the LinkRunner from powering down while reflecting traffic.

8 Select the IP Address configuration icon.

9 Select DHCP, the VLAN ID (optional), or manually enter an IP address the LinkRunner will use. Note the IP address. You will enter this address when setting up the source OneTouch AT analyzer.

10 Select the Reflector configuration icon.

11 Highlight the packet type icon.

12 Select the **MAC FLUKE** packet type.

13 Highlight the swap icon.

14 Select **MAC IP**.

15 Select the exit configuration icon.

16 Select the Reflector icon to run the Reflector.

To Configure the Source OneTouch AT Analyzer

1 Connect ac power to the OneTouch AT 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 Wired Performance test, and view its setup tab. See "Add a User Test" on page 45.

3 Tap the **Type** button. Set the type to **Peer** or **Reflector**. See "Configuration" on page 127.

Peer or Reflector - Tap this button and enter the IP address of the peer or reflector.

4 The **Name** button allows you to assign a custom name to the test. See also: "Name" on page 106.

5 → Rate - This is 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.

← Rate - This is 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 round-trip traffic, and only one rate can be specified.

6 **Allowed Loss** is the percentage of frames that can be lost. If this value is exceeded, the test will fail.

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

8 **Frame Size** is the size of the frames that the OneTouch 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 134.

9 The **DSCP** (Differentiated Services Code Point) control allows for verification of higher quality of service (QoS) for applications such as VoWiFi. Using the DSCP control, you can 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."

10 **Port** specifies the UDP port for the test's control connection. The same port must be specified on a peer endpoint. The next two higher port numbers are also used for the test. See "How it Works," below.

Run the Test

1 To run the test, ensure that you have started the endpoint, then 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.

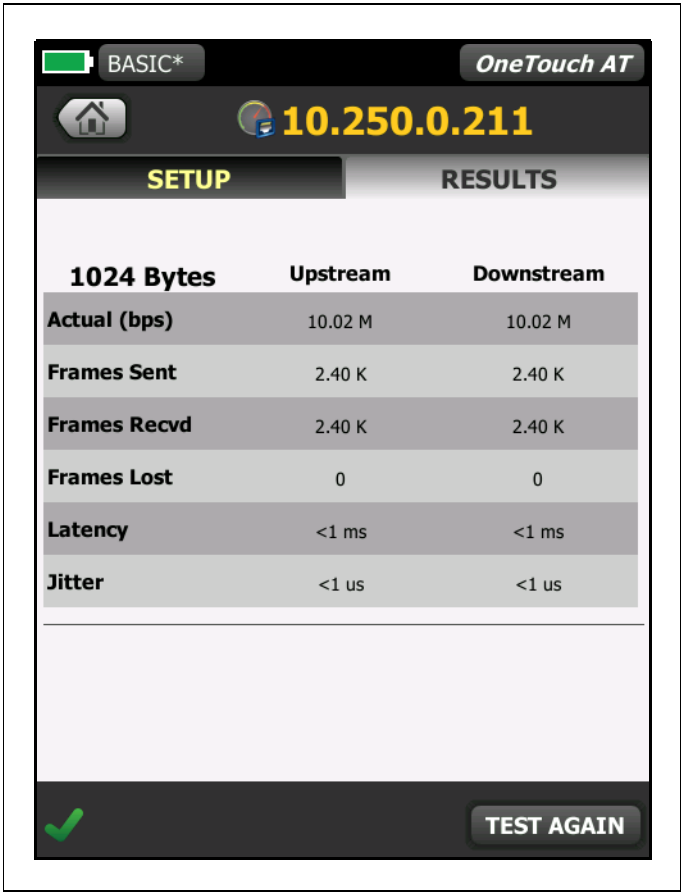
When using a peer endpoint (a OneTouch AT analyzer), separate upstream and downstream measurements are provided for rate, frames sent, frames received, and lost frames. Latency and jitter measurements are always made on the round-trip.

When using a reflector endpoint all measurements are made on the round-trip.

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.

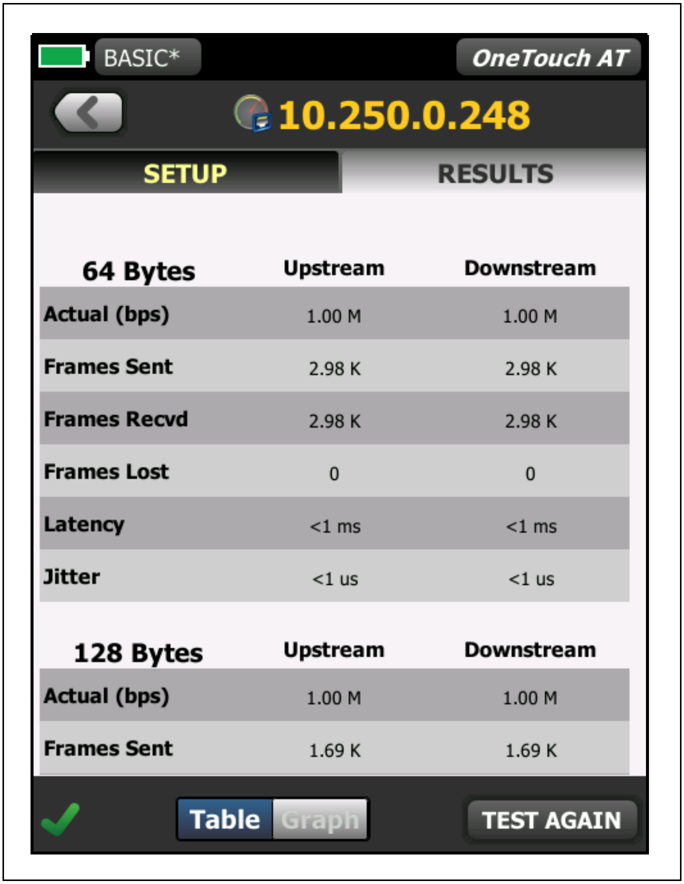
When you select a frame size other than “sweep” in the test configuration, the results screen looks like the image below.



1024 Bytes	Upstream	Downstream
Actual (bps)	10.02 M	10.02 M
Frames Sent	2.40 K	2.40 K
Frames Recvd	2.40 K	2.40 K
Frames Lost	0	0
Latency	<1 ms	<1 ms
Jitter	<1 us	<1 us

Figure 51. Wired Performance Test 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.



64 Bytes	Upstream	Downstream
Actual (bps)	1.00 M	1.00 M
Frames Sent	2.98 K	2.98 K
Frames Recvd	2.98 K	2.98 K
Frames Lost	0	0
Latency	<1 ms	<1 ms
Jitter	<1 us	<1 us

128 Bytes	Upstream	Downstream
Actual (bps)	1.00 M	1.00 M
Frames Sent	1.69 K	1.69 K

Figure 52. Wired Performance Test 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.

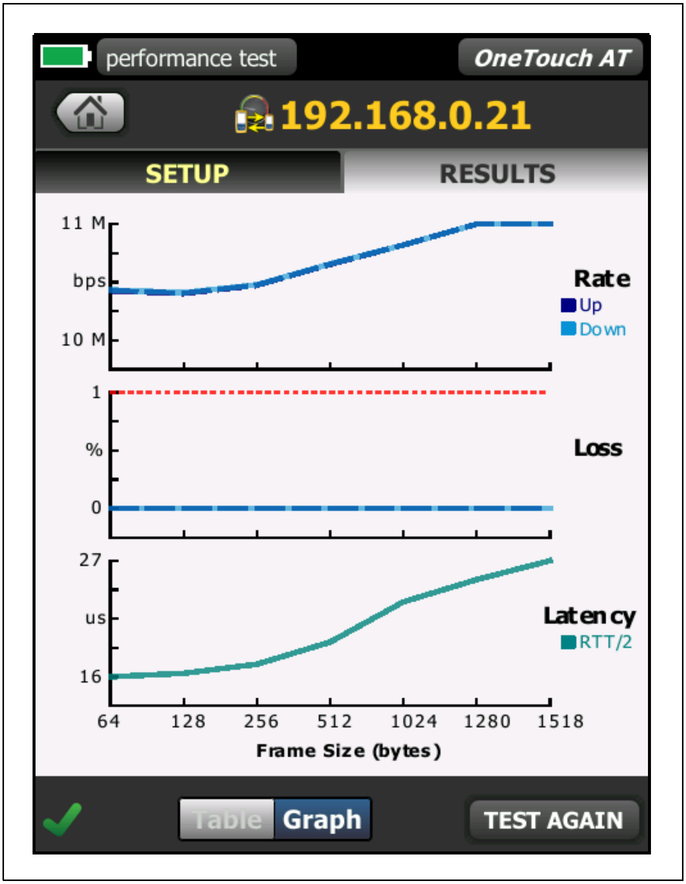


Figure 53. Wired Performance Test Results: RFC 2544 sweep, Graphical View

Rate (bps) is the measured bit rate.

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 the first frame is sent to the time that the last bit of the last frame is received.

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 round-trip 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 TEST AGAIN to re-run the test.

Wi-Fi Performance Test

Purpose

The OneTouch AT analyzer's Wi-Fi Performance Test provides point-to-point performance testing of a traffic stream across a Wi-Fi network segment into the wired IP network infrastructure. This test is used to validate 802.11 network performance. It qualifies Wi-Fi network performance in terms of throughput, loss, latency and jitter and integrates key Wi-Fi metrics as an indicator of overall local network health. The OneTouch AT analyzer exchanges a stream of traffic with peer devices, reflector devices or between its own wired and Wi-Fi ports (loopback) and measures the performance of the traffic stream.

Three test types are available: This OneTouch, Peer, and Reflector. The test is similar to the Wired Performance test but allows for the source device to operate in Wi-Fi mode and includes a third test type (This OneTouch).

Rates are user configurable up to 100 Mbps in both directions, with both directions tested simultaneously, with the exception of the Reflector test type. The user-selected frame size and rate (in bits-per-second) determines the number of transmitted frames per second.

The test passes if the measured amount of frame loss is lower than the user-configured **Loss Limitation.**

You can use the Wi-Fi Performance Test to

- Verify that a network configuration and RF environment deliver expected performance
- Evaluate newly deployed Wi-Fi infrastructure equipment
- Evaluate network performance prior to deployment of new services such as Video

Configuration

There are three test types: This OneTouch, Peer, and Reflector.

This OneTouch - This test type uses a single OneTouch AT analyzer as the source and the endpoint. The test will perform a loopback and provide separate upstream and downstream measurements for throughput, frames sent, frames received, and frames lost as well as Latency and Jitter measurements.

Peer - This test type uses two OneTouch AT analyzers. One of the analyzers will be the source, and the other analyzer will be the peer. 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 round trip traffic.

Reflector - A reflector is a LinkRunner AT 2000, LinkRunner Duo, or LinkRunner Pro. Frames are sent from the OneTouch AT analyzer (source) and returned from the LinkRunner (endpoint) to the OneTouch AT analyzer (source). When using a reflector, the analyzer uses round trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

To Configure a OneTouch AT analyzer as a Peer

Follow these steps to configure a peer (OneTouch AT analyzer) endpoint.

1 Connect ac power to the OneTouch AT 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. The Port button appears.

4 If the default port is blocked, in use by another application, or otherwise unavailable, tap the **Port** button and select a different port. Note that you must select the same port in the source OneTouch AT Wired Performance Test configuration.

5 Tap the **START** button START. The PEER screen appears. 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.

- The Address section of the screen shows information about the peer.
- The peer's IP address, subnet mask, and the control traffic port are shown.
- The peer's MAC address is displayed.
- The Connections section provides information about the connection to the source OneTouch AT analyzer. This section is populated with information when the source initiates the test and the connections are made.
- The IP address of the last source OneTouch AT analyzer to which the peer was connected is shown.
- The IP address of the currently connected source is shown.
- The test state is shown: Linking, Ready, Connecting, running, or finishing.
- The word "Ready" in the bottom-left corner indicates that the peer is ready to exchange traffic with the source.

To Configure a LinkRunner AT 2000 as a Reflector

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**.

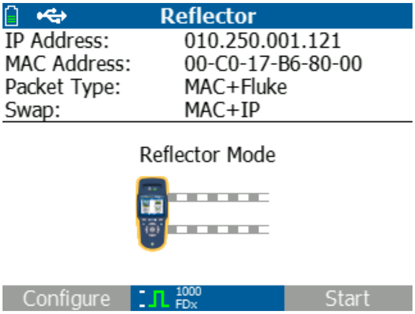
4 Under the Manage Power section, ensure that the **Auto Shutoff Enabled** check box is unchecked. This will prevent the LinkRunner from powering down while reflecting traffic.

5 Select **Save**.

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

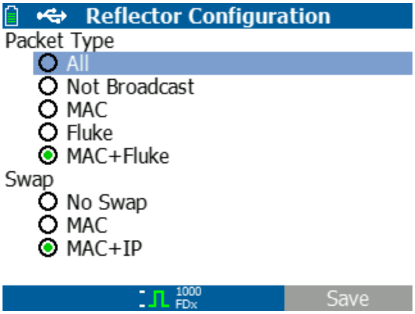


Reflector

IP Address: 010.250.001.121
MAC Address: 00-C0-17-B6-80-00
Packet Type: MAC+Fluke
Swap: MAC+IP

Reflector Mode

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



Reflector Configuration

Packet Type
○ All
○ Not Broadcast
○ MAC
○ Fluke
● MAC+Fluke

Swap
○ No Swap
○ MAC
● MAC+IP

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

To Configure a LinkRunner Duo or LinkRunner Pro as a Reflector

Note

Reflector is a LinkRunner Duo and LinkRunner Pro option that needs to be purchased separately. Refer to the LinkRunner documentation to enable this option.

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

2 Power on the LinkRunner.

3 Scroll-down and select the Configuration icon .

4 Select the User Preferences icon .

5 Select the Power Options icon ⏻.

6 Use the up or down key to select the infinity symbol ∞.

7 Press the Select key to set the option. This will prevent the LinkRunner from powering down while reflecting traffic.

8 Select the IP Address configuration icon .

9 Select DHCP, the VLAN ID (optional), or manually enter an IP address the LinkRunner will use. Note the IP address. You will enter this address when setting up the source OneTouch AT analyzer.

10 Select the Reflector configuration icon .

11 Highlight the packet type icon .

12 Select the **MAC FLUKE** packet type.

13 Highlight the swap icon .

14 Select **MAC IP**.

15 Select the exit configuration icon ☒.

16 Select the Reflector icon to run the Reflector .

Configure the Source OneTouch AT Analyzer

1 Connect ac power to the OneTouch AT 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 Wi-Fi Performance user test, and view its setup tab.

To run as This OneTouch test type

At the source OneTouch analyzer, in the Wi-Fi Performance test’s setup tab, ensure all options are set as described below.

Type - Select “This OneTouch” from the list. See “Configuration” on page 127.

The **Name** button allows you to assign a custom name to the test. See also: “Name” on page 106.

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

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

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

Duration is 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 is the size of the frames that the OneTouch analyzer will exchange with the endpoint. The header is included in the frame size.

The **DSCP** (Differentiated Services Code Point) control allows for verification of higher quality of service (QoS) for applications such as VoWiFi. Using the DSCP control, you can 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.”

Port specifies the UDP port for the data connection that will be used for the test. Note that the next higher port number will be used for data flowing in the opposite direction and only applies to the Peer and This OneTouch test type.

To run as the Peer Test Type

At the source OneTouch analyzer, in the Wi-Fi Performance test’s setup tab, ensure all options are set as described below.

Type - Select Peer from the list. See “Configuration” on page 127.

Peer - Enter the IP address of the endpoint to which you will be connecting.

The **Name** button allows you to customize the test name. See also: “Name” on page 106.

Rate - This is the rate of traffic from the Wi-Fi connection to the wired connection. Valid rates are from 100 Kbps to 100 Mbps.

Rate - This is the rate of traffic from the wired connection to the Wi-Fi connection. Valid rates are from 100 Kbps to 100 Mbps.

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

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

Frame Size is the size of the frames that the OneTouch analyzer will use for the test. The header is included in the frame size.

The **DSCP** (Differentiated Services Code Point) control allows for verification of higher quality of service (QoS) for applications such as VoWiFi. Using the DSCP control, you can 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."

Port specifies the UDP port for the data connection that will be used for the test. Note that the next higher port number will be used for data flowing in the opposite direction and only applies to the Peer and This OneTouch test type.

To run as the Reflector Test Type

At the source OneTouch analyzer, in the Wi-Fi Performance test's setup tab, ensure all options are set as described below.

Type - Select Reflector from the list. See "Configuration" on page 127.

Reflector - Enter the IP address of the endpoint to which you will be connecting.

The **Name** button allows you to assign a custom name to the test. See also: "Name" on page 106.

Rate - When using a reflector, upstream and downstream traffic are not individually measured. Results are based on round-trip traffic, and only one rate can be specified

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

Duration is 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 is the size of the frames that the OneTouch analyzer will exchange with the endpoint. The header is included in the frame size.

The **DSCP** (Differentiated Services Code Point) control allows for verification of higher quality of service (QoS) for applications such as VoWiFi. Using the DSCP control, you can 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.”

Port specifies the UDP port for the data connection that will be used for the test. Note that the next higher port number will be used for data flowing in the opposite direction and only applies to the Peer and This OneTouch test type.

How it Works

Each of the three test types establish a TCP control connection on a specified port for traffic from the Wi-Fi interface to the wired interface. Only the Peer and “This OneTouch” test types establish another TCP control connection on the next higher port number (specified port number +1) for traffic from the wired interface to the Wi-Fi interface. The Reflector test type uses a single TCP control connection due to the single round trip traffic stream.

In the Peer and "This OneTouch" test types, sequenced UDP traffic flows upstream on the specified port and downstream on the specified port +1, at the specified rates. The OneTouch analyzer measures and reports rate, loss, latency, jitter, sequence, etc.

In the Reflector test type, sequenced UDP traffic flows upstream and downstream on the single specified port. The OneTouch analyzer measures and reports rate, loss, latency, jitter, sequence, etc.

Along with IPv4 and IPv6 results, all Wi-Fi Performance tests include Wi-Fi network metrics computed over the duration of the test providing an indication of the health of the Wi-Fi connection

Roaming is not supported by the Wi-Fi Performance test.

Results

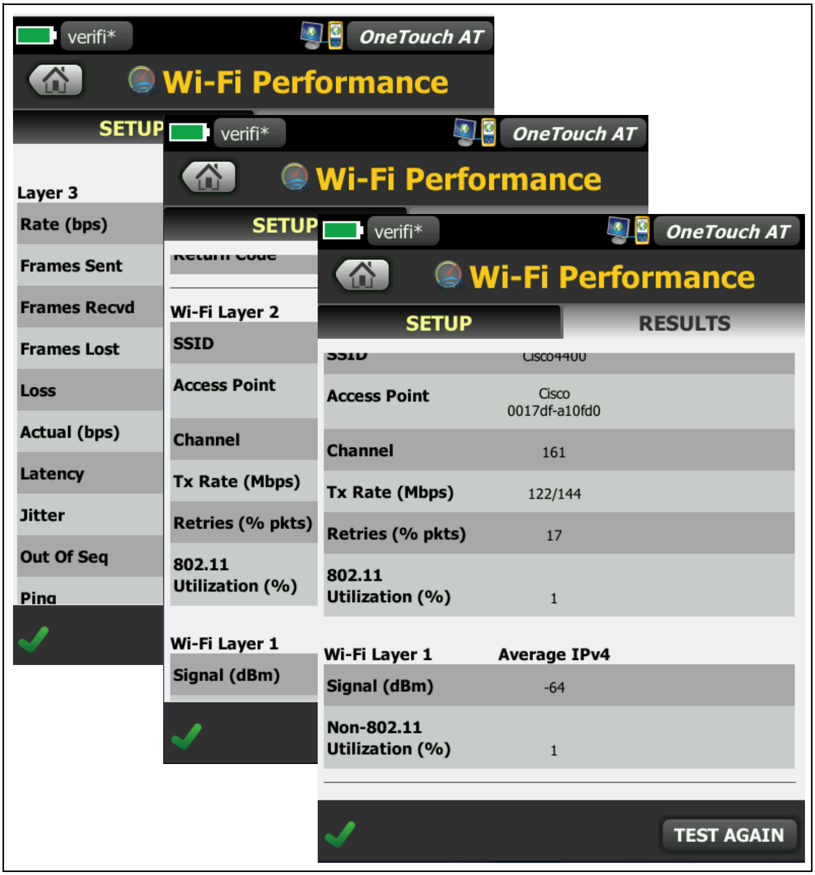
The Results tab shows test results separated into Layer 3, 2, and 1.

Layer 3 results

- Peer and Reflector test results are only available for IPv4.

- This OneTouch test results are available for IPv4 and IPv6, if configured for IPv6.
- The results in this layer are further separated into upstream and downstream connections. The Reflector test results will always be shown in one column.

Layer 2 and Layer 1 results show averaged Wi-Fi IPv4 and/or IPv6 metrics. IPv6 results will only be shown for the "This OneTouch" test type. See also: page 249.



Layer 3
Rate (bps)
Frames Sent
Frames Recvd
Frames Lost
Loss
Actual (bps)
Latency
Jitter
Out Of Seq
Ping

Return Code

Wi-Fi Layer 2
SSID
Access Point
Channel
Tx Rate (Mbps)
Retries (% pkts)
802.11 Utilization (%)

Wi-Fi Layer 1
Signal (dBm)

SSID	Cisco4400
Access Point	Cisco 0017df-a10fd0
Channel	161
Tx Rate (Mbps)	122/144
Retries (% pkts)	17
802.11 Utilization (%)	1
Wi-Fi Layer 1	**Average IPv4**
Signal (dBm)	-64
Non-802.11 Utilization (%)	1

Figure 54. Wi-Fi Performance Test Results

Layer 3 Results

The Peer and Reflector results shown in Layer 3 provide test metrics within a selected test duration for IPv4. The "This OneTouch" test type provides IPv4 test metrics and if configured, IPv6. Stream direction is indicated by the or icon at the top of a column.

Rate (bps) is the requested bit rate.

Frames Sent is the actual number of frames sent on the stream.

Frames Recvd is the actual number of frames received on the interface.

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

Loss is the percentage of frames that were lost.

Actual (bps) is the measured bit rate based on frames sent and the actual number of frames received.

Latency is the average one-way latency for "This OneTouch" and Reflector Wi-Fi Performance test types. The Peer test type is calculated by dividing the sum of the connection speed (from source to endpoint and then from endpoint to source) by two.

Jitter is the average frame delay variation.

Out of Seq is the number of frames that were received out-of-sequence.

A **Ping** test runs simultaneously with the Wi-Fi Performance test. If the Wi-Fi Performance 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.

Layer 2 Results

The results shown in Layer 2 provide an average of all collected IPv4 and/or IPv6 metrics for a specific test type during a selected test duration.

SSID - The name of the network on which the Wi-Fi connection was established during the test.

AP - This row shows the Access Point manufacturer and BSSID.

Channel - The channel number is shown.

Tx Rate - The transmission rate is shown in Mbps or Kbps, followed by a slash (/), then the maximum theoretical Tx rate. When the average rate is less than 30% of the maximum rate, a warning icon ⚠ is displayed.

Retries - A warning icon ⚠ is displayed when the average retry rate exceeds 40% of total packets.

802.11 Utilization - 802.11 utilization is reported in terms of the percentage of bandwidth usage on the connected channel. The utilization percentage value is based on the actual traffic level. During the Wi-Fi Performance Test, the OneTouch analyzer is a source of increased utilization, and it is the reason why this metric is not graded.

Layer 1 Results

The results shown in Layer 1 provide an average of all IPv4 and/or IPv6 metrics taken during a selected test duration. If you want to view IPv6 results, ensure that IPv6 is enabled on both wired and Wi-Fi interfaces. See also: page 249.

Signal strength statistics are displayed. A warning icon ⚠ is displayed when the average or maximum signal strength is equal to or below -75 dBm.

Non-802.11 Utilization - A warning icon ⚠ is displayed when non-802.11 utilization is greater than 20% of the channel’s bandwidth.

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.

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 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 106.

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.

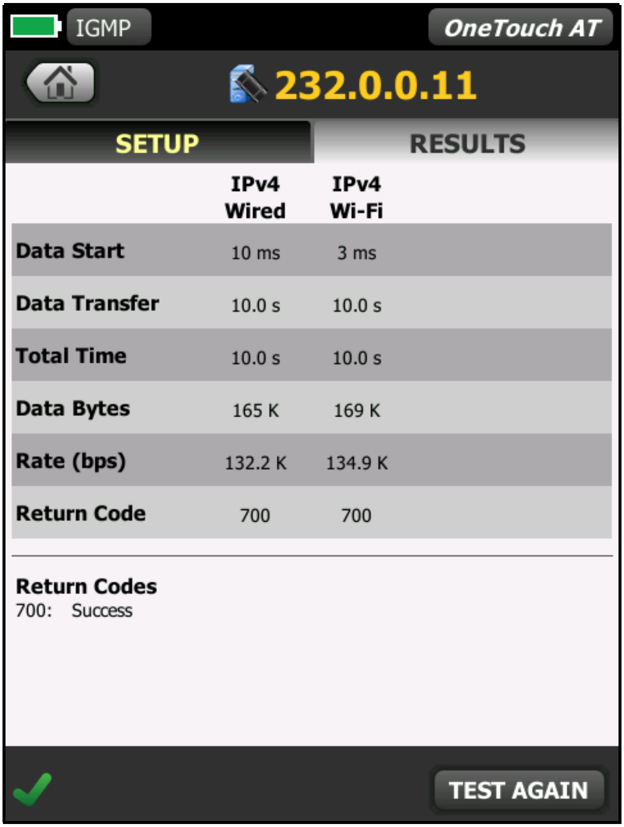
Version - If IGMP traffic other than the specified version is received, the test will fail. Note that in IGMPv3 the multicast source may be specified, thereby reducing the risk that an unauthorized party could supply the multicast data.

How it Works

The OneTouch 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 152.



	IPv4 Wired	IPv4 Wi-Fi
Data Start	10 ms	3 ms
Data Transfer	10.0 s	10.0 s
Total Time	10.0 s	10.0 s
Data Bytes	165 K	169 K
Rate (bps)	132.2 K	134.9 K
Return Code	700	700

Return Codes
700: Success

Figure 55. Multicast (IGMP) Test Results

Data Start is the amount of time it took to receive the first data byte after the OneTouch 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 TEST AGAIN 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 106.

The **Name** button allows you to assign a custom name to the test. See also: “Name” on page 106.

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.

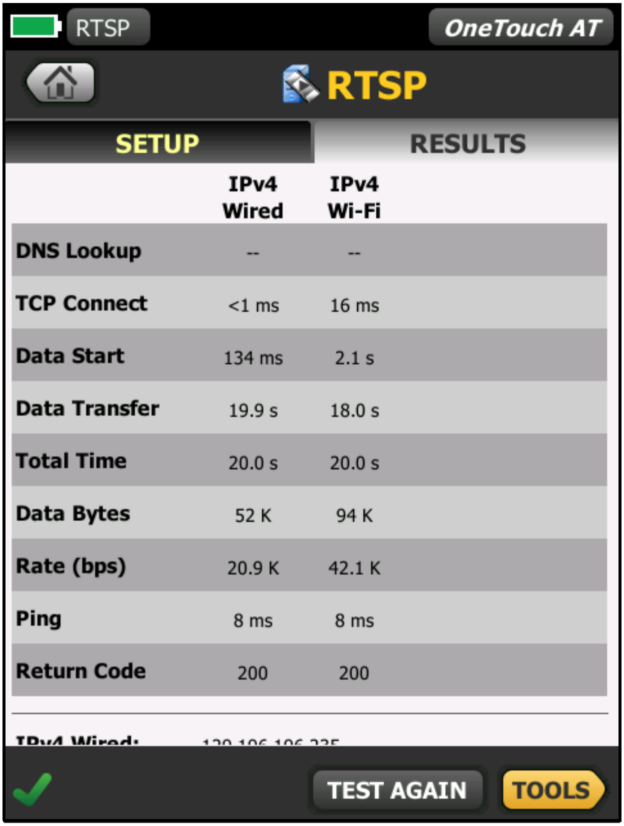
File is the name of the file that will be received (streamed).

How it Works

The OneTouch analyzer requests a session with the RTSP server. The file specified on the **File** button is streamed to the OneTouch 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.



	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	--	--
TCP Connect	<1 ms	16 ms
Data Start	134 ms	2.1 s
Data Transfer	19.9 s	18.0 s
Total Time	20.0 s	20.0 s
Data Bytes	52 K	94 K
Rate (bps)	20.9 K	42.1 K
Ping	8 ms	8 ms
Return Code	200	200

IPv4 Wired: 120.106.106.225

Figure 56. 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 OneTouch 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 or Wi-Fi connectivity using SMTP mail service.

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

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. If Wi-Fi or IPv6 are enabled (in addition to the wired IPv4 port), a separate message will be sent using each transport.

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 106.

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 OneTouch 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.

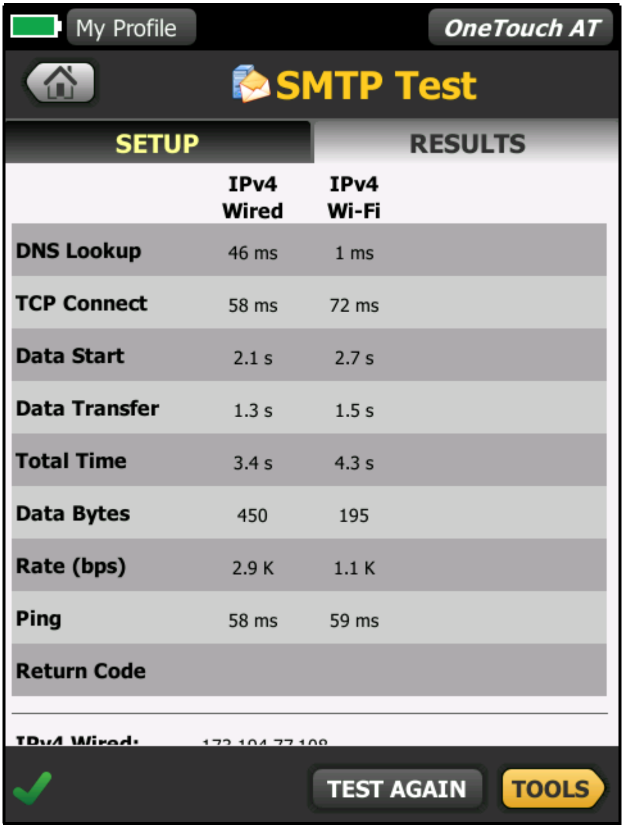
Login - If the SMTP server requires authentication, set **Login** to **On** and enter the username and password.

How it Works

The OneTouch analyzer adds the nearest switch information to the body of the email if it is sent via the wired interface. It adds AP information to the body of the email if sent over Wi-Fi. The OneTouch 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.



	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	46 ms	1 ms
TCP Connect	58 ms	72 ms
Data Start	2.1 s	2.7 s
Data Transfer	1.3 s	1.5 s
Total Time	3.4 s	4.3 s
Data Bytes	450	195
Rate (bps)	2.9 K	1.1 K
Ping	58 ms	59 ms
Return Code		

IPv4 Wired: 172.104.77.108

Figure 57. 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 OneTouch 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:

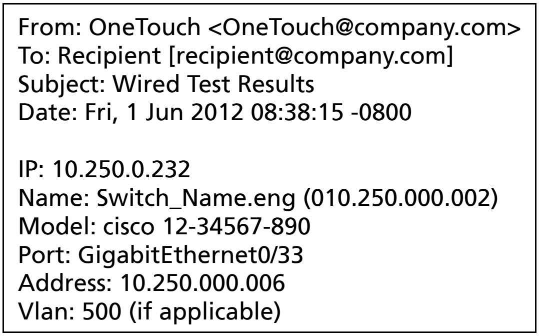
○ A progress spinner indicates the test is in progress.

✓ A green check mark indicates the test passed.

✗ A red x indicates the test failed.

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

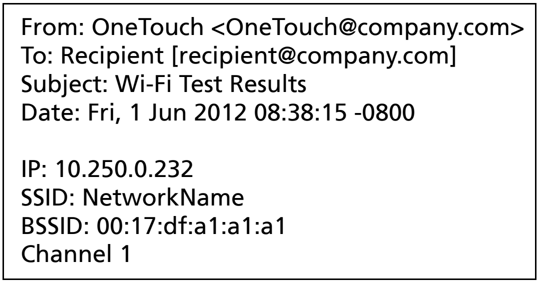
launch a browser against the target server, or Telnet/SSH to the server.



```
From: OneTouch <OneTouch@company.com>
To: Recipient [recipient@company.com]
Subject: Wired Test Results
Date: Fri, 1 Jun 2012 08:38:15 -0800

IP: 10.250.0.232
Name: Switch_Name.eng (010.250.000.002)
Model: cisco 12-34567-890
Port: GigabitEthernet0/33
Address: 10.250.000.006
Vlan: 500 (if applicable)
```

Figure 58. Email Sent From IPv4 Wired Connection



```
From: OneTouch <OneTouch@company.com>
To: Recipient [recipient@company.com]
Subject: Wi-Fi Test Results
Date: Fri, 1 Jun 2012 08:38:15 -0800

IP: 10.250.0.232
SSID: NetworkName
BSSID: 00:17:df:a1:a1:a1
Channel 1
```

Figure 59. Email Sent From IPv4 Wi-Fi Connection

Chapter 5: Profiles

OneTouch 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 PoE and 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 between the wired and Wi-Fi networks.

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.
- When you make changes to the current AP Authorization list, an asterisk appears after the profile name, indicating that the associated ACL has been modified.
- If you cycle power, the OneTouch 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 map the analyzer’s user file system as a network drive.

- See “Remote File Access Using an FTP Client” on page 314.
- See “Remote File Access Using a Mapped Network Drive (WebDAV)” on page 315.

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

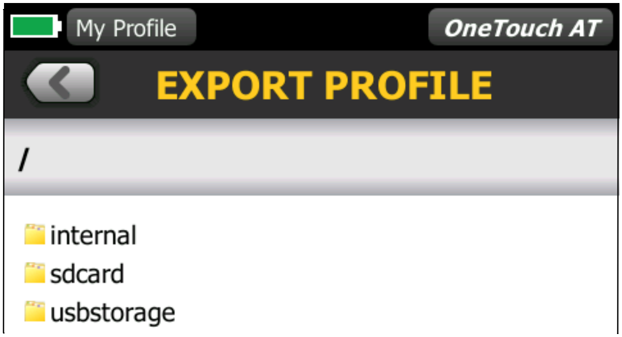
1 Connect a USB flash drive to the OneTouch analyzer. (You must do this before tapping the **MANAGE** button in step 3 so the USB flash drive will appear on the list.)

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 OneTouch.

9 Connect the USB flash drive to the destination OneTouch.

10 On the destination OneTouch, 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 OneTouch 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 303.) 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 analyzer. Profiles are not intended to be edited with a text editor. If they are edited outside the OneTouch analyzer they cannot be used because they are protected by a checksum.

Chapter 6: Wired Analysis

Wired Analysis

Description

The OneTouch analyzer discovers

- Devices in the broadcast domain
- 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.

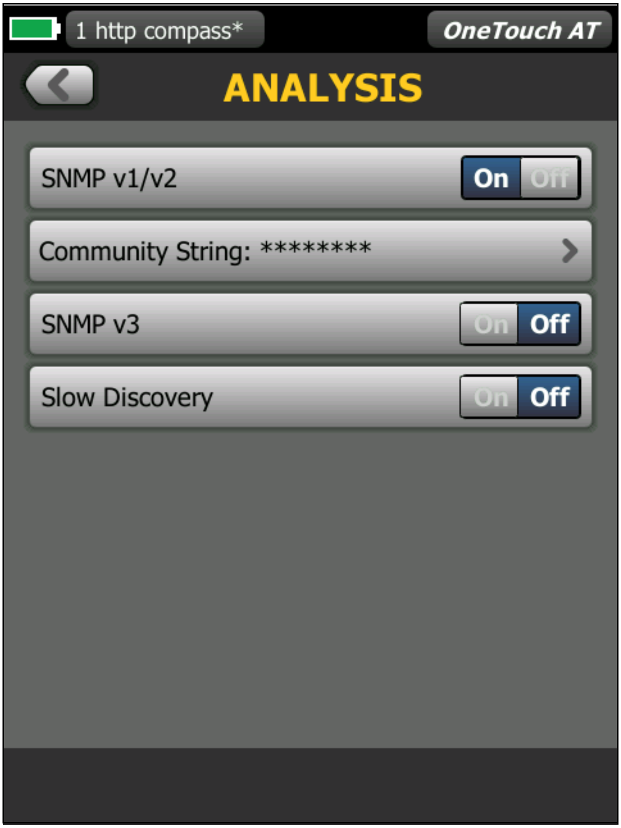
- Run path analysis to the device.
- Launch a web browser using the device as the target.
- Open a Telnet/SSH session with the device.

Configuration

To configure wired analysis:

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

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



1 http compass*

OneTouch AT

ANALYSIS

SNMP v1/v2 [✓ On] Off

Community String: ********

SNMP v3 On [✓ Off]

Slow Discovery On [✓ Off]

Figure 60. 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 38.

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.

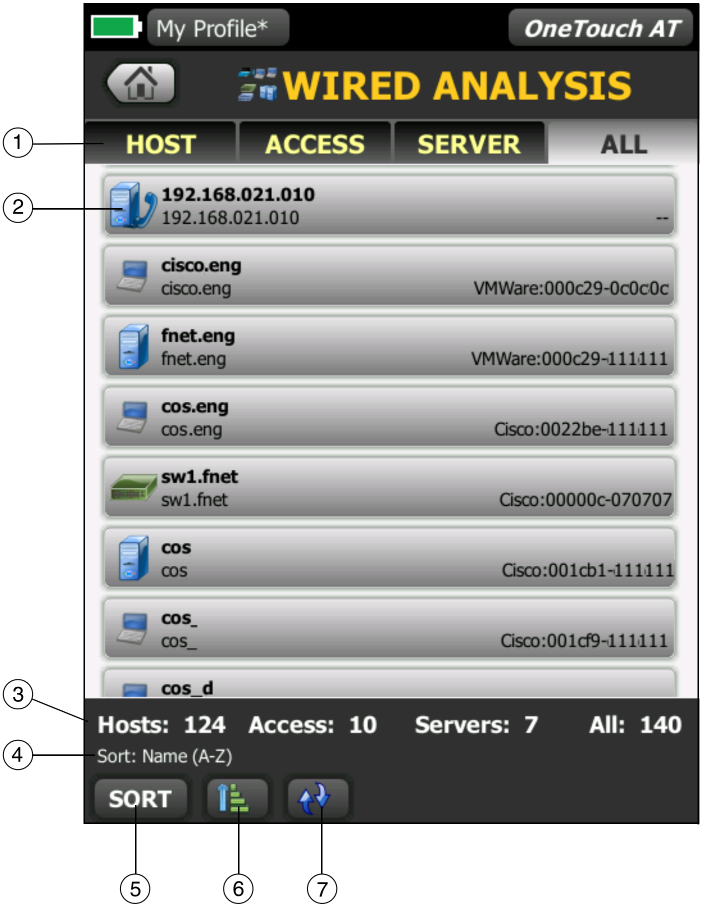
Devices are discovered using active and passive analysis methods.

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.



My Profile* OneTouch AT

WIRED ANALYSIS

HOST ACCESS SERVER ALL

192.168.021.010
192.168.021.010 --

cisco.eng
cisco.eng VMWare:000c29-0c0c0c

fnet.eng
fnet.eng VMWare:000c29-111111

cos.eng
cos.eng Cisco:0022be-111111

sw1.fnet
sw1.fnet Cisco:00000c-070707

cos
cos Cisco:001cb1-111111

cos_
cos_ Cisco:001cf9-111111

cos_d

Hosts: 124 Access: 10 Servers: 7 All: 140
Sort: Name (A-Z)

Figure 61. WIRED ANALYSIS Screen

① The HOST, ACCESS, AND SERVER tabs let you filter the Wired Analysis results. Access devices are switches, routers, etc. The ALL 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

Fluke Networks tool

VoIP call manager or VoIP TFTP server

VoIP phone

Virtual switch

Virtual machine

Hypervisor

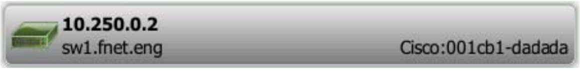
Wireless LAN controller

Wireless access point

Wi-Fi client

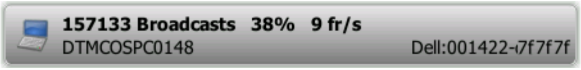
The information displayed on device buttons changes based on the sort key.

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.



10.250.0.2
sw1.fnet.eng Cisco:001cb1-dadada

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.



157133 Broadcasts 38% 9 fr/s
DTMCOSPC0148 Dell:001422-‹7f7f7f

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.

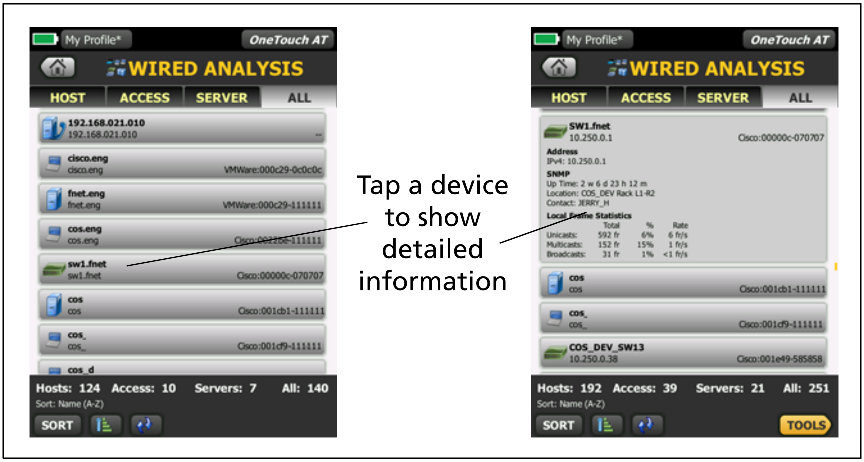
⑤ The **SORT** button SORT lets you sort the list of hosts, access devices, servers, or all devices. See “Wired Device Sorts” on page 179.

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.



192.168.021.010
192.168.021.010 --

cisco.eng
cisco.eng VMWare:000c29-0c0c0c

fnet.eng
fnet.eng VMWare:000c29-111111

cos.eng
cos.eng Cisco:00226e-111111

sw1.fnet
sw1.fnet Cisco:00000c-070707

cos
cos Cisco:001cb1-111111

cos_
cos_ Cisco:001cf9-111111

cos_d

Hosts: 124 Access: 10 Servers: 7 All: 140
Sort: Name (A-Z)

SW1.fnet
10.250.0.1 Cisco:00000c-070707

Address
IPv4: 10.250.0.1

SNMP
Up Time: 2 w 6 d 23 h 12 m
Location: COS_DEV Rack L1-R2
Contact: JERRY_H

Local Frame Statistics

	Total	%	Rate
Unicasts:	592 fr	6%	6 fr/s
Multicasts:	152 fr	15%	1 fr/s
Broadcasts:	31 fr	1%	<1 fr/s

cos
cos Cisco:001cb1-111111

cos_
cos_ Cisco:001cf9-111111

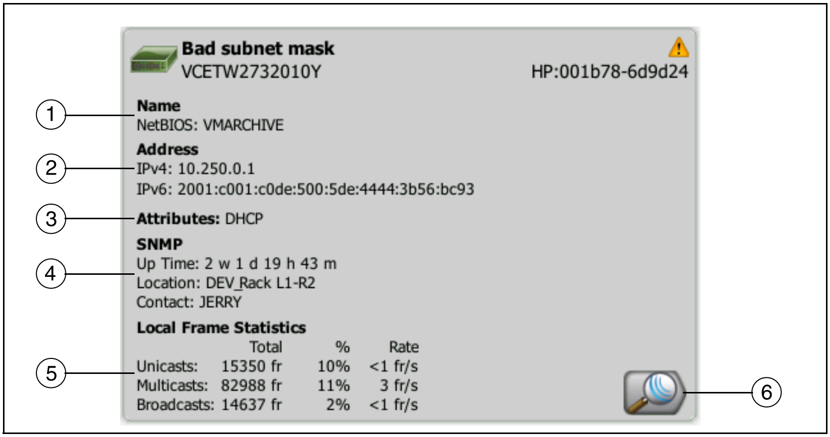
COS_DEV_SW13
10.250.0.38 Cisco:001e49-585858

Hosts: 192 Access: 39 Servers: 21 All: 251
Sort: Name (A-Z)

Tap a device to show detailed information

Figure 62. Displaying Wired Device Details

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



Bad subnet mask
VCETW2732010Y HP:001b78-6d9d24

Name
NetBIOS: VMARCHIVE

Address
IPv4: 10.250.0.1
IPv6: 2001:c001:c0de:500:5de:4444:3b56:bc93

Attributes: DHCP

SNMP
Up Time: 2 w 1 d 19 h 43 m
Location: DEV_Rack L1-R2
Contact: JERRY

Local Frame Statistics

	Total	%	Rate
Unicasts:	15350 fr	10%	<1 fr/s
Multicasts:	82988 fr	11%	3 fr/s
Broadcasts:	14637 fr	2%	<1 fr/s

Figure 63. 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 by the wired device.

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

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

⑥ Tap the Wi-Fi Discovery button 🔍, if shown, to go to the device’s Wi-Fi details screen. To return to the wired details screen, tap the Wired Discovery button 🔍. The discovery buttons will only be visible when a device has been discovered during both Wired and Wi-Fi Analysis.

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

  Lightweight wireless access point

  Wireless LAN controller

  Wi-Fi client

  Wireless access point

  Fluke Networks 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 in Wired Analysis

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 TOOLS.
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

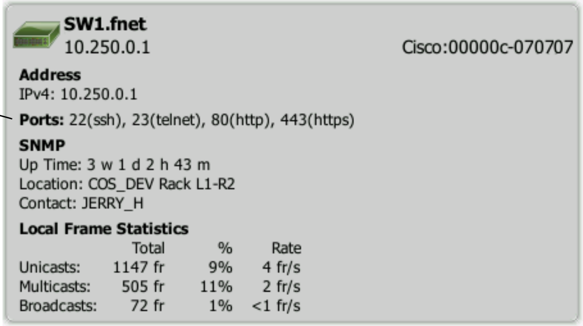
The Port Scan feature scans the target device for many commonly-used open ports. Results are reported on the device's button on the WIRED ANALYSIS screen. The device's button must be expanded to view the port scan results. To use the Port Scan feature:

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 OneTouch AT analyzer scans the target device for open ports. Results are reported on the device's expanded button.

Port scan results (open ports)



SW1.fnet
10.250.0.1 Cisco:00000c-070707

Address
IPv4: 10.250.0.1
Ports: 22(ssh), 23(telnet), 80(http), 443(https)

SNMP
Up Time: 3 w 1 d 2 h 43 m
Location: COS_DEV Rack L1-R2
Contact: JERRY_H

Local Frame Statistics

```
             Total      %     Rate
Unicasts:    1147 fr    9%    4 fr/s
Multicasts:   505 fr   11%    2 fr/s
Broadcasts:    72 fr    1%   <1 fr/s
```

Figure 64. 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 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) traceroute 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 174.

2 Run AutoTest.

3 Tap the Wired Analysis icon on the HOME screen.

4 Optional: Tap the **HOST**, **ACCESS**, or **SERVER** tab to narrow your view.

5 Tap a device’s button to expand it and view its details. The wired analysis TOOLS button TOOLS appears at the lower-right corner of the screen.

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

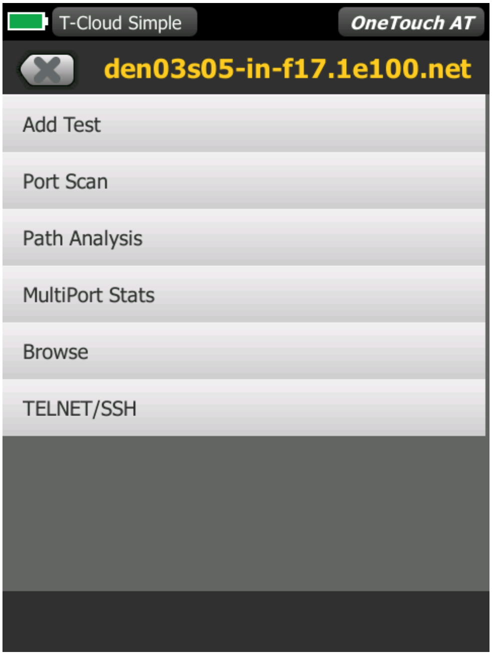


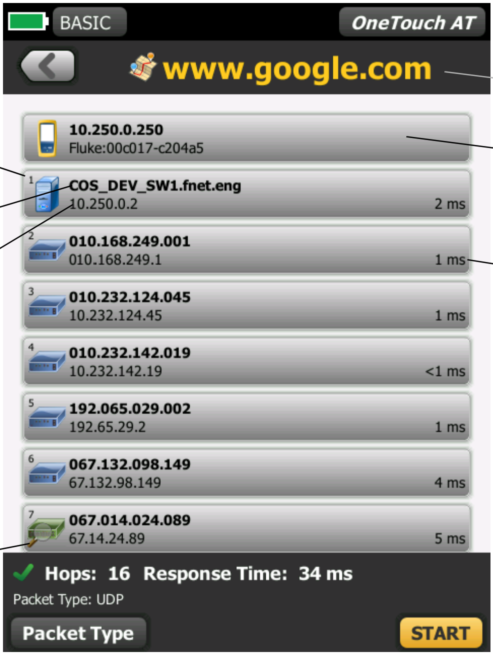
Figure 65. Wired Analysis Tools Menu

7 Tap the Path Analysis button.

The OneTouch AT 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 OneTouch AT 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 179.
- 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.



www.google.com

10.250.0.250
Fluke:00c017-c204a5

1 COS_DEV_SW1.fnet.eng
10.250.0.2 2 ms

2 010.168.249.001
010.168.249.1 1 ms

3 010.232.124.045
10.232.124.45 1 ms

4 010.232.142.019
10.232.142.19 <1 ms

5 192.065.029.002
192.65.29.2 1 ms

6 067.132.098.149
67.132.98.149 4 ms

7 067.014.024.089
67.14.24.89 5 ms

✓ Hops: 16 Response Time: 34 ms
Packet Type: UDP

Path analysis target

This OneTouch analyzer

Response time

Hop number

Best name

IP address

Magnifying glass indicates that SNMP port statistics are available when you tap the button

Figure 66. Path Analysis Results

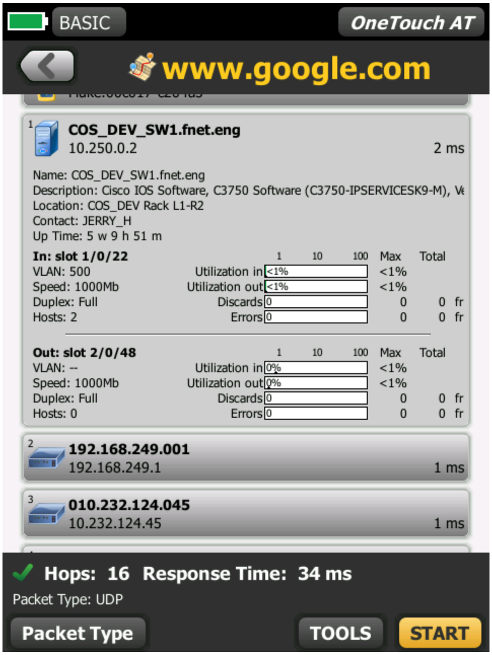
The following information is shown at the bottom of the screen.

- 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.



```
1 COS_DEV_SW1.fnet.eng
  10.250.0.2                                                   2 ms

Name: COS_DEV_SW1.fnet.eng
Description: Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Ve
Location: COS_DEV Rack L1-R2
Contact: JERRY_H
Up Time: 5 w 9 h 51 m

In: slot 1/0/22                       1     10    100   Max   Total
VLAN: 500             Utilization in  <1%               <1%
Speed: 1000Mb         Utilization out <1%               <1%
Duplex: Full                Discards  0                  0     0  fr
Hosts: 2                      Errors  0                  0     0  fr

Out: slot 2/0/48                      1     10    100   Max   Total
VLAN: --              Utilization in  0%                <1%
Speed: 1000Mb         Utilization out 0%                <1%
Duplex: Full                Discards  0                  0     0  fr
Hosts: 0                      Errors  0                  0     0  fr

2 192.168.249.001
  192.168.249.1                                                1 ms

3 010.232.124.045
  10.232.124.45                                                1 ms

✓ Hops: 16  Response Time: 34 ms
Packet Type: UDP
```

Figure 67. Path Analysis - Detailed Results

Tap the START button START to clear the results and run path analysis again.

MultiPort Statistics

The OneTouch AT 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 174.

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 171.

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 TOOLS button.

   If the OneTouch AT is configured for SNMP access to the device and MultiPort Statistics are available, the **MultiPort Stats** button appears in the tools menu, as shown below.

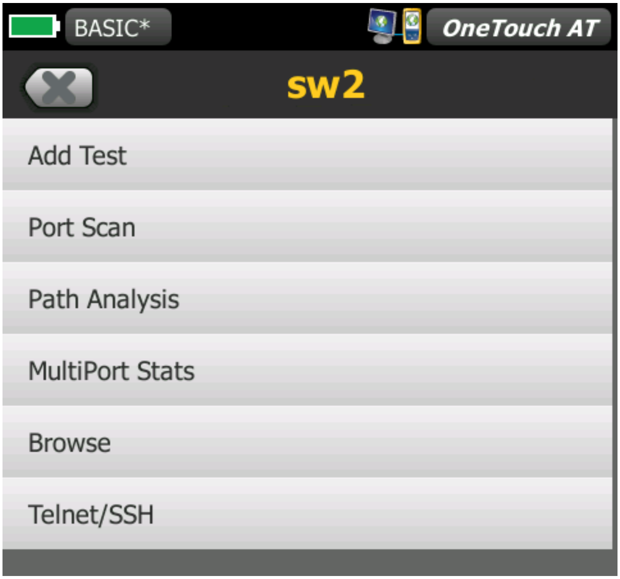


Figure 68. MultiPort Statistics Button on Wired Analysis Tools Menu

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 . If MultiPort Statistics are available, the MULTIPORT STATS button MULTIPORT STATS will be shown in the lower-right corner of the SWITCH or GATEWAY screen.

2 Tap the MULTIPORT STATS button MULTIPORT STATS to display the device’s port statistics.

MultiPort Statistics via Path Analysis

Path analysis is described beginning on page 183.

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.

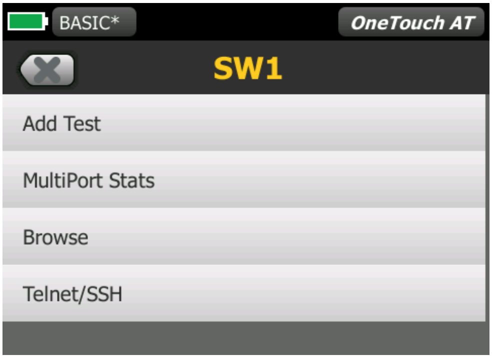
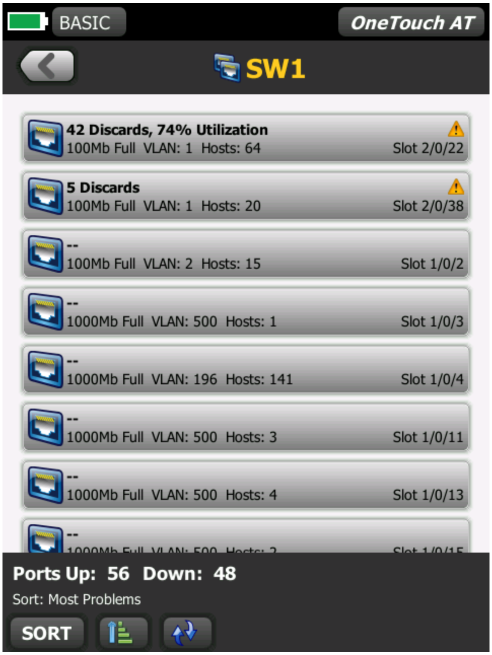


Figure 69. MultiPort Statistics Button on Path Analysis Tools Menu

3 Tap the **MultiPort Stats** button to display the device’s port statistics.

MultiPort Statistics Summary Screen

- When you tap the MultiPort Stats button, the OneTouch AT analyzer gathers information from the device and displays it on a summary screen.



42 Discards, 74% Utilization
100Mb Full VLAN: 1 Hosts: 64 Slot 2/0/22

5 Discards
100Mb Full VLAN: 1 Hosts: 20 Slot 2/0/38

--
100Mb Full VLAN: 2 Hosts: 15 Slot 1/0/2

--
1000Mb Full VLAN: 500 Hosts: 1 Slot 1/0/3

--
1000Mb Full VLAN: 196 Hosts: 141 Slot 1/0/4

--
1000Mb Full VLAN: 500 Hosts: 3 Slot 1/0/11

--
1000Mb Full VLAN: 500 Hosts: 4 Slot 1/0/13

--
1000Mb Full VLAN: 500 Hosts: 2 Slot 1/0/15

Ports Up: 56 Down: 48
Sort: Most Problems

Figure 70. 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

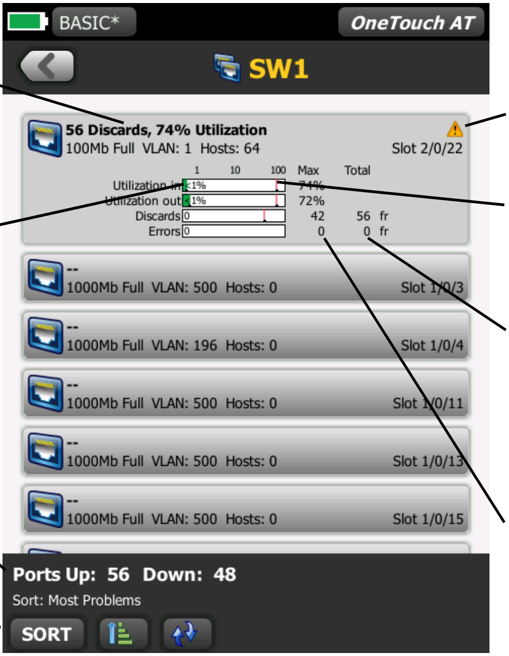
- Duplex mode
- Problems (problem severity)
- Utilization In/Out
- Utilization In
- Utilization Out
- VLAN number
- Host Count (number of connected hosts)

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.



56 Discards, 74% Utilization
100Mb Full VLAN: 1 Hosts: 64 Slot 2/0/22

	1 10 100	Max	Total	
Utilization in	<1%	74%		
Utilization out	<1%	72%		
Discards	0	42	56	fr
Errors	0	0	0	fr

--
1000Mb Full VLAN: 500 Hosts: 0 Slot 1/0/3

--
1000Mb Full VLAN: 196 Hosts: 0 Slot 1/0/4

--
1000Mb Full VLAN: 500 Hosts: 0 Slot 1/0/11

--
1000Mb Full VLAN: 500 Hosts: 0 Slot 1/0/13

--
1000Mb Full VLAN: 500 Hosts: 0 Slot 1/0/15

Ports Up: 56 Down: 48
Sort: Most Problems

Problem summary

Current value is indicated by a solid bar

Ports linked (up) and idle (down)

Sort controls

Triangle indicates an error or warning

Maximum observed value

Total since MultiPort statistics began

Maximum value observed

Figure 71. 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.

Web Browser

When you tap the **Browse** button, the browser is launched with the selected device as the target server. See "Browser" on page 262.

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 263.

Chapter 7: Wi-Fi Analysis

The OneTouch analyzer provides you with information and guidance to quickly assess the state of your Wi-Fi network and troubleshoot issues impacting your end users’ connectivity and performance experience.

OneTouch analyzer Wi-Fi analysis consists of discovery and analysis of 802.11 networks, access points, clients, and channels being used. Tools are available for troubleshooting client connectivity and locating devices that may pose a security risk or devices impacting network operations.

The analyzer supports 802.11 a/b/g/n technologies, operating in both the 2.4 GHz and 5 GHz bands. **Wi-Fi** must be enabled for Wi-Fi analysis to begin. See “Enable Wi-Fi” (below).

Enable Wi-Fi

To enable Wi-Fi on the OneTouch analyzer:

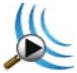
1. On the HOME screen, tap **TOOLS** 🛠.
2. Tap the **Wi-Fi** button.
3. Ensure that **Enable Wi-Fi** is **On**.

Wi-Fi setup is described in “Establish a Wi-Fi Connection” on page 51.

Wi-Fi Icon on the HOME Screen

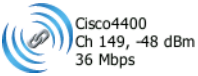
The Wi-Fi icon changes to indicate Wi-Fi link or scanning status. Tap the icon to initiate Wi-Fi analysis and display the Wi-Fi ANALYSIS screen.

Stopped



When you power-on the OneTouch analyzer, Wi-Fi is in the Stopped mode. The Wi-Fi adapter is idle. Tap the icon to initiate Wi-Fi analysis.

Linked and testing

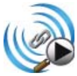


Cisco4400
Ch 149, -48 dBm
36 Mbps

If you have configured the OneTouch analyzer to connect to a Wi-Fi network, the analyzer will attempt to link when you run AutoTest. When a Wi-Fi link is established, the following values are shown next to the icon. The values are updated once per second.

- SSID (Network name)
- Channel number and signal level
- Connect rate

Linked but not actively testing



When AutoTest completes, the link is maintained and this icon is displayed. Tap the icon to drop the Wi-Fi link, start Wi-Fi scanning, and view the Wi-Fi ANALYSIS screen.

Scanning

This icon is shown when the analyzer is performing Wi-Fi analysis (scanning). The OneTouch analyzer continuously scans through all channels in the configured bands (2.4 GHz and/or 5 GHz). Tap the icon to display the Wi-Fi ANALYSIS screen.

Access Point Icon on the Home Screen

Tap the AP icon to view the Wi-Fi Network Connect test results.

See “Wi-Fi Network Connect Test” on page 89.

Wi-Fi Analysis

Passive Wi-Fi Analysis

The OneTouch AT analyzer discovers Wi-Fi networks and devices by passively monitoring (scanning) the 2.4 GHz and 5 GHz bands for network traffic.

Active Wi-Fi Analysis

Probing for SSIDs

When **Transmit Probes** is **On** the analyzer sends probe requests for all SSIDs that are configured in all saved Profiles, plus the currently loaded profile (regardless of whether it has been saved). This speeds the network discovery process and the resolution of non-broadcast [Hidden] SSIDs.

A hidden, unresolved network is shown in brackets (i.e, [Hidden]). A hidden, resolved name is also shown in brackets (e.g. [NetworkName]).

See Chapter 5: "Profiles," beginning on page 165.

1 Tap the TOOLS icon 🛠 on the HOME screen.

2 Tap the **Wi-Fi** button.

3 Ensure that **Enable Wi-Fi** is **On**.

4 Set **Transmit Probes** to **On** to probe for all SSIDs stored in Profiles.

Wi-Fi Network Connect Test and Scan Only Mode

When **Scan Only** is **Off** the analyzer attempts to connect to the configured network when AutoTest runs. See “Wi-Fi Network Connect Test” on page 89.

When **Scan Only** is **On** the analyzer does not attempt to connect to a Wi-Fi network when AutoTest runs.

1 Tap the TOOLS icon 🛠 on the HOME screen.

2 Tap the **Wi-Fi** button.

3 Ensure that **Enable Wi-Fi** is **On**.

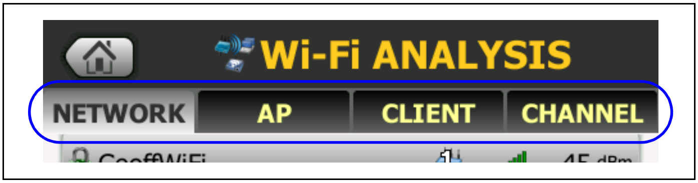
4 Set **Scan Only** to **On** or **Off**.

Wi-Fi Analysis Screens

There are four tabs on the Wi-Fi Analysis screen:

- Network
- AP (Access Point)
- Client
- Channel

Tap a tab to display the corresponding analysis screen.

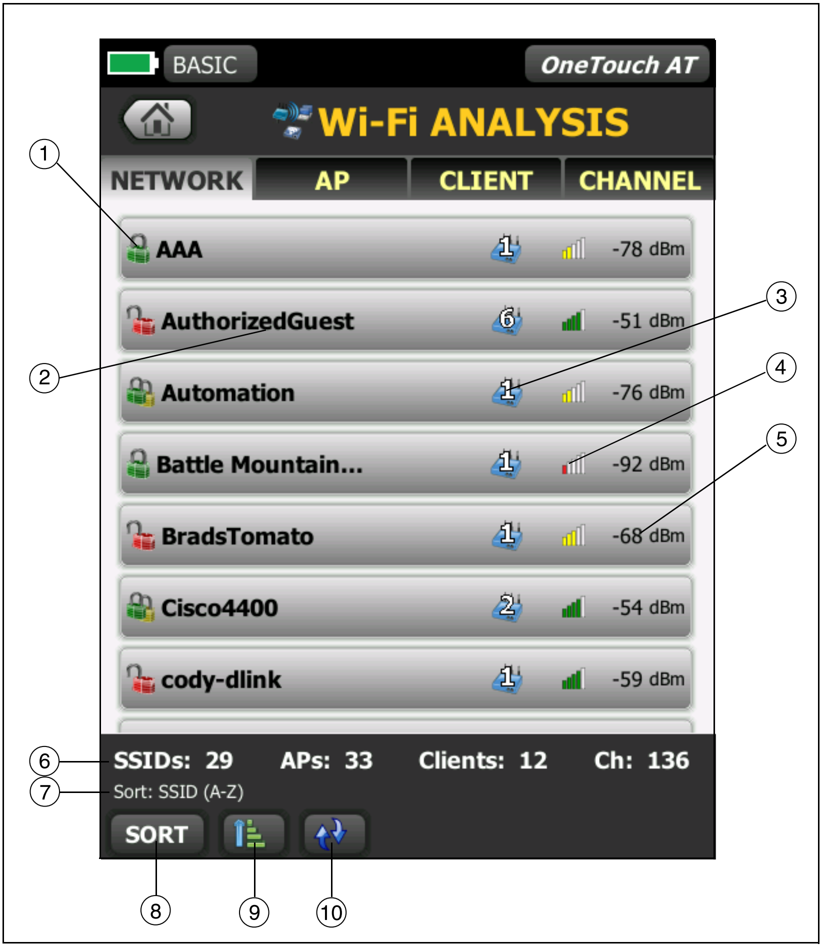


Network Analysis

The NETWORK analysis tab provides:

- A sortable list of all discovered Wi-Fi networks with summary information for each network (See Figure 72)
- A graphical representation of network coverage and important network details
- Filter buttons that provide deeper analysis of each network’s access points, clients, and channels

Each network's summary information is displayed on a button.



AAA 1 -78 dBm
AuthorizedGuest 6 -51 dBm
Automation 1 -76 dBm
Battle Mountain... 1 -92 dBm
BradsTomato 1 -68 dBm
Cisco4400 2 -54 dBm
cody-dlink 1 -59 dBm

SSIDs: 29 APs: 33 Clients: 12 Ch: 136
Sort: SSID (A-Z)

Figure 72. Wi-Fi Network Analysis Tab, Sorted by SSID

① This icon indicates the network’s security level.

🔒 A green lock indicates WPA-Personal, WPA-Enterprise, WPA2-Personal, or WPA2-Enterprise security are in use.

🔒 A yellow lock indicates WEP or 802.1X (using WEP encryption) are in use.

🔓 A red lock indicates that no security is in use.

🔒 A double lock indicates multiple security types are in use.

Note that the security type (e.g. WPA-Enterprise) is shown in the network detail screen. See page 208.

② This is the network’s name (its SSID). If the network name is hidden (i.e. not broadcast), the name is displayed in brackets. A hidden, unresolved name looks like this: [Hidden]. A hidden, resolved name looks like this: [Network Name].

③ This changes based on the sort key that you select after tapping the SORT button SORT. The access point icon 2 shows the number of discovered access points supporting the network. The clients icon 💻 shows the number of clients on the network. The ad hoc icon indicates an ad hoc network.

④ The signal strength icon provides a quick visual indication of the network’s signal strength as measured by the OneTouch analyzer.
📶 5 bars: greater than -50 dBm
📶 4 bars: -50 dBm to -64 dBm
📶 3 bars: -65 dBm to -74 dBm
📶 2 bars: -75 dBm to -84 dBm
📶 1 bar: -85 dBm or less

⑤ This is the network’s signal level (in dBm). For networks with more than one AP, this is the strongest signal level as measured by the OneTouch analyzer.

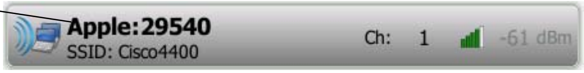
⑥ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of SSIDs (networks), APs (access points), and clients found. It also shows channel numbers as they are scanned.

⑦ The currently selected sort key is displayed above the **SORT** button .

⑧ The **SORT** button lets you sort the list of networks according to:

- SSID
- Signal level
- Number of access points
- Number of clients
- Security level
- Network type (infrastructure or ad hoc)

If the sort key is text, it is bold.



Apple:29540
SSID: Cisco4400
Ch: 1 -61 dBm

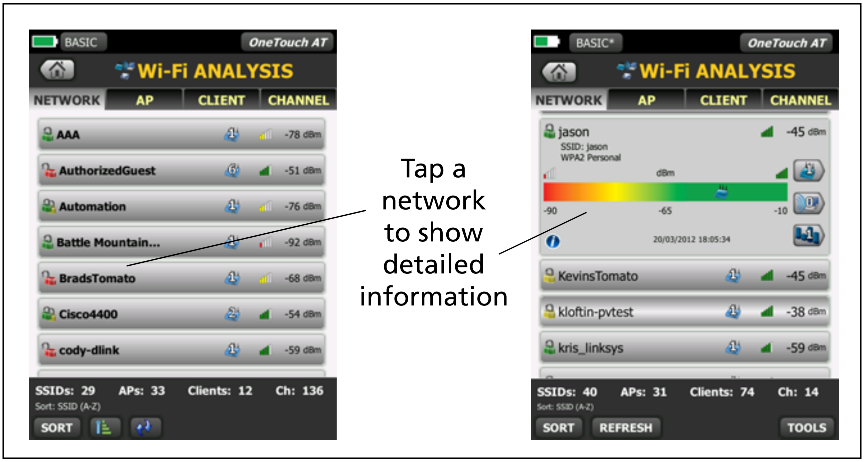
On network buttons, the sort key (except security and network type) appears in bold text.

⑨ The Sort Order button determines whether the sorted results are shown in ascending or descending order.

⑩ The **REFRESH** button clears all Wi-Fi analysis results and restarts Wi-Fi analysis.

To Show Network Details

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



AAA	-78 dBm
AuthorizedGuest	-51 dBm
Automation	-76 dBm
Battle Mountain...	-92 dBm
BradsTomato	-68 dBm
Cisco4400	-54 dBm
cody-dlink	-59 dBm

SSIDs: 29 APs: 33 Clients: 12 Ch: 136
Sort: SSID (A-Z)

Tap a network to show detailed information

jason -45 dBm
SSID: jason
WPA2 Personal
20/03/2012 18:05:34

KevinsTomato	-45 dBm
kloftin-pvtest	-38 dBm
kris_linksys	-59 dBm

SSIDs: 40 APs: 31 Clients: 74 Ch: 14
Sort: SSID (A-Z)

Figure 73. Displaying Wi-Fi Network Details

Network Details

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

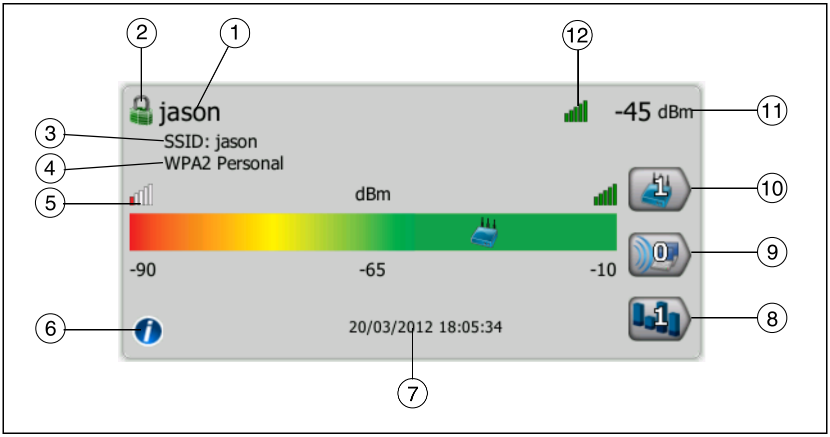


Figure 74. Wi-Fi Network Details

① The network's name (SSID) is shown here. If the name is very long, it may be truncated. The entire name is always shown on line ③.

② This icon indicates the network's security level. See page 205 for a description of how the icon's appearance changes based on the network's security level.

③ The full network name is shown here.

④ This is the network's security type.

⑤ The signal graph visually represents the network coverage provided by discovered access points. APs appear on the graph according to their signal strength. The scale is from -80 dBm to -10 dBm. The graph is updated real time.

⑥ Tap the information button to display quick tips about the screen.

⑦ This shows the date and time when the network was first discovered.

⑧ Tap the Channel Filter Button to show a summary of the channels the network is using. Tap the SHOW ALL SHOW ALL button to show all channels again.

⑨ Tap the Client Filter Button to show a summary of the clients discovered on the network. Tap the SHOW ALL SHOW ALL button to show all clients again.

⑩ Tap the AP Filter Button to show a summary of the APs configured for the network. Tap the SHOW ALL SHOW ALL button to show all APs again.

⑪ This is the network's signal level (in dBm). For networks with more than one AP, this is the strongest signal level as measured by the OneTouch analyzer.

⑫ The signal strength icon provides a quick visual indication of the network's signal strength as measured by the OneTouch analyzer. See page 205 for a list of the thresholds that change the icon's appearance.

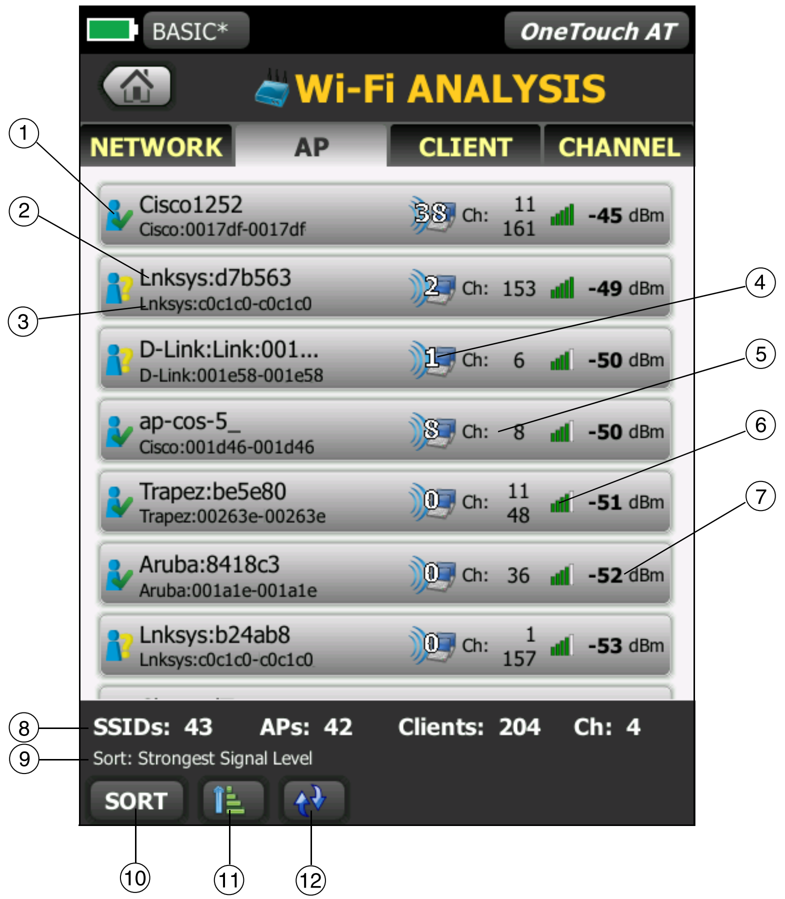
When a specific network, AP, or client is selected, details are shown and related tools are available. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen. See “Wi-Fi TOOLS” on page 234.

AP Analysis

The AP analysis tab provides:

- A sortable list of all discovered APs with summary information for each AP (See Figure 75) Note: In addition to discovery of 802.11agbn APs, OneTouch is able to discover APs that support the 802.11ac IEEE pre-standard using the 802.11n radio
- A graphical representation of AP details and trended measurements
- Filter buttons that provide deeper analysis of each AP's supported networks, associated clients, and channels used

Each AP's summary information is displayed on a button.



Cisco1252 — Cisco:0017df-0017df — 38 — Ch: 11 161 — -45 dBm

Lnksys:d7b563 — Lnksys:c0c1c0-c0c1c0 — 2 — Ch: 153 — -49 dBm

D-Link:Link:001... — D-Link:001e58-001e58 — 1 — Ch: 6 — -50 dBm

ap-cos-5_ — Cisco:001d46-001d46 — 8 — Ch: 8 — -50 dBm

Trapez:be5e80 — Trapez:00263e-00263e — 0 — Ch: 11 48 — -51 dBm

Aruba:8418c3 — Aruba:001a1e-001a1e — 0 — Ch: 36 — -52 dBm

Lnksys:b24ab8 — Lnksys:c0c1c0-c0c1c0 — 0 — Ch: 1 157 — -53 dBm

SSIDs: 43 APs: 42 Clients: 204 Ch: 4

Sort: Strongest Signal Level

Figure 75. AP Analysis Tab

① This icon indicates the AP's authorization status. Authorization classification provides a way to manage your list of access points so that you can identify unauthorized devices, neighbors' devices, etc.

- All new and unassigned APs are assigned a default status as described on page 235.
- You can change the Authorization Status for individual APs as described on page 236.

② The AP's Best Name has the following order of precedence: user-assigned name, advertised or discovered name, BSSID.

③ This shows the AP's MAC address. When you sort by "MAC Address" the numeric MAC address is shown. When you sort by "MAC Manufacturer," the first three octets (the manufacturer's Organizationally Unique Identifier) are replaced by the manufacturer's name.

④ This shows the number of clients associated to the AP.

⑤ This changes based on the sort key that you select after tapping the SORT button SORT. It can display the channels that the AP is using, or the 802.11 type. The 802.11 types in ascending order are: 802.11b, 802.11g, 802.11a, 802.11n, 802.11n-, 802.11n+, and 802.11ac.

⑥ The signal strength icon provides a quick visual indication of the AP's signal strength as measured by the OneTouch analyzer. See page 205 for a list of the thresholds that change the icon's appearance.

⑦ This changes based on the sort key that you select. This normally shows the AP's signal level (in dBm) as measured by the OneTouch analyzer. If you sort by utilization, this shows the percentage of the AP's bandwidth that is being used.

⑧ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of SSIDs (networks), APs (access points), and clients discovered. It also shows channel numbers as they are scanned.

⑨ The currently selected sort key is displayed above the **SORT** button.

⑩ The SORT button lets you sort the list of APs according to:

- Signal level
- AP name
- MAC manufacturer (displays the first three octets as the manufacturer’s name)
- MAC address (displays numeric MAC address)
- Channel number
- Utilization
- Retries (Retry Rate)
- Number of associated clients
- Authorization status
- 802.11 type

On AP buttons, the sort key (except authorization status and 802.11 type) appears bold or highlighted.

⑪ The Sort Order button determines whether the sorted results are shown in ascending or descending order.

⑫ The **REFRESH** button clears all Wi-Fi analysis results and restarts Wi-Fi analysis.

To Show AP Details

- Tap an AP to show its details.
- Tap the AP again to return to a summary view of APs.
- Tap a different AP to show its details. Only one AP’s details are shown at a time.

AP Details

The following section describes the AP button after it has been tapped to display details. This example shows an AP that is operating on two channels.

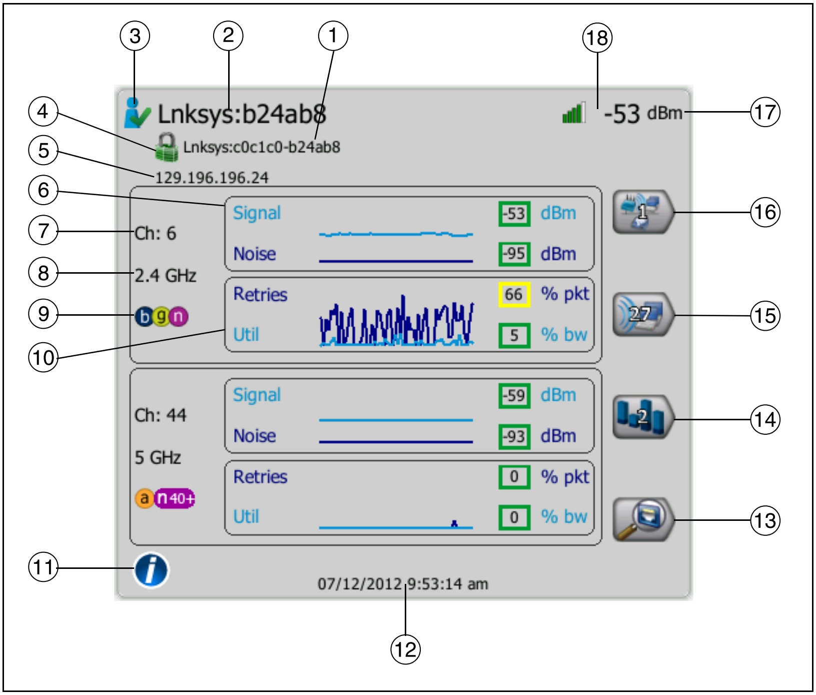


Figure 76. AP Details

① The AP's full Best Name is shown here. The AP's Best Name has the following order of precedence: user-assigned name, advertised or discovered name, BSSID.

② The AP's BSSID address is shown here.

③ This icon indicates the AP's Authorization Status. See page 212.

This icon indicates the AP's security level. See page 205 for a description of how the icon's appearance changes based on the security level. Multiple icons are shown when multiple security types are in use.

Note that the *network's* security type (e.g. WPA-Enterprise) is shown in the network detail screen. See page 208.

④ This icon indicates the AP's security level (i.e. the security method the client uses to connect to the AP/network). See page 205 for a description of how the icon's appearance changes based on the security level. Multiple icons are shown when multiple security types are in use

⑤ For APs that support Cisco extensions, an IP address is shown here. For an independent (fat) AP, this is the AP's IP address. For an interactive (thin) AP, this is the wireless LAN controller's IP address.

⑥ The Signal and Noise graph gives you an indication of the access point's coverage and the signal quality.

The upper line on this graph shows signal strength on a scale of 0 to -100 dBm.

- Signal values greater than -75 dBm are shown in a green box, indicating a strong signal.
- Signal values less than or equal to -75 dBm are shown in a yellow box, indicating a marginal or weak signal.

The lower line on the graph shows the noise level of the channels the AP is using.

- Noise values less than or equal to -80 dBm are shown in a green box, indicating a low noise level.
- Noise values greater than -80 dBm are shown in a yellow box, indicating a noisy environment.

⑦ The channels that the AP is using are displayed.

⑧ The bands that the AP is using are displayed.

⑨ The supported 802.11 media types that the AP is using are displayed.

⑩ The Retries and Utilization graph gives you an indication of network coverage, congestion, and capacity problems.

The retry rate is based on the percentage of total packets that have been re-sent. The scale is from 0% to 100%.

- Retry values less than or equal to 40% are shown in a green box.
- Retry values greater than 40% are shown in a yellow box. A high retry rate is an indicator of issues such as a noisy RF environment, associated clients located at the edge of AP range, or high traffic levels.

The utilization percentage value is based on the actual traffic level in relation to total available bandwidth. The scale is 0% to 100%.

- Utilization values of 25% or less are shown in a green box.
- Values greater than 25% are shown in a yellow box. High utilization indicates that an AP could be overloaded. Additional APs or load balancing may be necessary to mitigate the problem.

⑪ Tap the information button to display quick tips about the screen.

⑫ This is the date and time when the AP was first discovered.

⑬ Tap the Wired Discovery button 🔍, if shown, to go to the current device's wired details screen. To return to the Wi-Fi details screen, tap the Wi-Fi Discovery button 🔍 shown on the wired device details screen. The Discovery buttons will only be visible when a device has been discovered during Wired and Wi-Fi Analysis.

⑭ Tap the Channel Filter Button to show a summary of the channels the AP is using. Tap the SHOW ALL SHOW ALL button to show all channels again.

⑮ Tap the Client Filter Button to show a summary of the clients associated with the AP. Tap the SHOW ALL SHOW ALL button to show all clients again.

⑯ Tap the Network Filter Button to show a summary of the networks that are using the access point. Tap the SHOW ALL SHOW ALL button to show all networks again.

⑰ This changes based on the selected sort key. The AP’s signal level (in dBm) as measured by the OneTouch analyzer is displayed, or the AP’s utilization is displayed.

⑱ The signal strength icon provides a quick visual indication of the AP’s signal strength as measured by the OneTouch analyzer. See page 205 for a list of the thresholds that change the icon’s appearance.

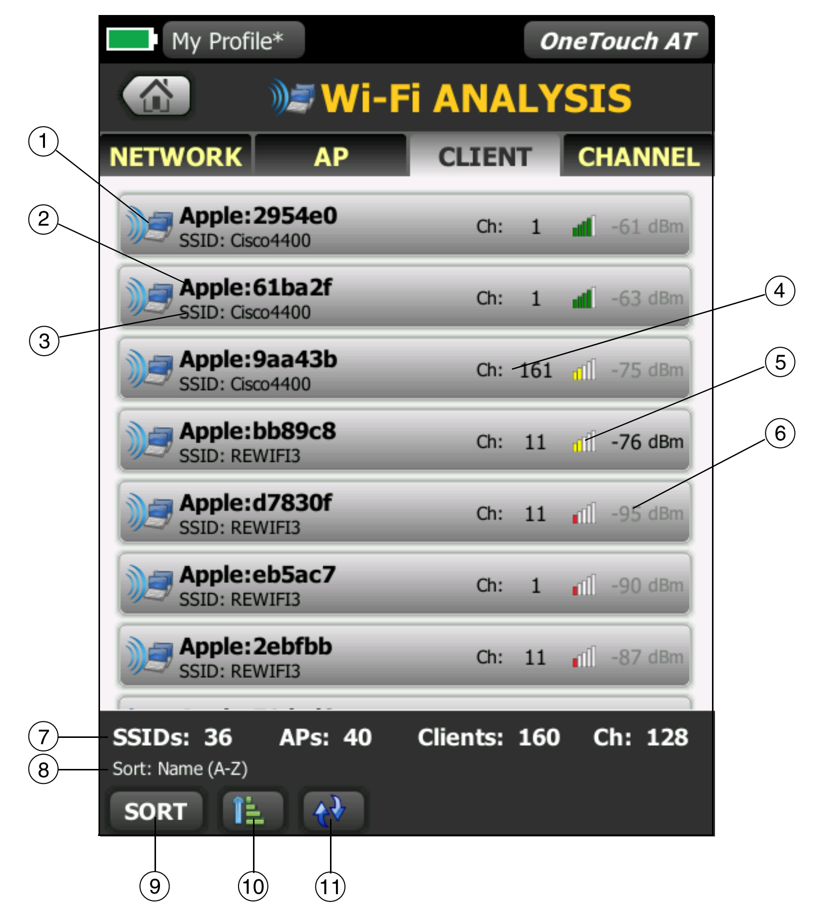
When a specific network, AP, or client is selected, details are shown and related tools are available. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen. See “Wi-Fi TOOLS” on page 234.

Client Analysis

The CLIENT analysis tab provides:

- A sortable list of all discovered clients with summary information for each network (See Figure 77)
- A graphical representation of client details and trended measurements
- Filter buttons that provide deeper analysis of each client’s channel usage, access point association, and its network

Each client is displayed with summary information on a button.



Apple:2954e0 SSID: Cisco4400 Ch: 1 -61 dBm

Apple:61ba2f SSID: Cisco4400 Ch: 1 -63 dBm

Apple:9aa43b SSID: Cisco4400 Ch: 161 -75 dBm

Apple:bb89c8 SSID: REWIFI3 Ch: 11 -76 dBm

Apple:d7830f SSID: REWIFI3 Ch: 11 -95 dBm

Apple:eb5ac7 SSID: REWIFI3 Ch: 1 -90 dBm

Apple:2ebfbb SSID: REWIFI3 Ch: 11 -87 dBm

SSIDs: 36 APs: 40 Clients: 160 Ch: 128

Sort: Name (A-Z)

Figure 77. Client Analysis Tab

① The Wi-Fi client icon indicates an associated client or a probing client .

② This is the client’s name.

③ This changes based on the sort key that you select. It normally shows the Network Name. But if you sort the client list by AP, the AP Best Name is shown. If you sort the list by MAC, the client's MAC address is shown.

④ This is the channel the client is using.

⑤ The signal strength icon provides a quick visual indication of the client's signal strength as measured by the OneTouch analyzer. See page 205 for a list of the thresholds that change the icon's appearance.

⑥ This changes based on the selected sort key. This shows the client's signal level (in dBm) as measured by the OneTouch analyzer, or the percentage of the AP's bandwidth that the client is using (utilization). If the client has not been heard recently, the value is shown in gray text instead of black.

⑦ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of SSIDs (networks), APs (access points), and clients discovered. It also shows channel numbers as they are scanned.

⑧ The currently selected sort key is displayed above the SORT button.

⑨ The SORT button lets you sort the list of clients according to:

- Signal level
- Client name
- MAC manufacturer (displays the first three octets as the manufacturer's name)
- MAC address (displays numeric MAC address)
- Channel number
- Utilization (the percentage of the AP's bandwidth that the client is using)
- Retries (Retry Rate)
- SSID
- Access point

- Association (associated or probing state)

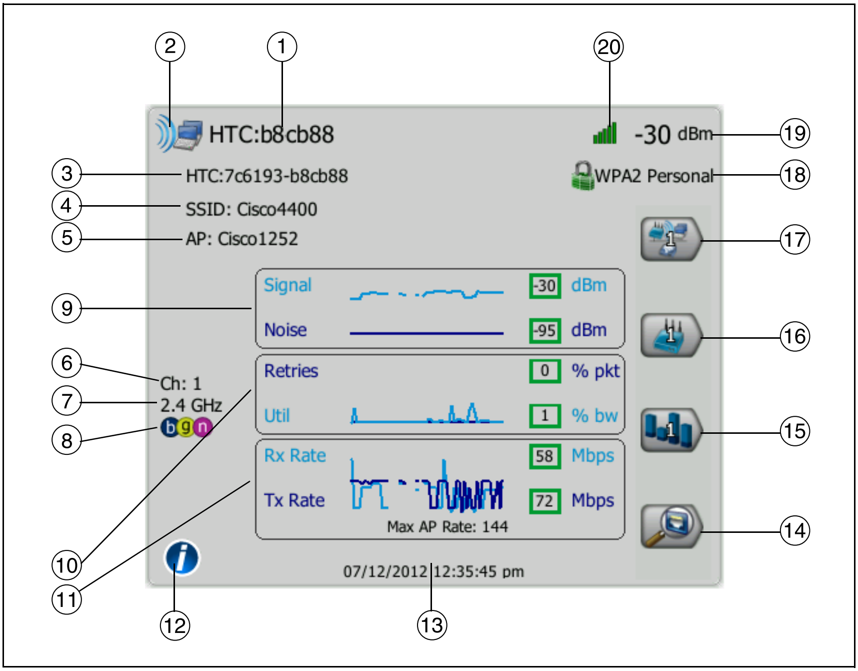
On client buttons, the sort key (except associated/probing) appears in bold text.

⑩ The Sort Order button determines whether the sorted results are shown in ascending or descending order.

⑪ The **REFRESH** button clears all Wi-Fi analysis results and restarts Wi-Fi analysis.

To Show Client Details

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



HTC:b8cb88 -30 dBm

HTC:7c6193-b8cb88 WPA2 Personal

SSID: Cisco4400

AP: Cisco1252

Signal	-30	dBm
Noise	-95	dBm
Retries	0	% pkt
Util	1	% bw
Rx Rate	58	Mbps
Tx Rate	72	Mbps

Max AP Rate: 144

Ch: 1
2.4 GHz

07/12/2012 12:35:45 pm

Figure 78. Associated Client Details

① Client’s manufacturer’s MAC address

② Wi-Fi client icon indicates an associated client or a probing client

③ Client’s MAC address, including manufacturer and raw MAC

④ Network to which the client is connected

⑤ AP to which the client associated

⑥ Channel the client is using

⑦ Band the client is using

⑧ Access point’s supported 802.11 media types

⑨ The Signal and Noise graph gives you an indication of the client’s signal strength as measured by the OneTouch analyzer.

The upper line on this graph shows signal strength on a scale of 0 to -100 dBm.

- Signal values greater than -75 dBm are shown in a green box, indicating a strong signal.
- Signal values less than or equal to -75 dBm are shown in a yellow box, indicating a marginal or weak signal. The client may be too far away from an access point for a reliable connection.

The lower line on the graph shows noise.

- Noise values less than or equal to -80 dBm are shown in a green box, indicating a low noise level.
- Noise values greater than -80 dBm are shown in a yellow box, indicating a noisy environment that can impact the quality of a client’s connection.

⑩ The Retries and Utilization graph gives you an indication of network coverage, congestion, and capacity problems.

The retry rate is based on the percentage of total packets that have been re-sent. The scale is from 0% to 100%.

- Values less than or equal to 40% are shown in a green box.
- Values greater than 40% are shown in a yellow box. A high retry rate is an indicator of problems such as a noisy RF environment, the client may be located at the edge of an AP’s range, or high traffic levels.

The utilization percentage value is based on a client’s actual traffic level in relation to total available bandwidth. The scale is 0% to 100%.

- Utilization values of 25% or less are shown in a green box.

- Values greater than 25% are shown in a yellow box. High utilization may indicate problems such as excessive use of bandwidth by an individual client, a client at the edge of an AP's range (causing excessive retries and therefore increased utilization), or a large amount of data being transmitted at a low data rate.

⑪ The Frame Rate graph shows the receive (Rx) and transmit (Tx) rates. The scale for this graph is based on the AP's maximum rate, which is shown at the bottom of the graph. Low data rates impact end users' response time. Excessive utilization, interference, and weak coverage can reduce performance.

- Rx and Tx values that are greater than 30% of an access point's maximum supported frame rate are shown in a green box.
- Rx and Tx values that are less than or equal to 30% of an access point's maximum supported frame rate are shown in a yellow box, indicating a slow actual data rate.

⑫ Tap the information button to display quick tips about the screen.

⑬ This is the time when the client was first discovered.

⑭ Tap the Wired Discovery button 🔍, if shown, to go to the current device's wired details screen. To return to the Wi-Fi details screen, tap the Wi-Fi Discovery button 🔍 shown on the wired device details screen. The Discovery buttons will only be visible when a device has been discovered during Wired and Wi-Fi Analysis.

⑮ Tap the Channel Filter Button to show a summary of the channel the client is using. Tap the SHOW ALL SHOW ALL button to show all channels again.

⑯ Tap the AP Filter Button to show a summary of the AP the client is using. Tap the SHOW ALL SHOW ALL button to show all APs again.

⑰ Tap the Network Filter Button to show a summary of the client's network. Tap the SHOW ALL SHOW ALL button to show all networks again.

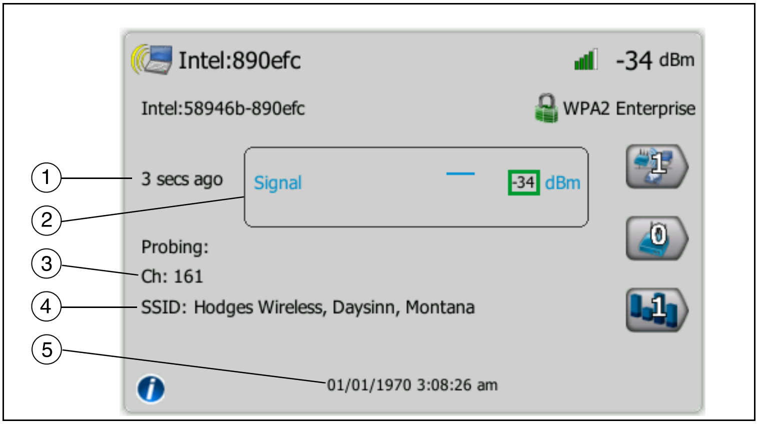
⑱ This icon indicates the AP's security level (i.e. the security method the client used to connect to the AP/network). See page 205 for a description of how the icon's appearance changes based on the security level. Multiple icons are shown when multiple security types are in use

⑲ This changes based on the selected sort key. This shows the client's signal level (in dBm) as measured by the OneTouch analyzer, or the client's utilization.

⑳ The signal strength icon provides a quick visual indication of the client's signal strength as measured by the OneTouch analyzer. See page 205 for a list of the thresholds that change the icon's appearance.

Probing Client Details

Details for clients that are probing appear as shown below.



Intel:890efc -34 dBm

Intel:58946b-890efc WPA2 Enterprise

3 secs ago

Signal -34 dBm

Probing:
Ch: 161
SSID: Hodges Wireless, Daysinn, Montana

01/01/1970 3:08:26 am

Figure 79. Probing Client Detail

① Time since the client last probed

② Client's signal level as measured by the OneTouch analyzer

③ Channels on which the client is probing

④ SSIDs the client is probing for

⑤ Time when the client was first discovered

For an explanation of other client details, see Figure 78.

When a specific network, AP, or client is selected, details are shown and related tools are available. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen. See “Wi-Fi TOOLS” on page 234.

Channel Analysis

The CHANNEL analysis tab provides:

- An overview of 802.11 and non-802.11 utilization of all channels, along with the number of APs discovered on each channel
- A sortable list of active 802.11 channels with summary information for each channel (See Figure 80)
- A graphical representation of channel utilization and important details of activity on the channel
- Filter buttons for analysis of an individual channel’s usage by specific networks, access points, and associated clients

The top button provides a channel overview. Channel summary buttons appear below for each channel.

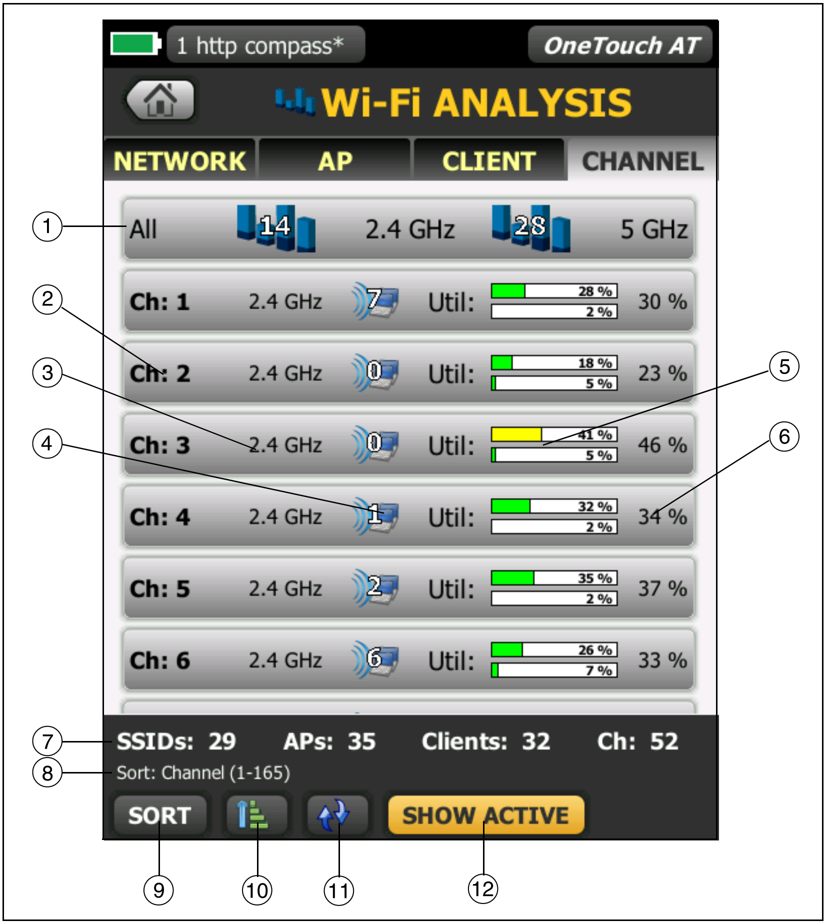


Figure 80. Channel Analysis Tab

① Tap ①, the Channel Overview button for a graphical overview of channels, access points, 802.11 traffic, and non-802.11 traffic.

The numbers on the blue bars of the Channel Overview button show the number of channels on each band, or the number of active channels on each band. See ⑫, the SHOW ACTIVE/SHOW ALL button.

② Channel number

③ Channel's band

④ This is the number of access points that are using the channel.

⑤ The channel utilization graph has two bars. The upper bar shows 802.11 utilization of the channel. The bar is normally green, but it turns yellow if 802.11 utilization exceeds 40%.

The lower bar shows non-802.11 utilization of the channel. The bar is normally green, but it turns yellow if non-802.11 utilization exceeds 20%.

⑥ This is the total percentage of 802.11 and non-802.11channel utilization.

⑦ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of SSIDs (networks), APs (access points), and clients discovered. It also shows channel numbers as they are scanned.

⑧ The currently selected sort key is displayed above the SORT button.

⑨ The SORT button lets you sort the list of channels according to:

- Channel number
- Band
- Total 802.11 plus non-802.11 utilization
- 802.11 utilization
- Non-802.11 utilization
- Signal level of the strongest AP on the channel
- Number of APs
- Number of associated clients

On channel buttons, the sort key (except 802.11 utilization and Non-802.11 utilization) appears in bold text.

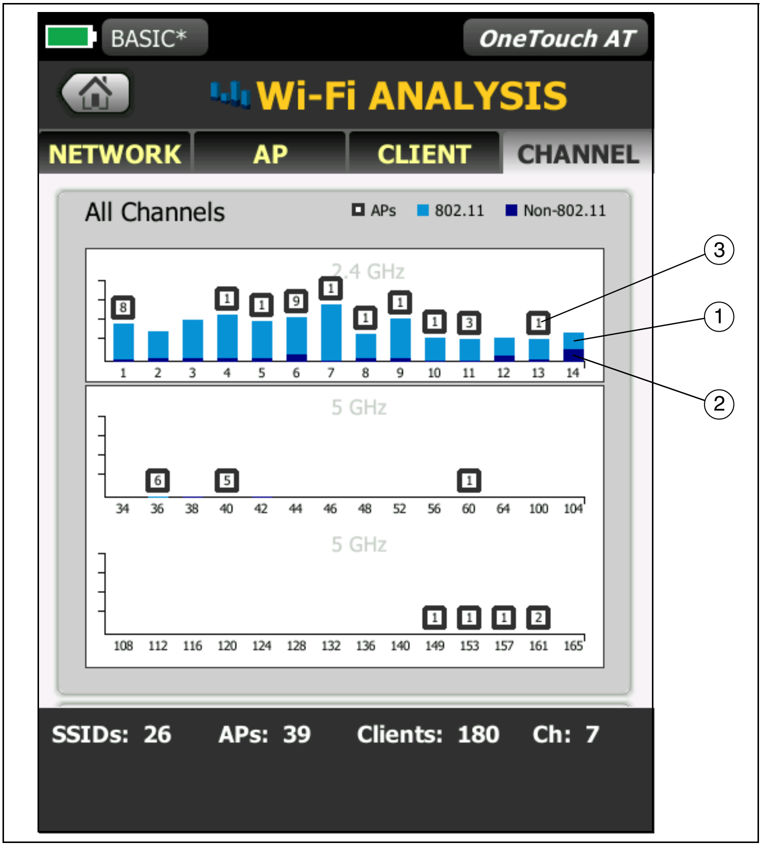
⑩ The Sort Order button determines whether the sorted results are shown in ascending or descending order.

⑪ The **REFRESH** button clears all Wi-Fi analysis results and restarts Wi-Fi analysis.

⑫ The SHOW ACTIVE/SHOW ALL button toggles the list between showing all channels or only channels on which an AP has been discovered.

Channel Overview

Tap the Channel Overview button for a graphical summary of access points, 802.11 traffic, and non-802.11 traffic on all channels.



SSIDs: 26 APs: 39 Clients: 180 Ch: 7

Figure 81. Channel Overview

① 802.11 utilization is shown in blue.

② Non-802.11 usage is shown in dark blue.

③ The number of APs discovered on each channel is shown above the channel. A blue 802.11 bar without a number above it indicates interference from an adjacent channel.

To Show Channel Details

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

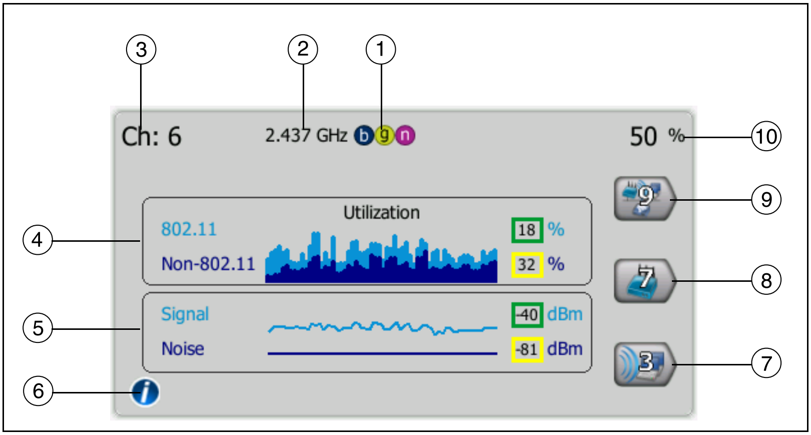


Figure 82. Wi-Fi Channel Details

① 802.11 media types supported in the respective band

② Channel frequency

③ Channel number

④ The utilization graph trends both 802.11 and non-802.11 utilization of the channel.

The upper portion of the stacked graph shows 802.11 utilization in light blue as a percentage of total bandwidth. The graph's scale is 0% to 100%.

- Utilization values less than 40% are shown in a green box.
- Utilization values greater than or equal to 40% are shown in a yellow box, indicating potentially excessive utilization.

The lower portion of the stacked graph shows non-802.11 utilization in dark blue as a percentage of total bandwidth.

- Non-802.11 utilization values less than or equal to 20% are shown in a green box.
- Non-802.11 utilization values greater than 20% are shown in a yellow box, indicating a noisy environment.

⑤ The Signal and Noise graph shows the power level of 802.11 signals and of noise.

The upper (light blue) line on this graph shows signal strength on a scale of 0 to -100 dBm. The displayed value is for the strongest received signal from an AP that is utilizing the channel.

- Signal values greater than -75 dBm are shown in a green box, indicating a strong signal.
- Signal values less than or equal to -75 dBm are shown in a yellow box, indicating a marginal or weak signal.

The lower (dark blue) line on the graph shows noise.

- Noise values less than or equal to -80 dBm are shown in a green box, indicating a low noise level.
- Noise values greater than -80 dBm are shown in a yellow box, indicating a noisy environment.

⑥ Tap the information button to display quick tips about the screen, such as the thresholds used to determine the color of the box in which a signal level is displayed.

⑦ Tap the Client Filter Button to show a summary of the clients discovered on the channel. Tap the SHOW ALL SHOW ALL button to show all clients again.

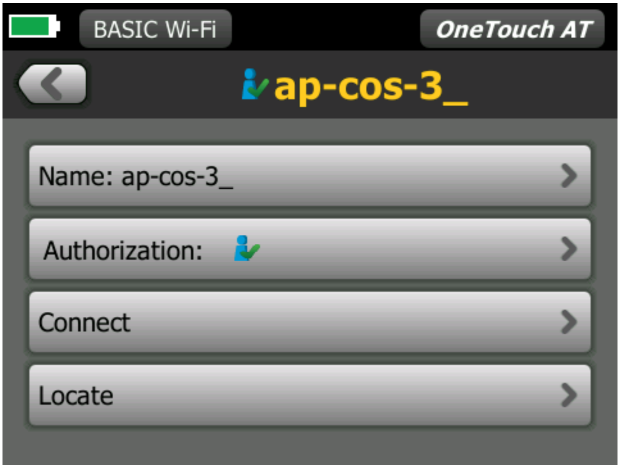
⑧ Tap the AP Filter Button to show a summary of the APs active on the channel. Tap the SHOW ALL SHOW ALL button to show all clients again.

⑨ Tap the Network Filter Button to show a summary of the networks utilizing the channel. Tap the SHOW ALL SHOW ALL button to show all clients again.

⑩ Total 802.11 and non-802.11 utilization of the channel

Wi-Fi TOOLS

When you tap a network, AP, or client button to show its details, the Wi-Fi **TOOLS** button TOOLS appears at the lower-right corner of the screen. Tap the TOOLS button to use a Wi-Fi tool.



BASIC Wi-Fi

OneTouch AT

ap-cos-3_

Name: ap-cos-3_

Authorization:

Connect

Locate

Figure 83. Wi-Fi AP Tools Screen

The following table shows the Wi-Fi tools you can use on networks, APs, and clients.

Wi-Fi Detail Button	Wi-Fi Tool			
	Name	Authori-zation	Connect	Locate
Network			•	
AP	•	•	•	•
Client				•

The Wi-Fi tools button is not available for use on **[Hidden]** networks.

Name Tool

Tap the **Name** button to assign a custom name to an AP for ease of identification. Your custom name will be displayed for the AP throughout the OneTouch analyzer's screens and in reports.

Authorization Status Tool and Default Setting

The authorization status tool allows you to classify access points on the network. Once you have assigned an authorization status to an AP, it is marked with an authorization status icon. When you display the AP list, you can quickly and easily identify new APs on the network, including unauthorized APs that may present a security risk.

An access point's authorization status can be set in one of two ways:

- When an AP is discovered, its authorization status is automatically set to the default status. The default status is configured via the HOME screen's TOOLS menu.
- You can change an AP's authorization status via the Wi-Fi Analysis TOOLS menu.

After configuring and saving an AP authorization list, you can export it and import it to another OneTouch analyzer, for use with a configured profile.

Set the Default AP Authorization Status

Each AP's authorization status is indicated by an icon. As each new AP is discovered, the OneTouch analyzer assigns it a default status of either Unknown ? or Authorized ✓. You can set the default status as follows:

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

2 Tap the **Wi-Fi** button.

3 Tap either the Authorized ✓ or the Unknown ? authorization default button.

This sets the status for all unassigned APs, and for new APs as they are discovered. If you have already assigned an authorization status to an AP, it is not affected by this change.

Change an AP’s Authorization Status

To set the Authorization Status of an AP:

1 Tap the Wi-Fi ANALYSIS AP tab.

2 Tap the button of the AP you want to assign an authorization status.

3 Tap the Wi-Fi **TOOLS** button TOOLS, which is located at the lower-right corner of the screen.

4 Tap the **Authorization** button.

5 Tap the authorization status you want to assign to the AP.

Authorization Status choices are:

? or ✓ Default, see “Set the Default AP Authorization Status” on page 235.

✗ Unauthorized - For APs that are not authorized on the network. These APs may present a security risk.

👥 Neighbor - For APs that are owned and controlled by neighboring organizations.

⚑ Flagged - To give visibility to a certain AP. This may be a temporary AP, a guest’s AP, etc.

? Unknown - For APs that have not yet been otherwise classified.

✓ Authorized - An AP that is approved for use on the network.

6 To store your Authorization Status settings, save the Authorization Profile. See “AP Authorization” on page 270.

Save an Authorization File

When you change the authorization status of one or more APs, the Profile name (which is located at the top of the display) is marked with an asterisk, indicating that there are unsaved changes in the ACL (Authorization Control List) that is used by the Profile.

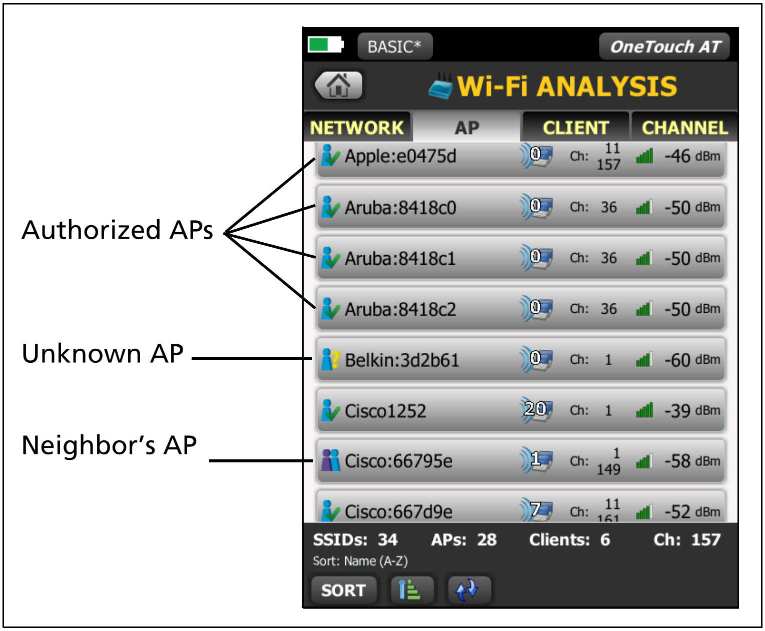
After configuring an AP authorization list, you can export it and import it to another OneTouch analyzer, for use with a configured profile.

To save an authorization file:

1. Tap the **TOOLS** button on the HOME screen.
2. Under the **File Tools** section, tap **AP Authorization**.
3. From this screen, you can save and load authorization profiles.
4. To import, export, rename, or delete authorization profiles, tap the **MANAGE** button.

Identify New APs on the Network

Once you have assigned an Authorization Status other than unknown to all discovered APs, and you have set the Authorization Default to Unknown, you can easily identify new APs as they appear on your network. New APs will have the Unknown icon.



Apple:e0475d	0	Ch: 11 157	-46 dBm
Aruba:8418c0	0	Ch: 36	-50 dBm
Aruba:8418c1	0	Ch: 36	-50 dBm
Aruba:8418c2	0	Ch: 36	-50 dBm
Belkin:3d2b61	0	Ch: 1	-60 dBm
Cisco1252	20	Ch: 1	-39 dBm
Cisco:66795e	1	Ch: 1 149	-58 dBm
Cisco:667d9e	7	Ch: 11 161	-52 dBm

SSIDs: 34 APs: 28 Clients: 6 Ch: 157
Sort: Name (A-Z)

Figure 84. AP Authorization Status

Connect Tool

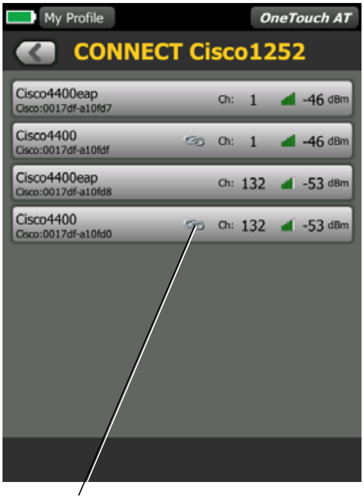
The Wi-Fi Connect tool lets you verify the ability to connect to networks and access points. The RESULTS tab shows a summary of the connection. The LOG tab provides details about the connection process, which can be useful when troubleshooting connection problems.

1 Tap a network button on the NETWORK tab, or tap an AP button on the AP tab. Network or AP details will be displayed.

2 Tap the Wi-Fi **TOOLS** button TOOLS to access the Connect tool.

3 If multiple SSIDs are available on AP, or if multiple channels are available for an SSID, a screen will appear in which you can make a selection.

Multiple SSIDs on an AP



CONNECT Cisco1252

Cisco4400eap Cisco:0017df-a10fd7		Ch: 1	-46 dBm
Cisco4400 Cisco:0017df-a10fdf	🔗	Ch: 1	-46 dBm
Cisco4400eap Cisco:0017df-a10fd8		Ch: 132	-53 dBm
Cisco4400 Cisco:0017df-a10fd0	🔗	Ch: 132	-53 dBm

This icon indicates that the current profile contains security credentials for the network

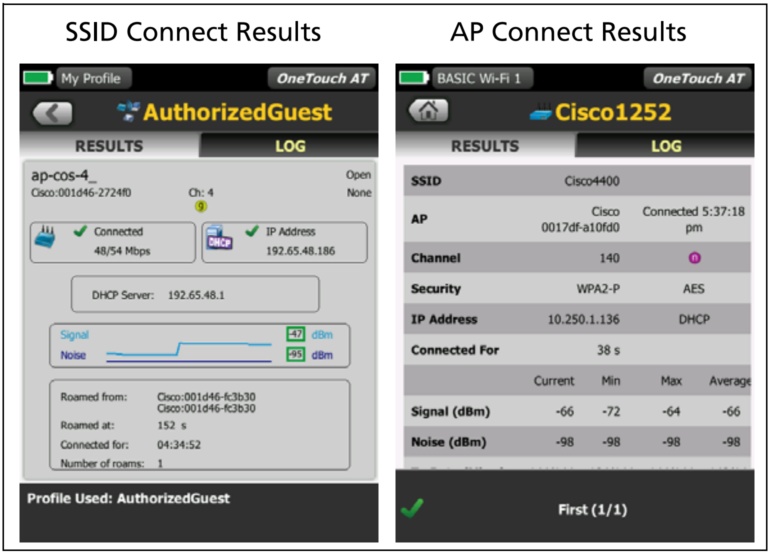
Figure 85. Multiple Choices for Connect tool.

4 Tap the **Connect** button to connect a network. Or, if connecting to an AP, tap the **Connect** button and select a network to complete the connection to the AP. The OneTouch analyzer connects and displays the RESULTS tab, or if it cannot connect, it displays an error message.

Note

The Connect test is not supported for [Hidden] SSIDs that have not been resolved. If [Hidden] is selected the Connect tool will not be available.

The Connect test is supported for 802.11ac capable APs. The connect rates will be at 802.11n rates or lower.



SSID Connect Results

ap-cos-4_ Open
Cisco:001d46-2724f0 Ch: 4 None

✓ Connected
48/54 Mbps

✓ IP Address
192.65.48.186

DHCP Server: 192.65.48.1

Signal -47 dBm
Noise -95 dBm

Roamed from: Cisco:001d46-fc3b30
Cisco:001d46-fc3b30
Roamed at: 152 s
Connected for: 04:34:52
Number of roams: 1

Profile Used: AuthorizedGuest

AP Connect Results

SSID		Cisco4400		
AP		Cisco 0017df-a10fd0	Connected 5:37:18 pm	
Channel		140	n	
Security		WPA2-P	AES	
IP Address		10.250.1.136	DHCP	
Connected For		38 s		
	Current	Min	Max	Average
Signal (dBm)	-66	-72	-64	-66
Noise (dBm)	-98	-98	-98	-98

✓ First (1/1)

Figure 86. Network and AP Connect Results

The network and AP connect RESULTS tabs show the network and AP, actual connection rate, the DHCP server’s IP address, etc.

The signal and noise graph is explained on page 215.

The SSID RESULTS tab includes roaming statistics for the current connection.

Roamed from: This is the prior AP to which the OneTouch analyzer was associated.

Roamed at: This is the time when the OneTouch analyzer associated with the current AP.

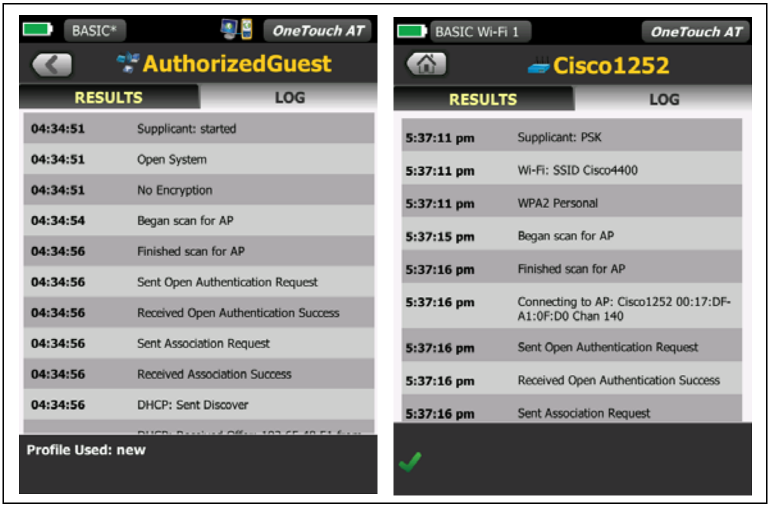
Connected for: This is the elapsed time that the OneTouch analyzer has been connected to the current AP.

Number of roams: This is the number of times the OneTouch analyzer has roamed to a new AP.

- If you connect to an SSID, you can roam among the APs that support the connected SSID.
- If you connect to a specific AP, no roaming will occur. If you move out of the AP's range, the connection will drop.

Profile Used: The profile in use is shown at the bottom of the screen.

5 Tap the LOG tab to show a detailed listing of each step of the connection. This is useful when troubleshooting connection problems.



```
04:34:51    Supplicant: started
04:34:51    Open System
04:34:51    No Encryption
04:34:54    Began scan for AP
04:34:56    Finished scan for AP
04:34:56    Sent Open Authentication Request
04:34:56    Received Open Authentication Success
04:34:56    Sent Association Request
04:34:56    Received Association Success
04:34:56    DHCP: Sent Discover
```

Profile Used: new

```
5:37:11 pm    Supplicant: PSK
5:37:11 pm    Wi-Fi: SSID Cisco4400
5:37:11 pm    WPA2 Personal
5:37:15 pm    Began scan for AP
5:37:16 pm    Finished scan for AP
5:37:16 pm    Connecting to AP: Cisco1252 00:17:DF-
              A1:0F:D0 Chan 140
5:37:16 pm    Sent Open Authentication Request
5:37:16 pm    Received Open Authentication Success
5:37:16 pm    Sent Association Request
```

Figure 87. Network and AP Connection Logs

See also: "Wi-Fi Network Connect Test" on page 89 and "Roaming Results Navigation Controls" on page 93.

Locate Tool

You can use the Locate function to find APs and clients.

You should use the directional antenna when performing a Locate task. See **www.flukenetworks.com/onetouch** for a list of available accessories.

1 Remove the stand from the back of the analyzer.

2 Snap the antenna holder onto the back of the analyzer. The antenna holder is included with the directional antenna.

3 Slide the directional antenna into the holder.

4 Connect the antenna to the External Antenna Connector (see page 27). The OneTouch analyzer automatically detects the presence of the antenna, and the external antenna icon is displayed on the Locate RESULTS screen.

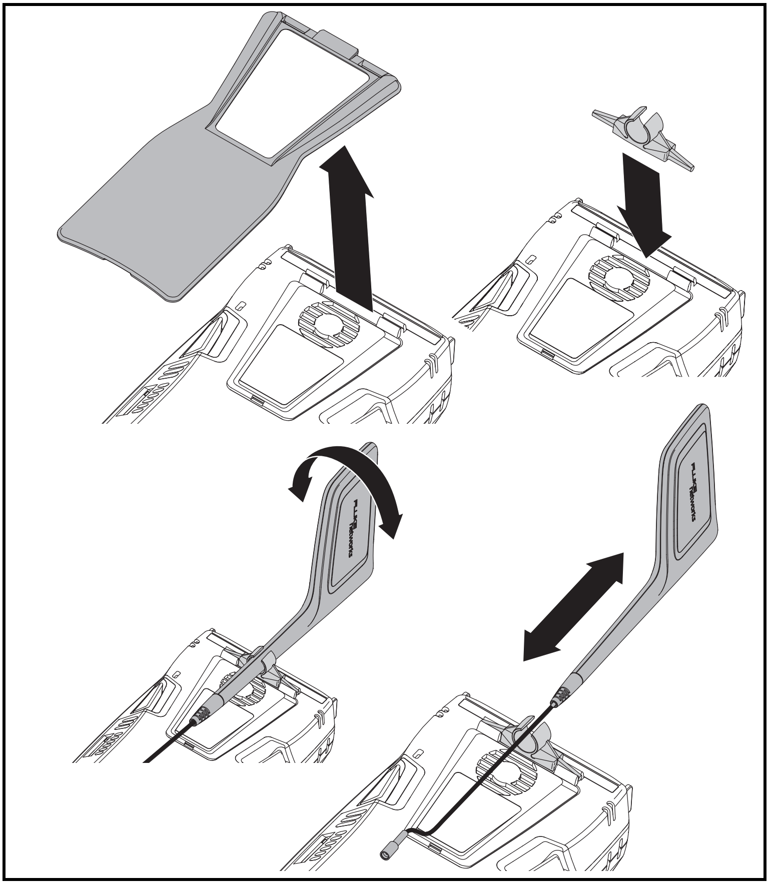


Figure 88. Directional Antenna Holder

5 Tap the **Locate** button.

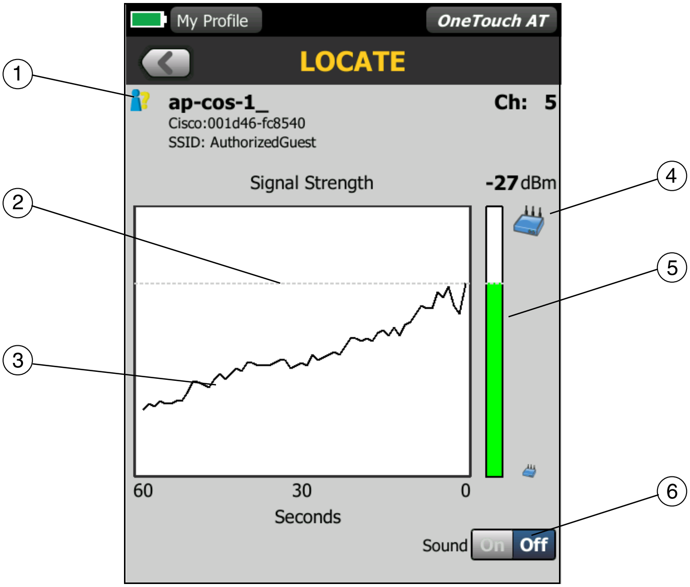
⚠ **CAUTION**

> **To avoid an accident, watch where you are going when you are in motion. Observe the signal strength graph only when you are stationary.**

6 The signal strength will generally increase when you move closer to the AP or client, and decrease when you move farther away. You can switch off **Sound** to silently locate a client or AP.

Note

> *The external antenna is only activated when in Locate mode. Locate is a receive-only mode; the OneTouch analyzer does not transmit.*



My Profile

OneTouch AT

LOCATE

ap-cos-1_ Ch: 5

Cisco:001d46-fc8540

SSID: AuthorizedGuest

Figure 89. Locate Screen

① The Authorization Status icon is described on page 236.

② The high water mark shows the strongest signal received since the test began.

③ One minute of data is displayed

④ This icon indicates whether an AP or a client is being located.

⑤ The Signal Strength Bar grows or shrinks based on signal strength. It changes color according to the signal strength thresholds shown on page 205. If the signal is lost, the bar turns gray.

⑥ You can switch off sound to silently locate APs or clients.

Chapter 8: Tools

Tap the TOOLS icon on the HOME screen to access the TOOLS screen.

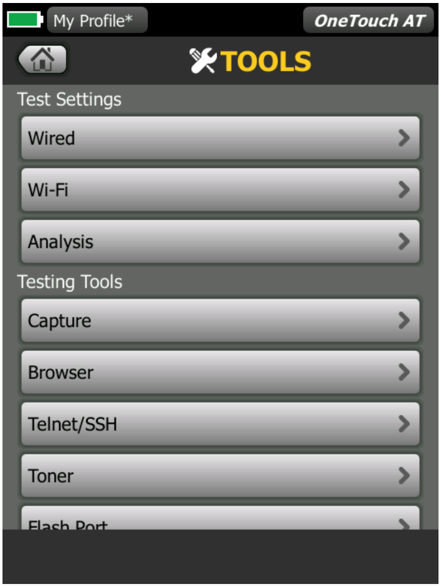


Figure 90. Tools Screen

Test Settings

The following test settings can be configured via the TOOLS screen. Refer to the following pages.

“Wired” on page 248

“Wi-Fi” on page 252

“SNMP” on page 174

“Slow Discovery” on page 174

Also included in this section:

"View or Change the analyzer's MAC Addresses" on page 250

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.

PoE (Power over Ethernet)

See "PoE Test" on page 79.

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. 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 OneTouch 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. See Chapter 10: "Managing Files," beginning on page 303.

Address

The IPv6 option on the ADDRESS screen determines whether the IPv6 columns are shown 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 both wired and Wi-Fi interfaces.

IPv4 - The analyzer's wired IPv4 address is always enabled. Tap the IPv4 address button to configure the OneTouch 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 OneTouch 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.

Enable IPv6 on the Wi-Fi Interface

To enable IPv6 address capability on the Wi-Fi interface:

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

2 In the Test Settings section, tap the **Wi-Fi** 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 analyzer for remote viewing or remote file access you will need to know the IP address of the management port.

Ethernet Port A MAC Address

To view or change the Network Under Test port MAC address:

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 MAC Address

To view or change the Wi-Fi Adapter MAC address:

1. On the HOME screen, tap **TOOLS**.
2. Tap the **Wi-Fi** button.
3. Set **Enable Wi-Fi** to **On**.
4. Tap the **Address** button.
5. Tap the **User MAC On** button.
6. Tap the **User MAC Address** button and enter the desired address.

VLAN

To make the OneTouch 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 OneTouch 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**.

Wi-Fi

See “Establish a Wi-Fi Connection” on page 51.

Analysis

See “SNMP” on page 174, and “Slow Discovery” on page 174.

Testing Tools

The following testing tools are available on the TOOLS screen.

Capture

See Chapter 9, "Packet Capture."

VoIP Analysis

The VoIP Analysis tool lets you connect inline between a VoIP phone and the network, for real-time troubleshooting and analysis of VoIP phone issues. The VoIP analysis tool reveals issues related to PoE, DHCP, TFTP, SIP, and SCCP. The tool provides visibility into unencrypted SIP (Session Initiation Protocol) and SCCP (Skinny Call Control Protocol) traffic. You can use VoIP Analysis to debug VoIP phone problems and quantify the quality of a VoIP call.

- Quickly diagnose IP phone boot-up and call control problems
- Measure key VoIP metrics, including frames sent, dropped frames, and Mean Opinion Scores (MOS)

Historically, MOS was a call quality score based on listeners’ subjective assessment of call quality. The ITU-T PESQ P.862 standard was created to provide an objective method for predicting the quality of services such as VoIP. It includes a calculation that quantifies an IP network’s performance, and thereby predicts call quality.

R-Factor is a call quality score based on parameters such as latency, jitter, and packet loss.

To Configure VoIP Analysis

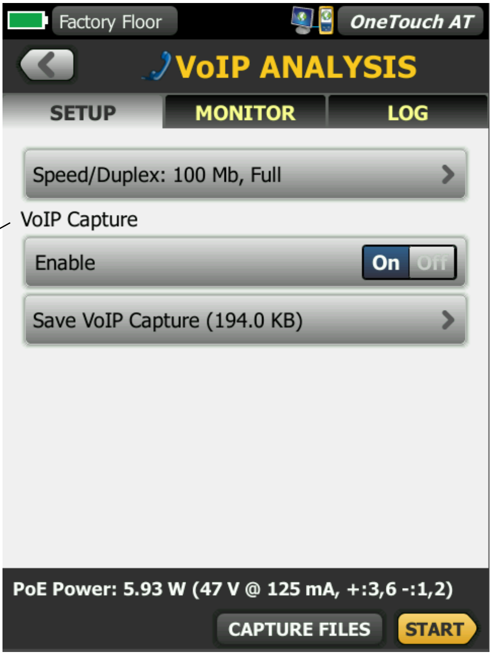
Connect the OneTouch AT analyzer inline between the VoIP phone and the switch as described below.

1 Connect the OneTouch AT analyzer's Port A to the switch.

2 Connect the OneTouch AT analyzer's Port B to the VoIP phone.

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

4 In the **Testing Tools** section, tap the **VoIP Analysis** button. The VoIP ANALYSIS screen is displayed. Ensure that the SETUP tab is selected.



Speed/Duplex: 100 Mb, Full

VoIP Capture

Enable: On

Save VoIP Capture (194.0 KB)

PoE Power: 5.93 W (47 V @ 125 mA, +:3,6 -:1,2)

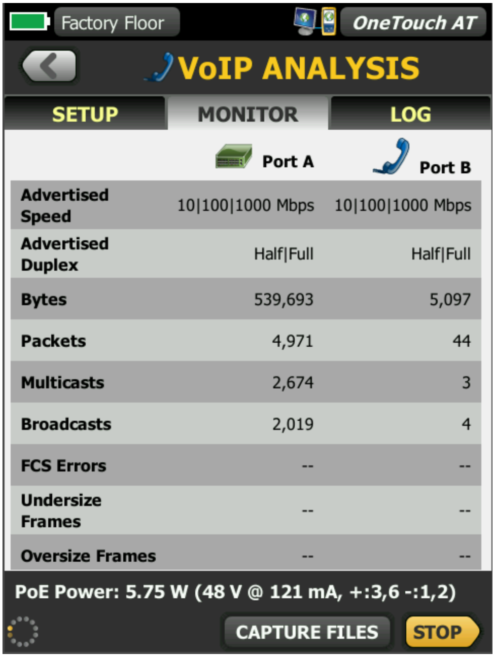
Optional feature

Figure 91. The VoIP Analysis Configuration Screen, SETUP Tab

5 Tap the **Speed/Duplex** button. Select the phone's link speed and the duplex mode.

6 Optional: Enable VoIP Analysis packet capture. See page 257.

7 Tap the **START** button START. The VoIP analysis results screen is displayed, with the MONITOR tab selected.



	Port A	Port B
Advertised Speed	10|100|1000 Mbps	10|100|1000 Mbps
Advertised Duplex	Half|Full	Half|Full
Bytes	539,693	5,097
Packets	4,971	44
Multicasts	2,674	3
Broadcasts	2,019	4
FCS Errors	--	--
Undersize Frames	--	--
Oversize Frames	--	--

PoE Power: 5.75 W (48 V @ 121 mA, +:3,6 -:1,2)

Figure 92. The VoIP Analysis Results Screen, MONITOR Tab

Note

If the test is started when the phone and network connections are reversed, a warning will be displayed and the test will terminate.

A progress spinner in the lower-left corner indicates that the test is in progress.

The phone powers-up

8 Observe the PoE Power status line at the bottom of the MONITOR screen. Compare the measured power with the power requirement of the VoIP phone to determine whether enough power is available to run the phone.

If PoE is not present on the link, the phone will fail to power-up and the status message “No link on Port B” will be displayed.

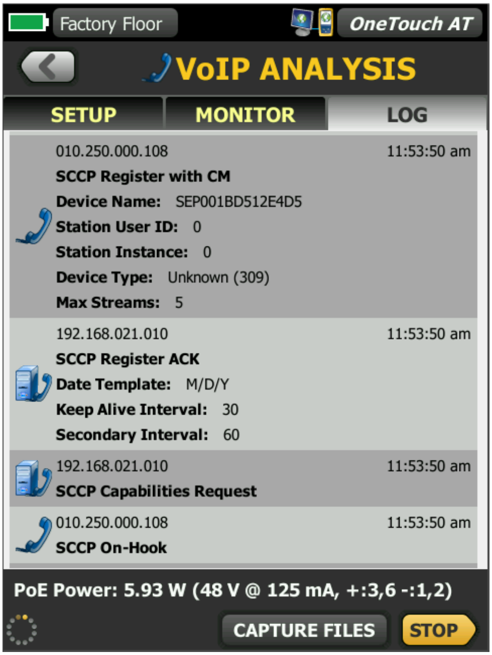
The phone boots up and establishes link

9 As the phone boots up and establishes link, observe the **Advertised Speed** and **Advertised Duplex** information at the top of the MONITOR screen. If they are not the same for the phone and the switch the phone may power up but no packets will be sent, as indicated by the **Packets** count.

Detailed information about the MONITOR screen is provided on page 260.

VoIP ANALYSIS Screen, LOG Tab

10 Tap the LOG tab. The LOG screen is displayed.



010.250.000.108 11:53:50 am
SCCP Register with CM
Device Name: SEP001BD512E4D5
Station User ID: 0
Station Instance: 0
Device Type: Unknown (309)
Max Streams: 5

192.168.021.010 11:53:50 am
SCCP Register ACK
Date Template: M/D/Y
Keep Alive Interval: 30
Secondary Interval: 60

192.168.021.010 11:53:50 am
SCCP Capabilities Request

010.250.000.108 11:53:50 am
SCCP On-Hook

PoE Power: 5.93 W (48 V @ 125 mA, +:3,6 -:1,2)

Figure 93. The VoIP Analysis Results Screen, LOG Tab

The LOG screen shows messages regarding VoIP-related protocols.

DHCP - Shows that the phone obtained an IP address

TFTP - Shows that the phone downloaded the IP Phone Load from the server

SIP or SCCP messages show initialization information, such as the phone registering with the call manager. When you place a call, messages show the call state, establishment of the RTP session, etc. When the call is terminated, packet statistics (including loss and jitter), MOS score, and R-factor are shown.

RTP - The RTP codec in use is shown, along with VLAN information and type of service (TOS), which specifies the call traffic’s priority.

The icons at the left side of the LOG screen indicate the type of device that sent the message.

☎	Phone connected to Port B
▬	Switch
DHCP	DHCP server
☎	VoIP call manager
FTP	VoIP TFTP server
☎	VoIP RTP (the near phone at Port B)
☎	VoIP RTP (the far phone)

Stopping the Test

To end the VoIP Analysis test, tap the back button <. When you tap the back button a second time power to the phone is removed.

VoIP Analysis Report

After running a VoIP analysis test you can tap the OneTouch AT button at the top-right corner of the screen to create a report that includes all of the information from the MONITOR and LOG screens.

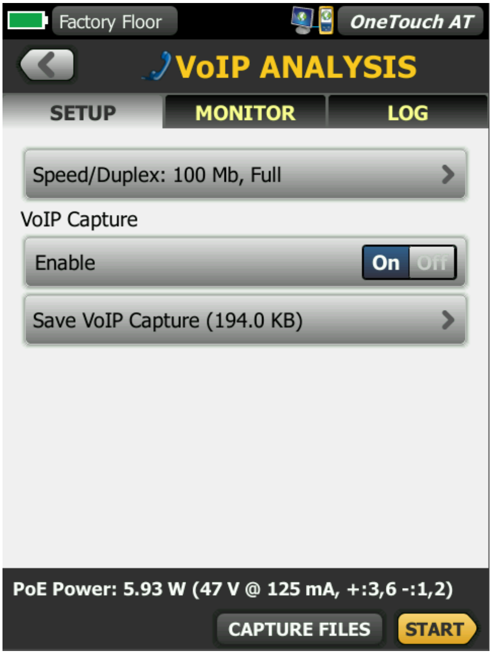
VoIP Analysis Packet Capture

When this option is purchased and enabled, VoIP analysis packet capture creates a capture file containing all traffic seen inline between the switch and the phone. The capture file can be saved and then analyzed using Fluke Networks ClearSight Analyzer software or other protocol analysis software. Use VoIP capture for saving VoIP traffic. Use packet capture (see Chapter 9: "Packet

Capture," beginning on page 281) to capture higher volume traffic.

1 Follow steps 1 through 5, beginning on page 253.

2 On the VoIP Capture Enable button, select **On**.



Speed/Duplex: 100 Mb, Full

Enable: On Off

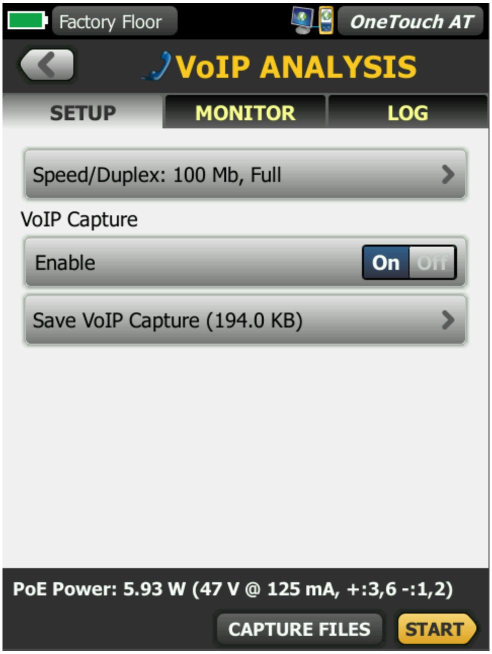
PoE Power: 5.93 W (47 V @ 125 mA, +:3,6 -:1,2)

Figure 94. The VoIP Analysis Configuration Screen

3 Tap the **START** button START.

4 Observe the MONITOR or LOG tab of the VoIP ANALYSIS screen. You can watch the phone power-up, boot-up, obtain an IP address, etc. You can place a call to generate traffic that you want to capture and analyze.

5 When you determine that the packets of interest have been exchanged, tap the back button to stop the test and the capture. The VoIP ANALYSIS configuration screen is displayed.



Speed/Duplex: 100 Mb, Full

VoIP Capture

Enable On Off

Save VoIP Capture (194.0 KB)

PoE Power: 5.93 W (47 V @ 125 mA, +:3,6 -:1,2)

Figure 95. The VoIP Analysis - Save VoIP Capture

The **Save VoIP Capture** button is displayed, indicating that packets were captured and they can be saved to a file.

6 Tap the **Save VoIP Capture** button.

The CAPTURE FILENAME screen is displayed.

By default, the capture file name format is cap–<date><time>.cap

You can use the keyboard to change the capture file name if desired. The .cap extension cannot be changed.

7 Tap the **DONE** button. The VoIP capture file is saved on the SD card and the VoIP ANALYSIS screen is displayed.

Managing Capture Files

You can view and manage the list of captured files as follows:

1 Tap the **CAPTURE FILES** button CAPTURE FILES.

The list of capture files is displayed.

- The IMPORT button lets you copy a capture file from another OneTouch AT analyzer to the SD card.

Select a file from the list.

- Buttons are displayed at the bottom of the screen that allow you to delete, rename, or export capture files.
- To move or copy capture files to a PC, eject the SD card and read it using a PC. Or see “Managing Files” on page 303.

Analyzing Capture Files

You can use Fluke Networks ClearSight Analyzer software or other protocol analysis software to analyze the captured packets on a PC.

VoIP ANALYSIS Screen, MONITOR Tab

The MONITOR tab displays link information and packet statistics. The following section provides details regarding the information displayed on the MONITOR tab.

The phone’s and the switch’s **Advertised Speed** and **Advertised Duplex** are shown. Ensure that you selected the correct speed and duplex for the phone in step 5.

The number of **bytes** and **packets** received from the switch on Port A, and the number of bytes and packets received from the VoIP phone on Port B are displayed.

Multicasts and **broadcasts** received on each port are shown.

FCS Errors - This counter increments for each frame received that has an integral length (8-bit multiple) of 64-1518 bytes and contains a frame check sequence error.

Undersize Frames - This counter increments each time a frame is received that is less than 64 bytes in length, contains a valid FCS, and was otherwise well formed. This count does not include range or length errors.

Undersize frames may be caused by a faulty or corrupt LAN driver.

Oversize Frames - This counter increments each time a frame is received that exceeds 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN), contains a valid FCS, and was otherwise well formed.

In general you should not see oversize frames, though their presence is not a guarantee that the network is failing. Oversize frames may be caused by a faulty or corrupt LAN driver.

Fragments - This counter increments for each frame received that contains an invalid FCS and is less than 64 bytes in length. This includes integral and non-integral lengths.

Jabbers - This counter increments for each frame that exceeds 1518 bytes in length (non-VLAN) or 1522 bytes (on a VLAN) and contains an invalid FCS. This includes alignment errors.

Possible causes include a bad NIC or transceiver, faulty or corrupt NIC driver, bad cabling, grounding problems, and nodes jamming the network due to above normal collision rates.

A possible solution would be to identify the node(s) that are sending out excessive errors and replace the defective hardware.

Dropped Frames - This counter increments for each frame that is received but is later dropped due to a lack of system resources.

Control Frames - This counter increments for each MAC control frame received (PAUSE and unsupported) from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, with a valid CRC.

PAUSE Frames - This counter increments each time a PAUSE MAC control frame is received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, with a valid CRC.

Unknown OP codes - This counter increments each time a MAC control frame is received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, and contains an opcode other than PAUSE, but the frame has a valid CRC.

Alignment Errors - This counter increments for each frame received that is from 64 bytes to 1518 bytes (non-VLAN) or 1522 bytes (on a VLAN) in length, contains an invalid FCS, and is not an integral number of bytes.

Alignment errors may manifest as an inability to connect to the network or as intermittent connectivity.

Frame Length Errors - This counter increments for each frame received in which the 802.3 length field did not match the number of data bytes actually received (46-1500 bytes). The counter does not increment if the length field is not a valid 802.3 length, such as an Ethertype value.

Code Errors - This counter increments each time a valid carrier is present and at least one invalid data symbol is detected.

Carrier Sense Errors - This counter shows the number of times that the carrier sense condition was lost or was not asserted when attempting to transmit frames. The count increments at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Browser

The OneTouch 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 or Wi-Fi Ethernet connection to your network. You can use a copper or fiber connection at Port A, or a copper connection at the management port.
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: the management port, the wired port (Port A, using copper or fiber), or the Wi-Fi port.

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 TOOLS.

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 or Wi-Fi Ethernet connection to your network. You can use a copper or fiber connection at Port A, or a copper connection at the management port.

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: the management port, the wired port (Port A, using copper or fiber), or the Wi-Fi port.

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 OneTouch analyzer starts a telnet or SSH session.

Use the on-screen keyboard to type your commands.

To end the session, tap the back button <.

Toner

Toner can help you locate a copper network cable.

The OneTouch analyzer creates a signal in the cable. You then place a probe on nearby cables until you identify the cable with the tone. The OneTouch analyzer can produce a tone that is compatible with virtually any cable toner probe.

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

2 In the **Testing Tools** section, tap **Toner**.

3 Tap the **Mode** button.

4 Choose a toning mode that is compatible with your probe. Choices are Intellitone, Analog 400 Hz, and Analog 1000 Hz. When you select a mode, the previous screen appears.

5 Tap the **START** button to begin toning. A progress wheel appears on the OneTouch analyzer's screen, indicating toning is in progress.

6 Use the probe to test suspected cables until you find the one that is connected to the OneTouch analyzer. See your toner probe manual for details.

7 Tap the **STOP** button when you have located the cable.

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 OneTouch 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 OneTouch 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 OneTouch 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 OneTouch analyzer's screen.

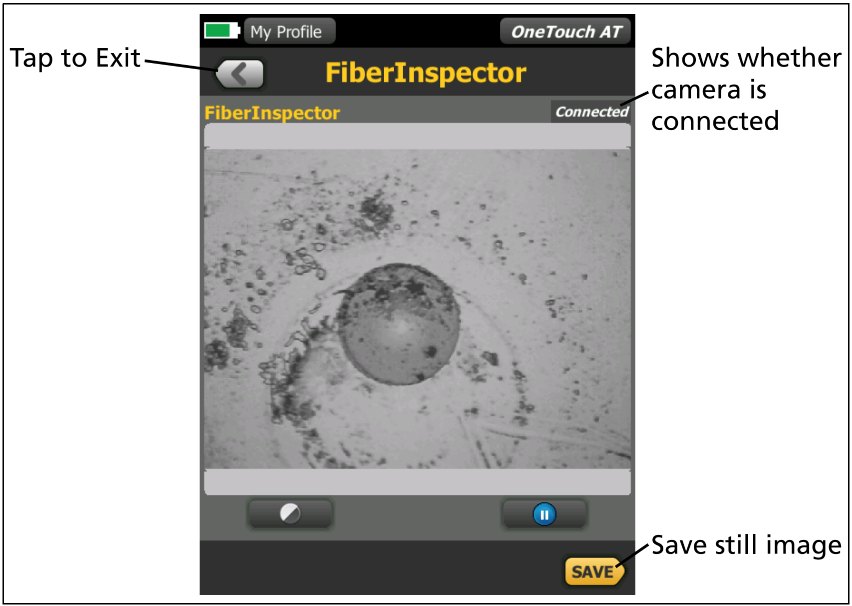


Figure 96. FiberInspector Image of an Endface

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**.

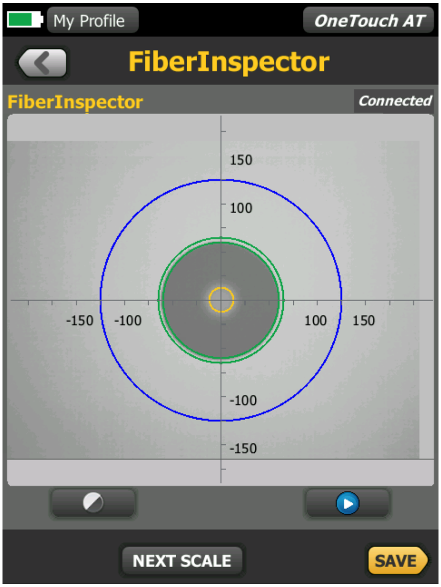


Figure 97. FiberInspector Image with Measurement Scales
(fiber with 50 µm core shown)

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 OneTouch 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 OneTouch analyzer's screen.

4 Have the remote colleague establish a remote connection to the OneTouch analyzer via a web browser (as described on page 312). 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.

File Tools

The following file tools are available on the TOOLS screen.

Profiles

See Chapter 5: "Profiles," beginning on page 165.

AP Authorization

See “Save an Authorization File” on page 238.

Reports

The OneTouch analyzer can create a comprehensive report in PDF format with specific report options. The available options are Tools Settings, AutoTest, Wired Analysis, Wi-Fi Analysis, and VoIP Analysis.

When you initially power on a OneTouch analyzer, only two selectable report options are available, the Tools Settings and AutoTest. You must run AutoTest to include AutoTest data in the saved report.

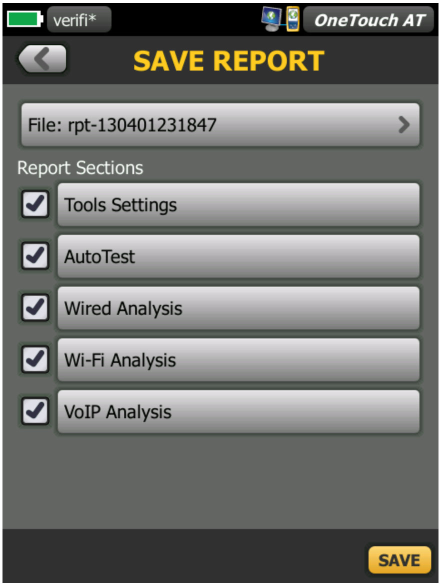
Obtaining Report Options

If you want to see AutoTest, Wired Analysis, Wi-Fi Analysis, or VoIP Analysis options included in your saved report, follow these guidelines:

- To obtain AutoTest and Wired Analysis data in your report run AutoTest, select its check box, and save.
- To obtain Wi-Fi Analysis data in your report, run Wi-Fi Analysis, select its check box, and save.
- To obtain VoIP Analysis data in your report, run VoIP Analysis, select its check box, and save.

Note

The OneTouch analyzer must be connected to the wired network to display the Wired Analysis option in the SAVE report option list.



File: rpt-130401231847

Report Sections

☑ Tools Settings

☑ AutoTest

☑ Wired Analysis

☑ Wi-Fi Analysis

☑ VoIP Analysis

Figure 98. Available Report options

To save a OneTouch analyzer report:

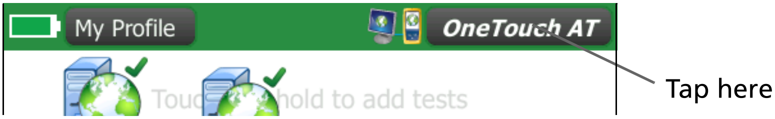
1. On the HOME screen, tap **TOOLS**.
2. Scroll down to the File Tools section, and tap **Reports**.
3. Tap the **SAVE** button.
4. Change the file name if desired, then tap the **Done** button.
5. Use the check boxes to select report options to be included in the report.
6. Tap the **SAVE** button. The report is saved in PDF format to the analyzer’s /internal/Reports directory. You can access the saved file as described in Chapter 10: "Managing Files," beginning on page 303.
7. Tap **VIEW** to see the saved report on the OneTouch analyzer. See also: page 312.

Screens

Save a Screen Image

You can take a screen shot of the OneTouch analyzer's display as follows:

① Tap the text that says OneTouch AT 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 OneTouch screens using the SCREENS tool. You can manage (import, export, rename, or delete) previously saved OneTouch 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 OneTouch 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 management port is the RJ-45 Ethernet port located on the left side of the OneTouch analyzer.

The Management port links automatically when connected to a network. You do not have to tap the AutoTest button ✓TEST to make the management port link.

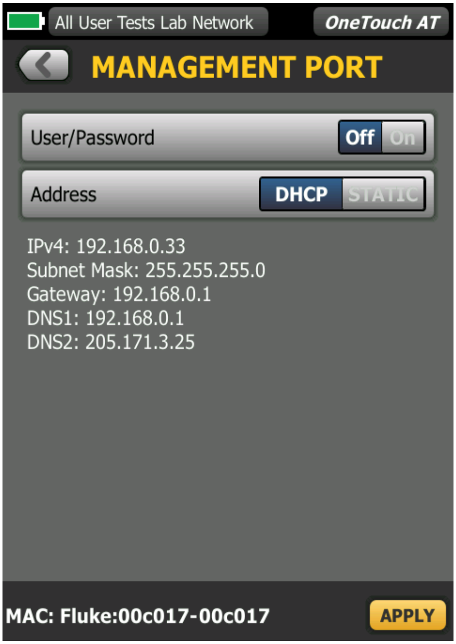
The OneTouch analyzer’s management port can be used for:

- Remote viewing and control of the OneTouch analyzer via web browser
- Accessing the OneTouch 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

To configure the Management Port:

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

2 Scroll down to the Maintenance Tools section and tap **Management Port**. The management port screen is displayed.



IPv4: 192.168.0.33
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.1
DNS1: 192.168.0.1
DNS2: 205.171.3.25

MAC: Fluke:00c017-00c017

Figure 99. Management Port Screen

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 Tap the **Apply** button.

Address Control (DHCP or Static)

The Address control can be set to DHCP or Static. When set to DHCP, the OneTouch analyzer gets its IP address, subnet mask, etc. from the DHCP server.

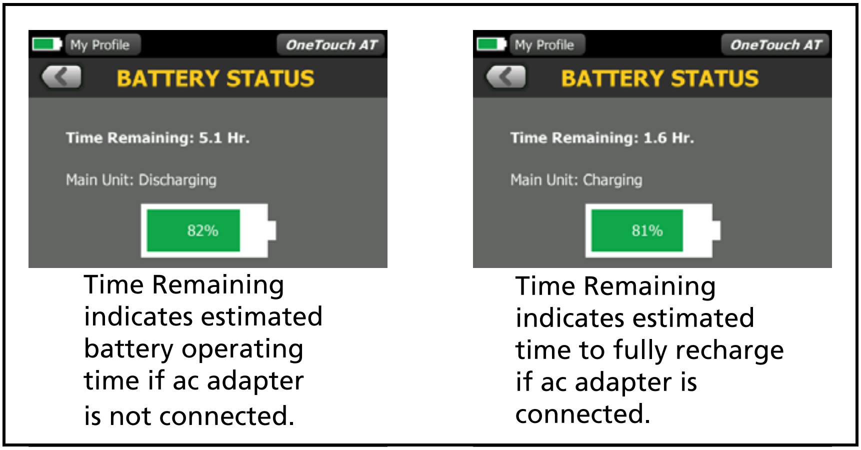
If the analyzer has obtained an IP address via DHCP, and you subsequently switch the Address control to Static, the currently configured IP address, subnet mask, etc. will be retained until you change it.

Setting a static IP address for the OneTouch 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 OneTouch analyzer and view the Management Port screen.

If a network administrator needs to reserve an IP address for the OneTouch 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 250.

Battery Status

This screen shows the battery's status.



Time Remaining: 5.1 Hr.

Main Unit: Discharging

82%

Time Remaining indicates estimated battery operating time if ac adapter is not connected.

Time Remaining: 1.6 Hr.

Main Unit: Charging

81%

Time Remaining indicates estimated time to fully recharge if ac adapter is connected.

Figure 100. Battery Status Screen

Language

See "Set the Language" on page 19.

Date/Time

See "Date/Time" on page 42.

Number

See "Number Format" on page 43.

Length

See "Units for Length Measurements" on page 43.

Timeout Period

See "Timeout Periods (Power-Down and Backlight)" on page 43.

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**.

Power Line Frequency

4 See "Power Line Frequency" on page 43.

Display Brightness

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 OneTouch analyzer on battery power.

Software Update

To prevent problems caused by losing power during a software update, supply power to the OneTouch analyzer with the ac adapter.

To update software, download the new software image file from www.flukenetworks.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 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.

Options

If you did not purchase your OneTouch 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 Fluke Networks. 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.

Restore Factory Defaults, Erase Data

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 OneTouch 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 can be performed on Wi-Fi or wired connections.

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 packet capture option can be included at time of purchase, or it can be purchased separately by contacting Fluke Networks (see page 17).

The OneTouch AT analyzer can silently monitor and record wired and Wi-Fi 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 OneTouch 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 Fluke Networks ClearSight Analyzer or other packet capture analysis software.

General Information about 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.
- You can create a Wi-Fi packet capture filter to capture only packets that are going to and from a particular AP.

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 101.

Port Filter =
80

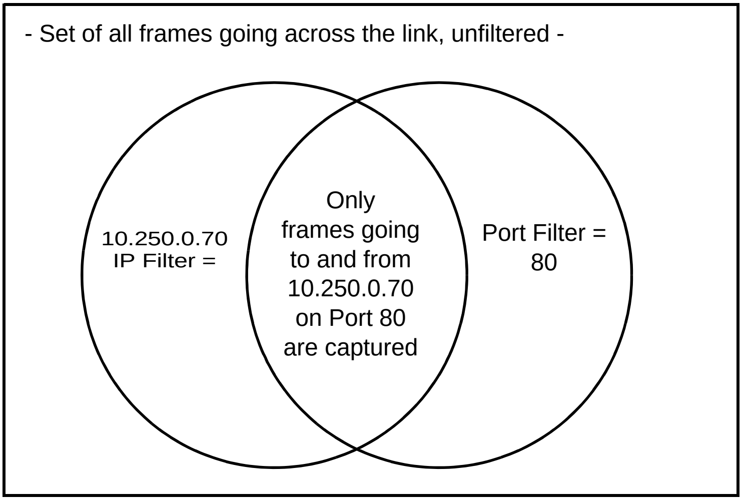

- Set of all frames going across the link, unfiltered -
10.250.0.70
IP Filter =
Only frames going to and from 10.250.0.70 on Port 80 are captured
Port Filter =
80

Figure 101. 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.

Wired Packet Capture Connection Options

Port A Only (Single-ended Packet Capture)

In single-ended packet capture, the OneTouch analyzer captures traffic at Port A of the OneTouch analyzer. When performing single-ended packet capture, the OneTouch analyzer is typically connected to a span port, mirror port, or tap.

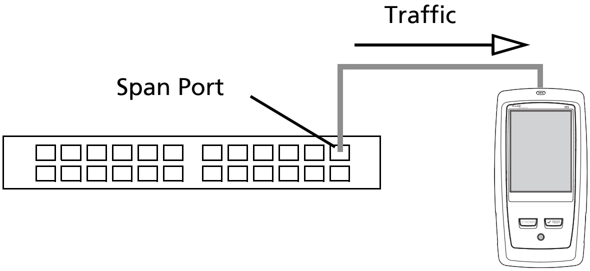


Figure 102. Single-Ended Packet Capture

Ports A and B

The OneTouch analyzer can capture traffic from ports A and B simultaneously. When performing packet capture on ports A and B traffic is captured on both ports but is not routed between the two ports.

Inline Packet Capture

When performing inline packet capture, the OneTouch analyzer captures traffic flowing between ports A and B. The OneTouch analyzer is inserted in the link, with one side of the link connected to the OneTouch analyzer Port A, and the other side connected to Port B.

Device or Network

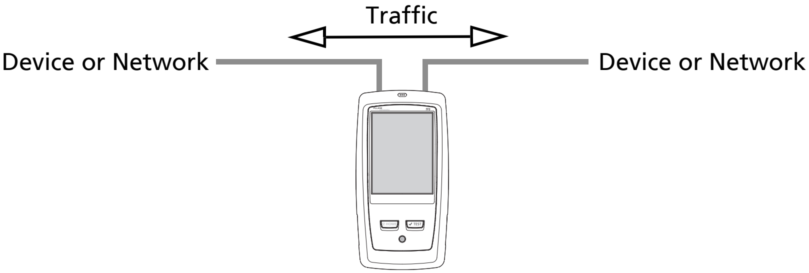


Figure 103. Inline Packet Capture

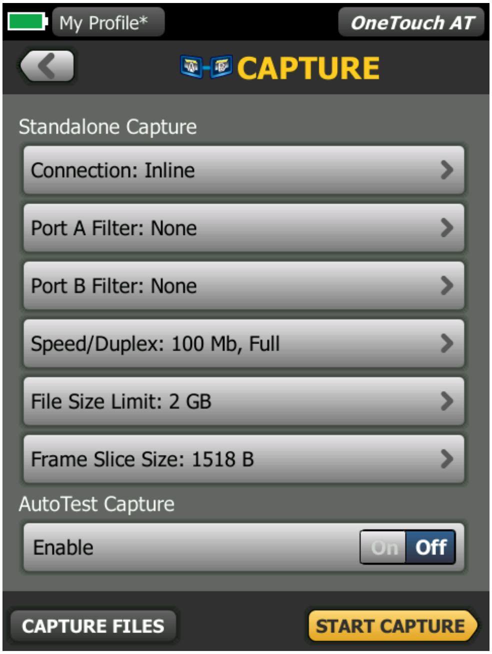
This connection method is preferred when performing tasks such as debugging communication problems between an endpoint (e.g. access point, PC, phone, camera) and the network.

- If present, PoE is passed through when using inline packet capture.
- All traffic is passed between the ports regardless of filters that you have set. See “General Information about Capture Filters” on page 282.
- Traffic is passed between ports only when the packet capture is running. Link is dropped when you leave the CAPTURE screen.

To Configure Wired Packet Capture

1. On the HOME screen, tap **TOOLS** .
2. In the **Testing Tools** section, tap **Capture**.
3. Tap the **Connection** button and select one of the following options.
    - Port A only
    - Ports A and B
    - Inline

The CAPTURE screen is displayed.



Standalone Capture

Connection: Inline

Port A Filter: None

Port B Filter: None

Speed/Duplex: 100 Mb, Full

File Size Limit: 2 GB

Frame Slice Size: 1518 B

AutoTest Capture

Enable — On Off

Figure 104. The Wired CAPTURE Screen

Port A Filter and Port B Filter

From the CAPTURE screen, tap the **Filter** button for Port A or Port B. You can set up independent filters for packets received at Port A and at Port B.

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 exclude non-IPv6 traffic. Only IPv6 traffic is captured.

COPY FROM B and COPY FROM A Buttons

These buttons copy the filter settings from the other port.

Inline Speed and Duplex

When using inline packet capture, set the speed and duplex in the capture configuration to match the link where you are inserting the OneTouch AT analyzer.

File Size Limit and Frame Slice Size

Limits control the amount of data that will be captured.

Frame Size Limit

The OneTouch 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.

Next Step

See “Start Packet Capture” on page 298

Wi-Fi Packet Capture

The OneTouch AT analyzer can be used to capture 802.11 packets on RF channels for the purpose of analyzing and troubleshooting difficult Wi-Fi problems.

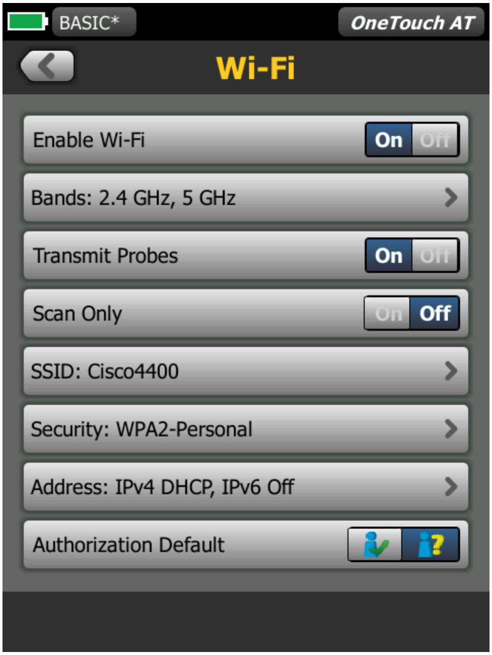
The OneTouch AT Wi-Fi option is required, and the option must be enabled as described below.

Enable Wi-Fi

1 Press the HOME key on the front panel to display the HOME screen.

2 Tap the **TOOLS** icon .

3 Tap the **Wi-Fi** button. The Wi-Fi settings screen is displayed



BASIC*

OneTouch AT

Wi-Fi

Enable Wi-Fi: On [✓ On] Off

Bands: 2.4 GHz, 5 GHz

Transmit Probes: [✓ On] Off

Scan Only: On [✓ Off]

SSID: Cisco4400

Security: WPA2-Personal

Address: IPv4 DHCP, IPv6 Off

Authorization Default

Figure 105. Wi-Fi Test Settings Screen

4 Ensure that **Enable Wi-Fi** is **On**.

Configure Wi-Fi Packet Filtering

You can manually configure filtering, or you can let the OneTouch analyzer automatically configure a filter to capture traffic on a specific access point (AP), client, or channel.

- To manually configure a filter, start with the TOOLS button on the HOME screen
- To automatically configure an AP, client, or channel filter, start with the Wi-Fi ANALYSIS screen.

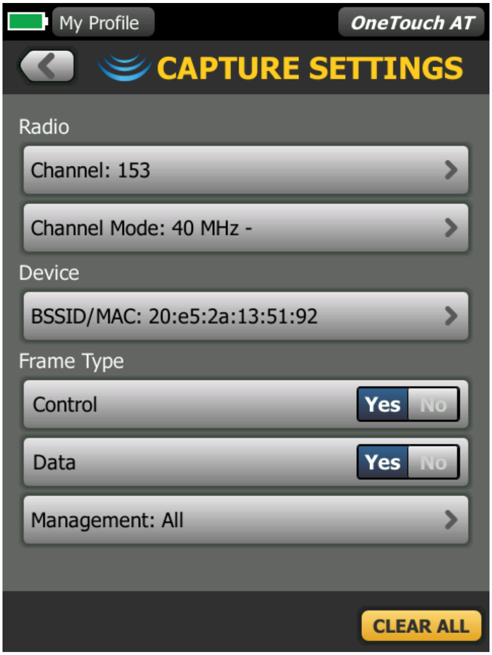
To Manually Configure a Filter

1 On the HOME screen, tap the Tools icon 🔧.

2 In the Testing Tools section of the screen, tap the **Capture** button. The CAPTURE screen is displayed.

3 Tap the **Connection** button and select **Wi-Fi**.

4 Tap the **Wi-Fi Filter** button. The CAPTURE SETTINGS screen is displayed.



Radio

Channel: 153

Channel Mode: 40 MHz -

Device

BSSID/MAC: 20:e5:2a:13:51:92

Frame Type

Control Yes No

Data Yes No

Management: All

Figure 106. Wi-Fi CAPTURE SETTINGS Screen

The CAPTURE SETTINGS options are described below.

Channel

Tap the channel button to set the channel on which packets will be captured.

Channel Mode

By default, the channel mode is configured for a channel width of 20 MHz. Access points supporting legacy 802.11a/b/g protocols use a single, 20 MHz channel only. Access points that support the 802.11n protocol can be configured to use either a single 20 MHz channel or, for higher performance, use two, consecutive 20 MHz channels i.e., a 40 MHz bonded channel.

When capturing traffic for an access point that is configured to use a bonded channel, the channel mode should be set to 40 MHz + (primary channel plus adjacent higher channel number) or 40MHz – (primary channel plus adjacent lower channel number), to match the access point configuration. Only permissible bonding options are available based on the selected channel; e.g., channel 34 bonding can only be 40 MHz + because it is the first channel in the 5 GHZ band. If a bonded channel is not configured correctly, some packets will be missing from the capture.

Device BSSID/MAC

Enter a BSSID to capture only packets going to or from the target device.

Control Frames

Control frames assist in the exchange of data frames between stations. Common control frame types include Request to Send (RTS), Clear to Send (CTS), and Acknowledgement (ACK).

Select **Yes** to capture control frames.

Data Frames

Select **Yes** to capture data frames.

To view the data contents of WEP- or PSK-encrypted packets, use the encryption key and decryption-capable software such as Fluke Networks ClearSight Analyzer or Wireshark.

Management Frames

Tap the Management button to open the MANAGEMENT FRAMES screen. This screen lets you customize the capture to include or exclude various types of management frames, such as beacons, association requests, probe responses, etc.

Set a frame type to **Yes** to include it in the capture; set it to **No** to exclude it from the capture.

The button at the lower right corner of the screen toggles between **CLEAR ALL** and **SET ALL**.

Files Size Limit and Frame Slice Size

Tap the back button ‹ to return from the CAPTURE SETTINGS screen to the CAPTURE screen.

See “File Size Limit and Frame Slice Size” on page 288.

File Format

Tap the **File Format** button and select the packet analyzer software you will use for packet analysis. The button displays the packet analysis software name and the radio header type is shown in parenthesis.

The pcap application programming interface (API) is used for all file formats. The radio header is specific to each selection.

The radio header contains Wi-Fi radio signal information such as channel number, signal strength, and bit rate.

Select **None** to exclude radio header information from captured packets.

Next Step

See “Start Packet Capture” on page 298

To Automatically Configure a Filter

When you access the capture tool via Wi-Fi analysis, the OneTouch AT analyzer automatically configures a filter to capture traffic on an AP, client, or channel.

You can implement further filtering if desired. Control and data frames can be included or excluded from the capture, as can many types of management frames.

Open the Wi-Fi ANALYSIS Screen

On the HOME screen, tap the Wi-Fi icon. The icon's appearance indicates the Wi-Fi status.

If the Wi-Fi status is

(stopped), (scanning), or (linked, not testing) the Wi-Fi ANALYSIS screen will be displayed and Wi-Fi analysis will begin.

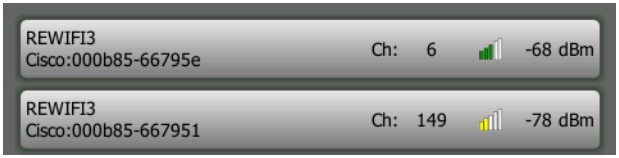
If the Wi-Fi adapter is linked and testing , stop the AutoTest that is in progress or wait for it to finish. Then tap the Wi-Fi icon. The Wi-Fi ANALYSIS screen is displayed.

Filter by AP

Only packets to or from the selected AP are captured. Further filtering can be implemented as described later in this chapter.

1. On the Wi-Fi ANALYSIS screen, tap the **AP** tab.
2. Select an AP to display its details. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen.
3. Tap the **TOOLS** button.
4. Tap the **Capture** button.

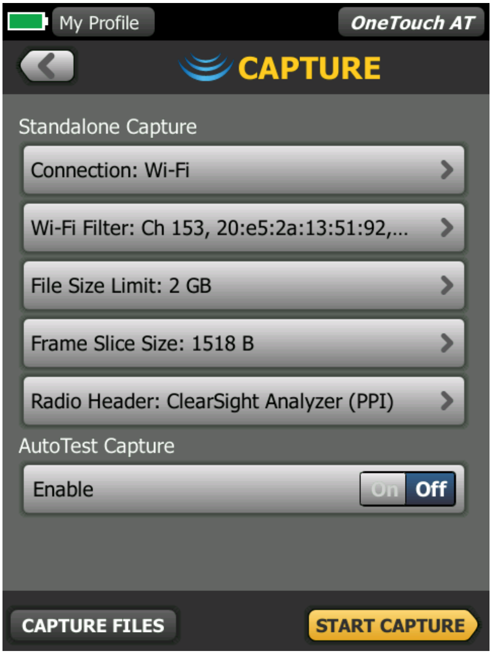
5 For dual-band APs or APs that support multiple SSIDs, select the BSSID and channel of interest.



REWIFI3
Cisco:000b85-66795e Ch: 6 -68 dBm

REWIFI3
Cisco:000b85-667951 Ch: 149 -78 dBm

The CAPTURE screen is displayed and the filter configuration is indicated on the **Wi-Fi Filter** button.



Standalone Capture

Connection: Wi-Fi

Wi-Fi Filter: Ch 153, 20:e5:2a:13:51:92,...

File Size Limit: 2 GB

Frame Slice Size: 1518 B

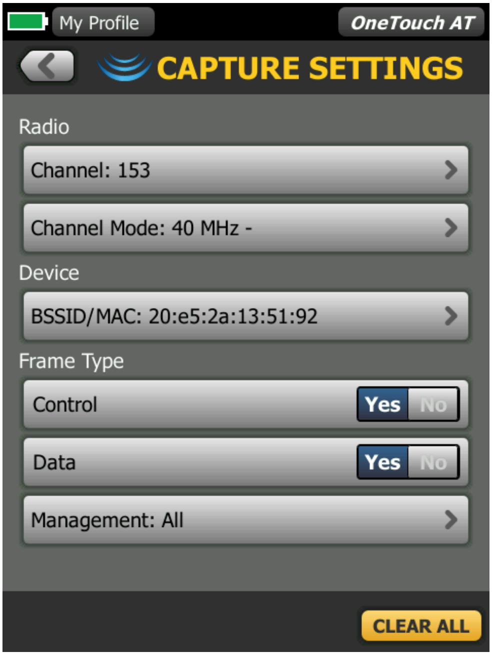
Radio Header: ClearSight Analyzer (PPI)

AutoTest Capture

Enable On Off

Figure 107. Wi-Fi CAPTURE Screen

6 Tap the **Wi-Fi Filter** button. The CAPTURE SETTINGS screen is displayed.



Radio

Channel: 153

Channel Mode: 40 MHz -

Device

BSSID/MAC: 20:e5:2a:13:51:92

Frame Type

Control [✓ Yes] No

Data [✓ Yes] No

Management: All

Figure 108. CAPTURE SETTINGS Screen

From this screen, you can further modify your capture settings.

For more information see "To Manually Configure a Filter" on page 290.

To start the capture see "Start Packet Capture" on page 298.

Filter by Client

Only packets to and from the selected client are captured. Further filtering can be implemented as described later in this chapter.

1 On the Wi-Fi ANALYSIS screen, tap the **CLIENT** tab.

2 Select a client to display its details. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen.

3. Tap the **TOOLS** button.
4. Tap the **Capture** button. The CAPTURE screen is displayed and the client’s channel number and MAC are shown on the **Wi-Fi Filter** button.
5. Tap the **Wi-Fi Filter** button. The CAPTURE SETTINGS screen is displayed.

From this screen, you can further modify your capture settings.

For more information see “To Manually Configure a Filter” on page 290.

To start the capture see “Start Packet Capture” on page 298.

Filter by Channel

Only packets on the selected channel are captured.

1. On the Wi-Fi ANALYSIS screen, tap the **CHANNEL** tab.
2. Select a channel to display its details. The Wi-Fi **TOOLS** button TOOLS appears in the lower-right corner of the screen.
3. Tap the **TOOLS** button.
4. Tap the **Capture** button. The CAPTURE screen is displayed and the channel number and channel width are shown on the **Wi-Fi Filter** button.
5. Tap the **Wi-Fi Filter** button. The CAPTURE SETTINGS screen is displayed.

From this screen, you can further modify your capture settings.

For more information see “To Manually Configure a Filter” on page 290.

To start the capture see “Start Packet Capture” on page 298.

Start Packet Capture

1 On the CAPTURE screen, tap the **START CAPTURE** button. The CAPTURE FILENAME screen is displayed.

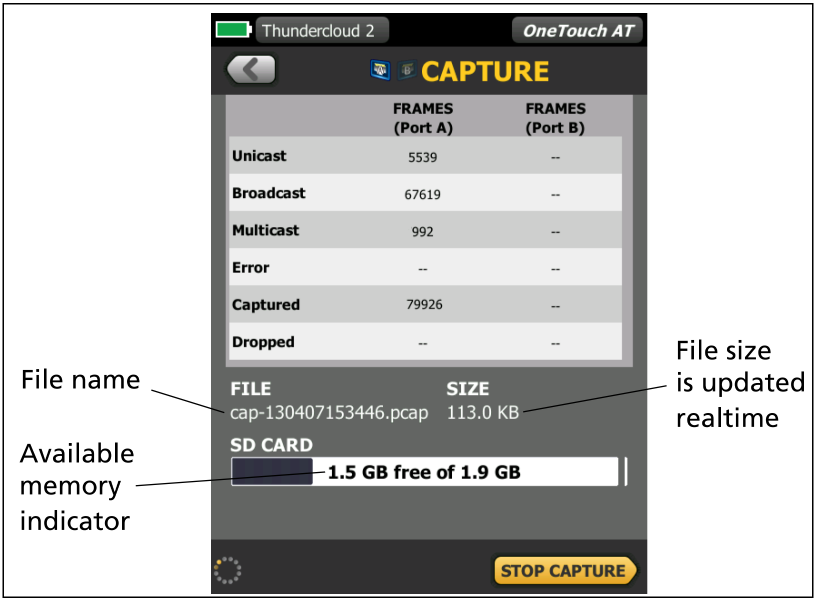
By default, the capture file name format is as follows:

- cap–<date><time>.pcap (wired capture files)
- wcap–<date><time>.pcap (Wi-Fi 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 Port A and Port B.



	FRAMES (Port A)	FRAMES (Port B)
Unicast	5539	--
Broadcast	67619	--
Multicast	992	--
Error	--	--
Captured	79926	--
Dropped	--	--

FILE: cap-130407153446.pcap
SIZE: 113.0 KB

SD CARD: 1.5 GB free of 1.9 GB

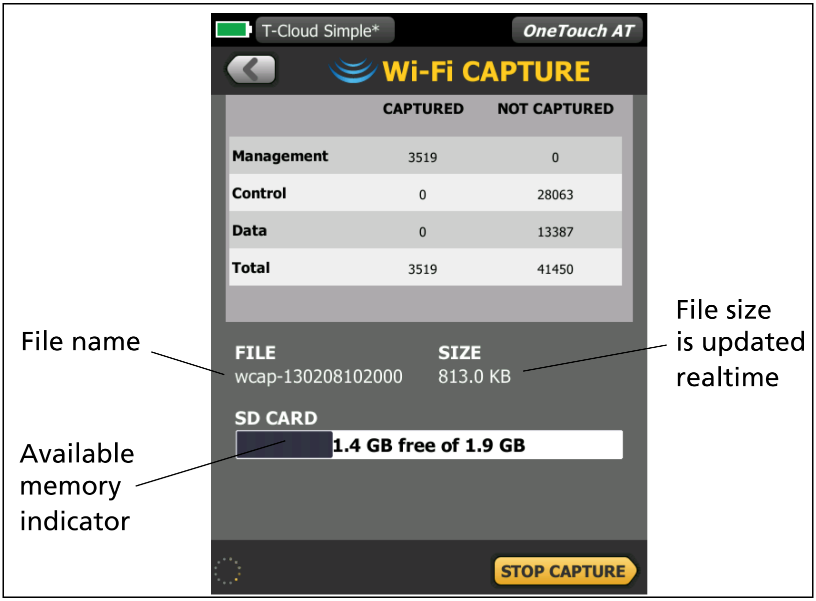
File name

Available memory indicator

File size is updated realtime

Figure 109. Wired Capture Results

As a Wi-Fi packet capture progresses, management, control, data, and total frame counts are shown.



	CAPTURED	NOT CAPTURED
Management	3519	0
Control	0	28063
Data	0	13387
Total	3519	41450

FILE
wcap-130208102000

SIZE
813.0 KB

SD CARD
1.4 GB free of 1.9 GB

Figure 110. Wi-Fi 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 reappears. 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 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 and Wi-Fi 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 button *OneTouch AT* 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.

Wired and Wi-Fi results are merged into a single capture file.

The AutoTest capture file size is limited to 32 MB per wired or Wi-Fi interface, or 64 MB if both wired and Wi-Fi interfaces are used.

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.

Note

Wi-Fi packets are received as 802.11 data frames. In Wi-Fi capture, the 802.11 header is removed. 802.11 management and control frames are not captured.

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 CAPTURE FILES.

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 303.

Analyzing Capture Files

You can use Fluke Networks 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
- AP Authorization (Authorization Control Lists/ACLs)
- Reports
- Screens
- Certificates
- Packet captures

Profiles, AP Authorization lists, 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 248.

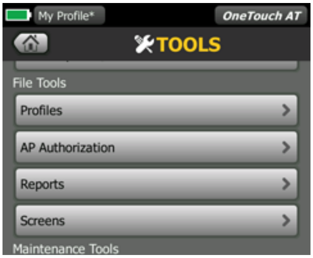
Packet captures can be managed using the Capture tool. See page 302.

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, AP Authorization, 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.

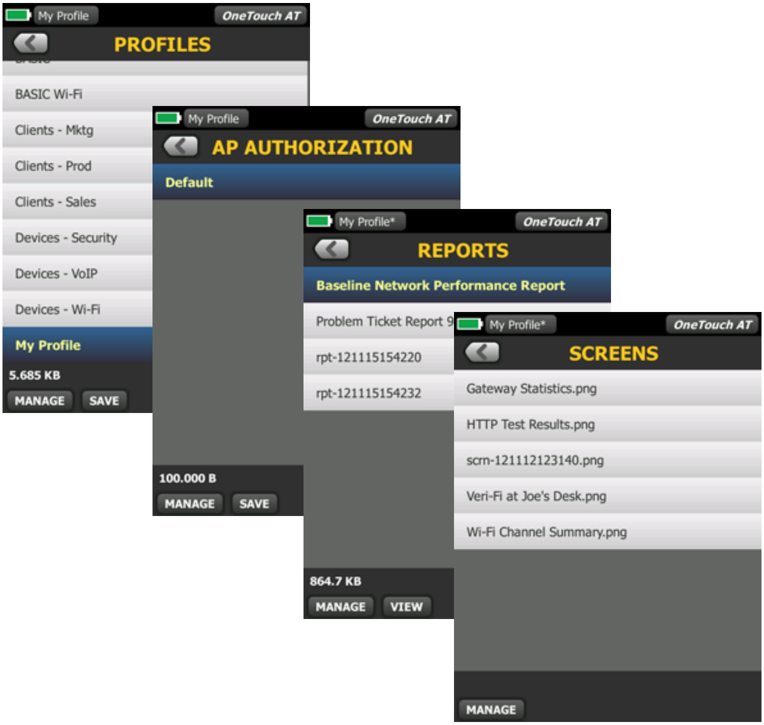


Figure 111. The Four File Manager Screens

The following section describes buttons that are available on one of more of the file manager screens.

SAVE

The **SAVE** button saves the current profile, AP authorization list, or report.

When you tap the **SAVE** button, the SAVE AS screen is displayed.

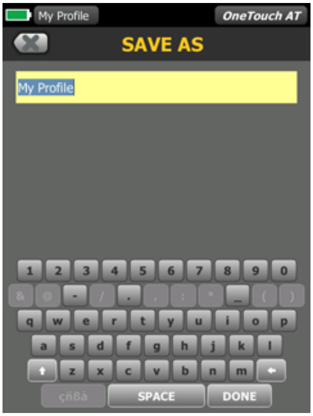


Figure 112. SAVE AS Screen

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

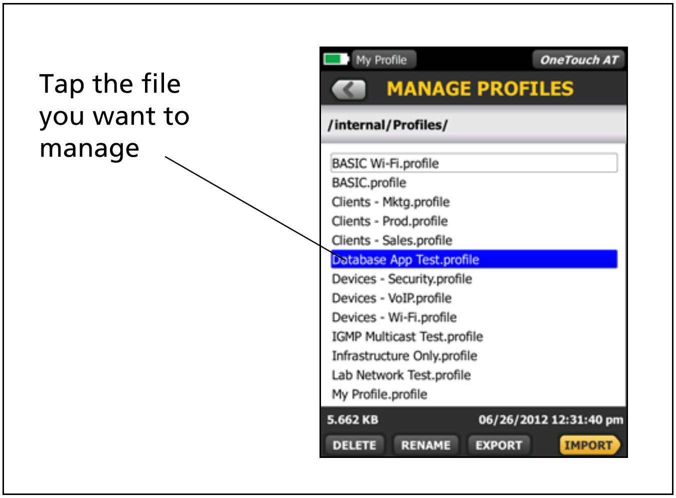
The **LOAD** button is available in the PROFILES file manager and the AP AUTHORIZATION file manager.

When you tap the **LOAD** button, the current profile or AP authorization list is replaced by the one you load. So consider saving the current profile or AP authorization list before you tap the **LOAD** button.

The **LOAD** button puts the highlighted profile or AP authorization list into use. A loaded profile or AP authorization list 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 33.

MANAGE

Profiles, AP authorization lists, reports, and screens each have their own directory in OneTouch analyzer's internal memory. Tap the **MANAGE** button to manage files in the Profiles, ACLs, Reports, or Screens directory. Then tap the file that you want to manage.



Tap the file you want to manage

/internal/Profiles/

BASIC Wi-Fi.profile
BASIC.profile
Clients - Mktg.profile
Clients - Prod.profile
Clients - Sales.profile
Database App Test.profile
Devices - Security.profile
Devices - VoIP.profile
Devices - Wi-Fi.profile
IGMP Multicast Test.profile
Infrastructure Only.profile
Lab Network Test.profile
My Profile.profile

5.662 KB 06/26/2012 12:31:40 pm

Figure 113. 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.

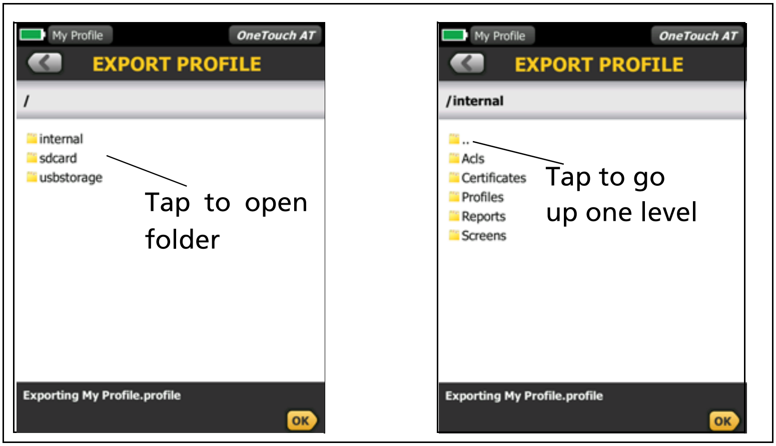
RENAME

RENAME lets you change the name of a profile, AP authorization list, 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.



Exporting My Profile.profile

Tap to open folder

Exporting My Profile.profile

Tap to go up one level

Figure 114. 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, AP authorization list, 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 OneTouch 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,
AP authorization lists must have the .acl 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 OneTouch analyzer remotely when you connect to its management port.

Remote viewing of the OneTouch analyzer's user interface is possible via a web browser or a VNC client connection. To remotely access the file system, connect via Web, FTP, 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

Connect Using a Web Browser

To connect to the OneTouch analyzer using a web browser:

1 Obtain the IP address of the management port as described on page 273.

2 Open a web browser.

3 Enter the OneTouch analyzer's Management Port IP address in the web browser's address field. The OneTouch analyzer's remote access browser home page will appear.

4 Tap the **Remote Control** button.

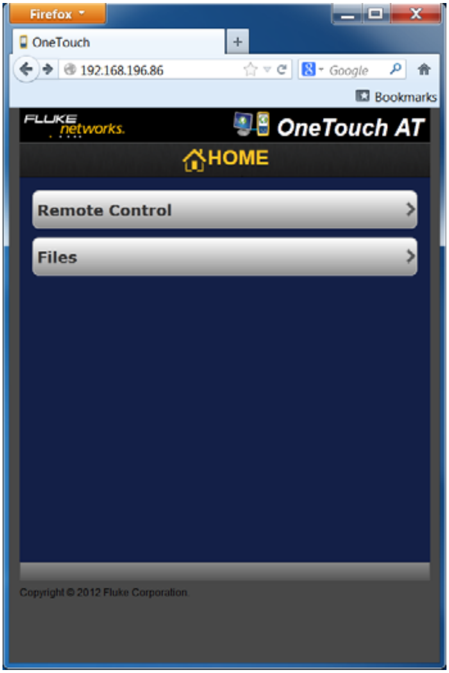
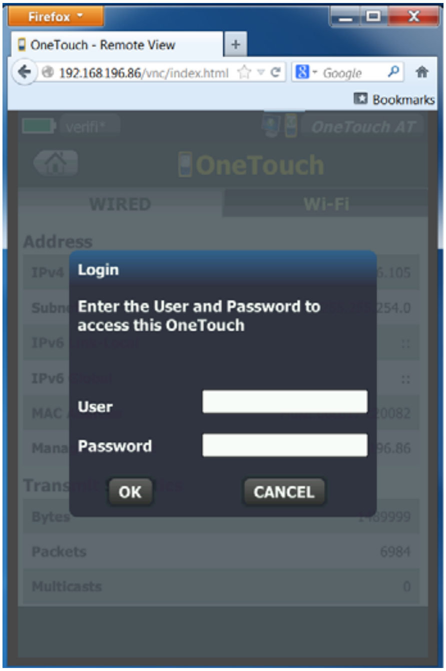


Figure 115. Remote Access Browser Home Page

5 If required, enter the **User** name and **Password** for the OneTouch analyzer. The OneTouch analyzer's HOME screen is displayed.



Login

Enter the User and Password to access this OneTouch

User

Password

Figure 116. Browser Remote Access Login Credentials

6 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items. You can use the Up/Down arrows or the PgUp/PgDn keys to scroll vertically.

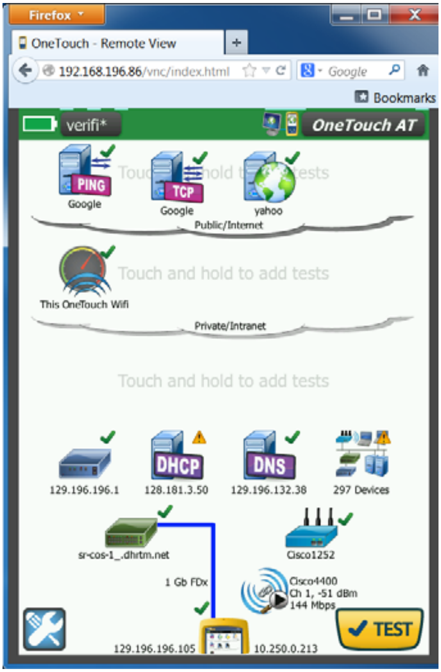


Figure 117. Remote Access One Touch Home Screen

Connect Using a VNC Client

To connect to the OneTouch analyzer using a VNC Client:

1. Obtain the IP address of the management port as described on page 273.
2. Provide the OneTouch analyzer's management port IP address to your VNC client.
3. Connect using your VNC client.
4. If required, enter the OneTouch analyzer's remote access **user** name and **password**. See "Configure Login Credentials for Remote Access" on page 274.

5 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.

Remote File Access

You can remotely access files on the OneTouch analyzer using a Web Browser, FTP, 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 273.

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: page 274.

5 Select the **Files** button.

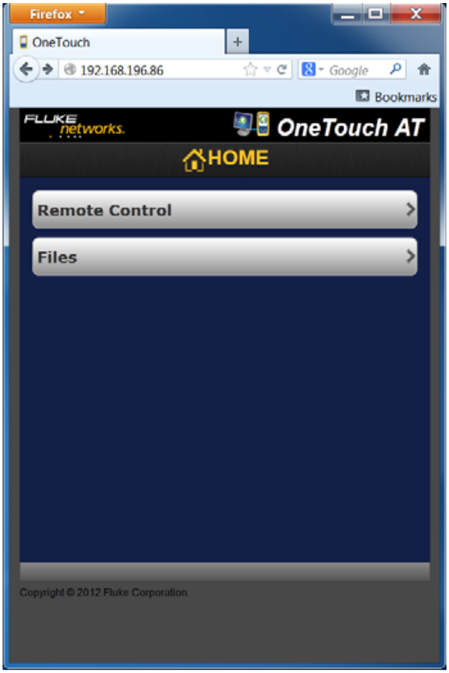
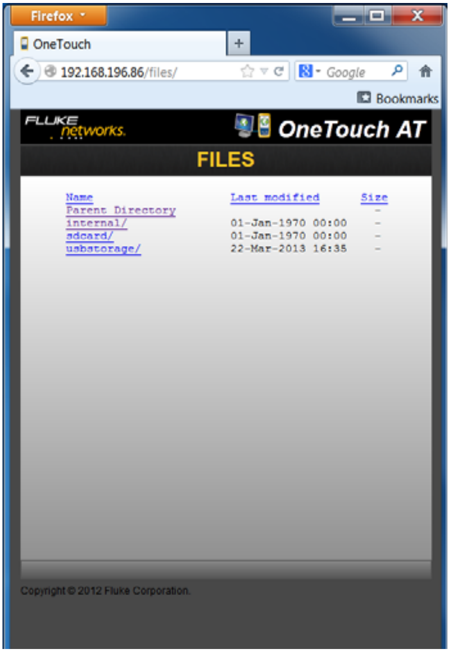


Figure 118. Remote Access Browser Home Page

6 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.



```
Name                       Last modified        Size
Parent Directory                                 -
internal/                  01-Jan-1970 00:00     -
sdcard/                    01-Jan-1970 00:00     -
usbstorage/                22-Mar-2013 16:35     -
```

Copyright © 2012 Fluke Corporation.

Figure 119. OneTouch analyzer Remote File Access

7 Download a file by clicking on the filename.

Note

You cannot delete, rename, move, or upload files using a Web Browser.

Remote File Access Using an FTP Client

To connect to the OneTouch analyzer's user file system with an FTP Client:

1 Obtain the IP address of the management port as described on page 273.

2 Provide the OneTouch 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 OneTouch analyzer’s files.

Remote File Access Using a Mapped Network Drive (WebDAV)

The OneTouch AT 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 7 computer.

1 Obtain the IP address of the management port as described on page 273.

2 Select the Windows 7 button.

3 Right-click **Computer**.

4 Select **Map network drive...**.

5 In the Map Network Drive dialog, select an available drive letter.

6 Enter the path to your OneTouch. 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 OneTouch analyzer’s management port. See also: page 274.

You may experience delays when using the network drive if there is no proxy server between the computer and the OneTouch. 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 OneTouch 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 OneTouch analyzer.

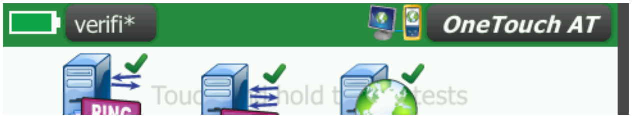
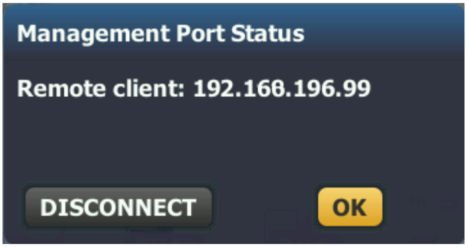


Figure 120. Remote Access icon located in Shortcut Bar

2 Select the **Disconnect** button.


Management Port Status

Remote client: 192.168.196.99

Figure 121. 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

- 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 OneTouch analyzer while you are connected, your remote session will be terminated. The OneTouch analyzer does not support concurrent remote user sessions.

SD Card

To manage files using an SD card, insert it into the OneTouch analyzer. See “SD card slot” on page 26. The OneTouch 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 OneTouch analyzer. See “USB-A Connector” on page 25. The OneTouch 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 servicable component. Do not open the case except to replace the battery.**
- **Use only replacement parts that are approved by Fluke Networks.**
- **Use only service centers that are approved by Fluke Networks.**

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 a 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 323 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 122.

Use only Fluke Networks battery model number TFS-BAT.

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.

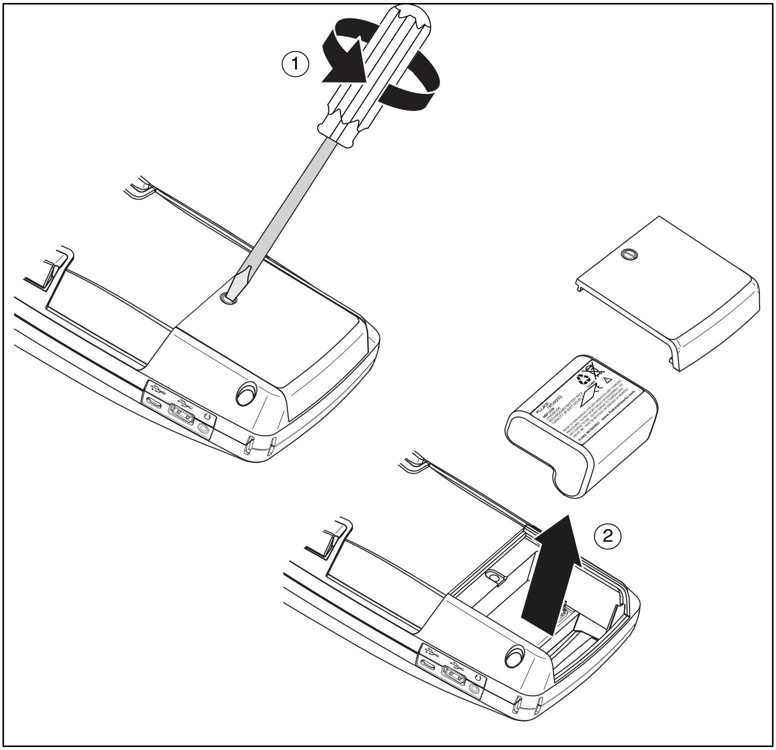


Figure 122. Remove and Install the Battery

Chapter 12: 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 61010-1:2001
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 61326-1:2006

[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: ± 6 feet (± 2 meters) or 5%, whichever is greater. Length measurement is based on Nominal Velocity of Propagation (NVP) for CAT 5e cable.

Network Ports

Network analysis ports	Two RJ-45 10/100/1000BASE-T Ethernet Two Small Form-factor Pluggable (SFP) 100BASE-FX/ 1000BASE-X Ethernet
Not for connection to telephone networks	The OneTouch AT analyzer is NOT designed for connection to a telephone network. The OneTouch AT 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 10BASE-T **IEEE 100BASE-T** **IEEE 1000BASE-T** **IEEE 100BASE-FX** **IEEE 1000BASE-X**	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 analyzer supports 100BASE-FX and 1000BASE-X SFP adapters.

Wi-Fi Antennas

Internal Wi-Fi antennas	Three internal 2.4 GHz, 1.1 dBi peak, 5 GHz, 3.2 dBi peak antennas.
External directional antenna	Antenna, frequency range 2.4 - 2.5 and 4.9 - 5.9 GHz. Minimum gain 5.0 dBi peak in the 2.4 GHz band, and 7.0 dBi peak in the 5 GHz band.
External antenna connector[1]	Reverse SMA

[1] External antenna port is receive-only (no transmit).

Wi-Fi Adapter

Applicant's name	Qualcomm Athheros, Inc.
Equipment name	Wi-Fi testing device
Model number	AR5BHB112
Manufacturing Year/ Month	2012/06
Manufacturer	Atheros Communications, Inc.
Country of origin	USA

Data rate	802.11a: 6/9/12/24/36/48/54 Mbps 802.11b: 1/2/5.5/11 Mbps 802.11g: 6/9/12/24/36/48/54 Mbps 802.11n (20 MHz): MCS0-23, up to 216 Mbps 802.11n (40 MHz): MCS0-23, up to 450 Mbps
Operating frequency	2.412 ~ 2.484 GHz (Industrial Scientific Medical Band) 5.170 ~ 5.825 GHz
Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X
Transmit output power[1] (tolerance: ±2.0 dBm)	802.11a: 12 dBm ± 2 dBm @ 54 Mbps 802.11b: 17 dBm ± 2 dBm @ 11 Mbps 802.11g: 16 dBm ± 2 dBm @ 54 Mbps 802.11gn HT20: 16 dBm ± 2 dBm @ MCS0 802.11gn HT20: 15 dBm ± 2 dBm @ MCS7 802.11gn HT40: 15 dBm ± 2 dBm @ MCS0 802.11gn HT40: 14 dBm ± 2 dBm @ MCS7 802.11an HT20: 15 dBm ± 2 dBm @ MCS0 802.11an HT20: 12 dBm ± 2 dBm @ MCS7 802.11an HT40: 14 dBm ± 2 dBm @ MCS0 802.11an HT40: 11 dBm ± 2 dBm @ MCS7
Receive sensitivity (tolerance: ±2 dBm)	802.11a: -81 dBm ± 2 dBm @ 54 Mbps 802.11b: -92 dBm ± 2 dBm @ 11 Mbps 802.11g: -82 dBm ± 2 dBm @ 54 Mbps 802.11gn HT20: -79 dBm ± 2 dBm @ MCS7 802.11gn HT40: -76 dBm ± 2 dBm @ MCS7 802.11an HT20: -78 dBm ± 2 dBm @ MCS7 802.11an HT40: -74 dBm ± 2 dBm @ MCS7
Power consumption (typical)	Transmit: 80 mA Receive: 350 mA

[1] The maximum power setting will vary by channel and according to individual country regulations.

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 US	Listed by the Canadian Standards Association.
N10140	Conforms to relevant Australian standards
KC	Conforms to relevant South Korean EMC Standards

Memory

Internal memory	The OneTouch 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. The supplied SD card has a capacity of 4 GB. FAT and FAT32 file systems are supported.
USB 2.0 port	The OneTouch 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.

FCC and IC Interference Statement

Federal Communication Commission and Industry Canada Interference Statement:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC and IC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada.

Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Identification Numbers

FCC ID: WA7-AR5BHB112

IC ID: 6627C-AR5BHB112

Exposure to RF Energy

THIS MODEL DEVICE MEETS U.S. AND INTERNATIONAL REQUIREMENTS FOR EXPOSURE TO RADIO FREQUENCY RADIATION.

The OneTouch AT is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government and by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). The device also meets the European Radio and Telecommunications Terminal Equipment (R&TTE) directive, for protecting the health and safety of the user and other persons.

These limits are part of comprehensive guidelines that establish permitted levels of RF energy for the general population. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

Before a device model is available for sale to the public, it must be tested and certified to operate within the limits for safe exposure established by the FCC and international organizations. The tests are performed in positions and locations (e.g., next to the body) as required by the FCC for each model. The FCC has granted an Equipment Authorization for this model device with all reported SAR levels (see below) evaluated as in compliance with the FCC RF emission guidelines.

This device meets RF exposure guidelines when the antennas are positioned at a minimum distance from the body. In order to transmit data or messages, this device requires a quality connection to the network. In some cases, transmission of data or messages may be delayed until such a connection becomes available. Be sure that the recommended distance is observed until the transmission is complete.

The exposure standard for wireless devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. Tests for SAR are conducted using standard operating positions specified by the FCC with the device transmitting at its highest certified power level in all tested frequency bands. The SAR limit set by the FCC is 1.6 W/kg. The international guidelines state that the SAR limit for mobile devices used by the public is 2.0 W/kg averaged over 10 grams of body tissue. SAR values may vary depending on national reporting requirements and the network band. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value because the device operates at multiple power levels and uses only the power required to reach the network.

SAR information on this model device is on file with the FCC and can be found under the Display Grant section http://www.fcc.gov/oet/fccid after searching on FCC ID: WA7-AR5BHB112.

Europe-EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN61010-1: 2001 A11: 2004
  Safety requirements for electrical equipment for measurement, control, and laboratory use
- EN50385: (2002-08)
  Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz to 40 GHz) - General public

- EN 300 328 V1.7.1: (2006-10)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 893 V1.4.1: (2007-07)
  Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- EN 301 489-1 V1.8.1: (2008-04)
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17 V2.1.1 (2009-05)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment
- EN 60950-1: Information technology equipment - Safety - Part1: General requirements
- EN 301 893 V1.5.1: (2008-12) Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

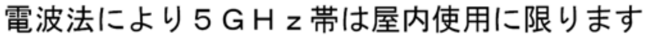
This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 MHz to 2483.5 MHz.

For detailed information the end-user should contact the national spectrum authority in France.

Japan Statement



電波法により５ＧＨｚ帯は屋内使用に限ります

(5 GHz radio band method is limited to indoor use.)

Brazil Statement

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

(This equipment operates on a secondary basis and, consequently, must accept harmful interference, including from stations of the same kind, and may not cause harmful interference to systems operating on a primary basis.)

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 —